

#31 Junho 2007
LINUX
MAGAZINE

LINUX

MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

exemplar de
Assinante
venda proibida

MONITORAMENTO DE REDES

p.31

CONHEÇA EM PROFUNDIDADE O NAGIOS, A MAIS IMPORTANTE
FERRAMENTA DE CÓDIGO ABERTO PARA MONITORAMENTO

- » **Instale e configure o Nagios e seus plugins** p.32
- » **Interface profissional com o GroundWork** p.40
- » **Plugins personalizados usando Perl** p.74

ACORDO NOVELL-MS p.26

CEO da Novell explica o significado da
parceria em entrevista exclusiva

VIRTUALBOX p.60

Competência e velocidade no
rival aberto do VMware

VEJA TAMBÉM NESTA EDIÇÃO:

- » **Curso LPI: Última aula para LPI-1** r 47
- » **Looking Glass, o inovador desktop 3D da Sun** r 45
- » **Ext4: Esse sistema de arquivos vale a pena?** l 57
- » **Dados confiáveis com as barreiras de escrita** l 69
- » **Autenticação segura no Squid com Digest e OpenLDAP** l 64

FRACTO

Hospedagem de sites

Registros de Domínios

Servidor VPS

Servidor Dedicado

Servidor Virtual

Collocation

IP Dedicado

0800

Planos DDD/DDI

VPN IP

Frame Relay

Ligações Locais

www.fracto.com.br
SP (11) 3523-1580
3835-6990
RJ (21) 3723-1580

**Agente
Autorizado
Intelig**
Telecom

SOLUÇÕES

COMPLETAS PARA SUA EMPRESA
CRESCER A CADA DIA.

Expediente editorial

Diretor Geral

Rafael Peregrino da Silva
peregrino@linuxmagazine.com.br

Editor-chefe

Tadeu Carmona
tcarmona@linuxmagazine.com.br

Editor

Pablo Hess
phess@linuxmagazine.com.br

Revisão

Arali Lobo Gomes
agomes@linuxmagazine.com.br

Assistente de Arte

Renan Herrera
rherrera@linuxmagazine.com.br

Centros de Competência

Centro de Competência em Software:

Oliver Frommel: ofrommel@linuxnewmedia.de
Kristian Kibling: kkibling@linuxnewmedia.de
Peter Kreussel: pkreussel@linuxnewmedia.de
Marcel Hilzinger: hilzinger@linuxnewmedia.de
Andrea Müller: amueller@linuxnewmedia.de

Centro de Competência em Redes e Segurança:

Achim Leitner: aleitner@linuxnewmedia.de
Jens-Christoph B.: jbreindel@linuxnewmedia.de
Hans-Georg Eber: hgesser@linuxnewmedia.de
Thomas L.: tleichtenstern@linuxnewmedia.de
Max Werner: mwerner@linuxnewmedia.de

Correspondentes & Colaboradores

Augusto Campos, Cezar Taurion, Charly Kühnast, Emanuel dos Reis Rodrigues, Fabrizio Ciacchi, James Mohr, Joe Casad, Julian Hein, Klaus Knopper, Luciano Siqueira, Marcel Hilzinger, Martin Steigewald, Michael Schilli, Thomas Leichtenstern, Zack Brown

Anúncios:

Rafael Peregrino da Silva (Brasil)
anuncios@linuxmagazine.com.br
Tel.: +55 (0)11 2161 5400
Fax: +55 (0)11 2161 5410

Osmund Schmidt (Alemanha, Áustria e Suíça)
anzeigen@linux-magazine.com

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

Assinaturas:

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

Na Internet:

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

Circulação

Cláudio Guilherme dos Santos
csantos@linuxmagazine.com.br

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

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

Linux é uma marca registrada de Linus Torvalds.

Linux Magazine é publicada mensalmente por:

Linux New Media do Brasil Editora Ltda.

Av. Fagundes Filho, 134
Conj. 53 – Saúde
04304-000 – São Paulo – SP – Brasil
Tel.: +55 (0)11 2161 5400
Fax: +55 (0)11 2161 5410

Direitos Autorais e Marcas Registradas © 2004 - 2007:
Linux New Media do Brasil Editora Ltda.

Distribuição: Distmag

Impressão e Acabamento: Parma

ISSN 1806-9428

Impresso no Brasil



Enquanto durou

Prezados leitores da Linux Magazine,

Mahatma Gandhi versou sobre os resultados de seu protesto pacífico contra a tirania britânica: “Primeiro eles o ignoram. Depois riem de você. Depois o combatem. E então você vence”. Embora essas palavras possuam um significado bem definido no espaço – a Índia – e no tempo – a primeira metade do século XX –, elas já foram muito usadas por várias pessoas que se sentiram de alguma forma oprimidas.

Uma das comunidades que mais abraçou tais pensamentos como algo profético é a do Software Livre e de Código Aberto (SL/CA), como se pode ver no inspiradíssimo vídeo “Truth happens” criado pela Red Hat. O opressor referido, nesse caso, era a Microsoft, com suas práticas monopolistas já publicamente punidas.

Durante alguns meses, certamente muitos integrantes da comunidade do SL/CA acreditaram que a “profecia” não se realizaria, pois a Microsoft teria parado de combater o Linux. Através do acordo com a Novell, especulava-se que a empresa de Bill Gates estaria disposta, finalmente, a colaborar com o SL/CA. Como se costuma dizer, essa crença foi boa enquanto durou.

Na entrevista concedida por Ron Hovsepian a Rafael Peregrino, publicada à página 26 desta edição, o CEO e Presidente da Novell afirma que sua empresa e a Microsoft concordam que processar usuários não faz bem à imagem da autora da ação. Redmond mostrou que essa colocação só se aplica quando há um acordo para tornar obrigatório esse comportamento.

Até mesmo Bill Hilf, mentor do SL/CA dentro da Microsoft e coordenador do propalado laboratório de interoperabilidade, mostrou um sério desconhecimento da afinidade entre a tecnologia do SL/CA e o mercado corporativo, afirmando que “O Linux está morto. Até Linus tem um emprego.”

A ofensiva da fabricante do Windows contra o Linux, incluindo sua postura após o anúncio inicial de que processaria os usuários do sistema operacional aberto, reforçou a forte estratégia de FUD (medo, incerteza e dúvida, na sigla em inglês) iniciada com sua nada memorável campanha “Get the facts”.

É marcante o contraste com a Sun de Simon Phipps – também entrevistado nesta edição –, que mostra uma compreensão bem mais profunda dessa tecnologia. A fabricante do OpenSolaris e maior contribuidora do SL/CA em 2006 demonstra compromisso com seus consumidores e desenvolvedores ao criar uma licença livre para uso geral – e não apenas em favor de si mesma –, e também um sólido interesse nessa nova tecnologia, ao buscar formas de lucrar com softwares abertos.

Se são essas as armas que se apresentam no combate contra o SL/CA, só nos resta esperar pela validação da conclusão: “E então você vence”.

Pablo Hess
Editor

Nota: A seção *Preview* da última edição da **Linux Magazine** informava que na edição atual seriam publicadas matérias sobre softwares de *groupware* e também sobre o *Abaqus*. Infelizmente, tivemos de reorganizar a pauta da **Linux Magazine** de junho, e publicaremos as matérias sobre esses assuntos na edição de julho (número 32).



CAPA

O verdadeiro Grande Irmão

32

O versátil Nagios monitora sua rede através de plugins, e emite alertas antes que haja problemas com máquinas e serviços. Aprenda em profundidade como instalar, usar e gerenciar esse ícone do monitoramento de redes.

Trabalho de base

40

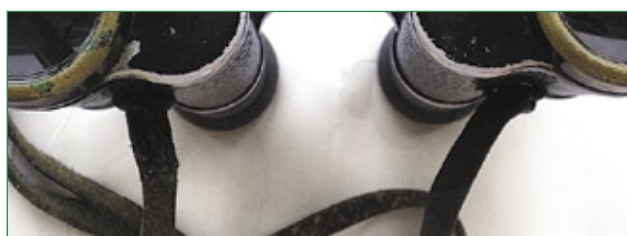
O Nagios possui uma interface web bastante básica. O GroundWork é uma interface mais amigável e com visual profissional para essa ferramenta.

PROGRAMAÇÃO

Plugando no Nagios

74

Veja como utilizar a versátil linguagem Perl para criar plugins personalizados para o daemon de monitoramento de redes Nagios.



COLUNAS

Augusto Campos	08
Charly Kühnast	10
Klaus Knopper	12
Zack Brown	14

NOTÍCIAS

Segurança	16
♦ OpenOffice.org	
♦ XMMS	
♦ File	
♦ Libwpd	
♦ Biblioteca do KDE	
♦ Squid	
♦ Evolution	
♦ Firefox	
♦ NAS	
♦ Inkscape	
♦ Apache JK Tomcat Connector	
Geral	18
♦ Microsoft: Linux viola patentes	
♦ Notebooks para todos	
♦ Easy Linux está de volta	
♦ Gaim vira Pidgin	
♦ Debates sobre o formato ODF	
♦ De iniciante a "power user" em um livro	

CORPORATE

Notícias	20
♦ Virtualização mudará cenário de TI, diz Gartner	
♦ Insigne investe em relacionamento e busca novos parceiros	
♦ Ponto Frio economiza 20% com Linux	
♦ Linux em appliance da SanDisk	
♦ Novo VP da Novell para América Latina	
♦ Red Hat e IBM pelo mainframe	
♦ Workstation HP com Linux a preços reduzidos	
Reportagem: Linux Park	22
Entrevista: Ron Hovsepian	26
Entrevista: Simon Phipps	28
Coluna: Cezar Taurion	30

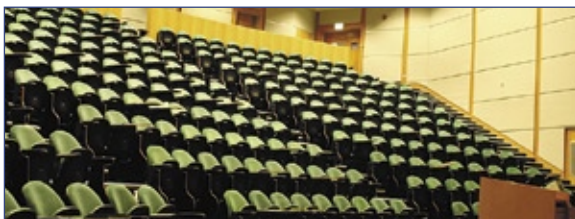
ANÁLISE

Outra visão	45
O ambiente desktop 3D Looking Glass oferece uma nova visão da área de trabalho.	

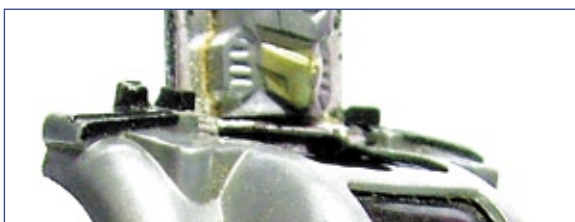


Tutorial

LPI nível 1: Aula 6	47
Configure compartilhamentos de rede e aprenda a administrar a segurança do sistema na última aula da série de preparação para a certificação LPI nível 1.	



Pronto para o futuro	57
O próximo sistema de arquivos da família Ext oferece melhor desempenho e sistemas de arquivo maiores. Você está preparado para o Ext4?	



Caixinha virtual	60
Se você quer fugir das ferramentas de virtualização muito complexas ou caras, experimente o VirtualBox.	



SYSADMIN

Acesso mais seguro	64
Use o sistema de autenticação por Digest no Squid e evite a exposição de senhas.	



Organizando a fila	69
Um bom disco rígido e um sistema de arquivos com journal não eliminam totalmente a perda de dados. É preciso ir além.	

SERVIÇOS

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

Emails para o editor

Permissão de Escrita

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

Moda do Vista

Tenho comprado a revista nas bancas há alguns meses, e até pensei em fazer uma assinatura. Porém, me incomodam as várias citações a sistemas Microsoft nas matérias.

Acho que vocês estão se afastando dos objetivos de seus leitores. Não preciso de informações sobre os produtos da Microsoft – já existem muitas revistas sobre esse assunto. Estou mais interessado em artigos sobre o mundo do software Livre e em discussões úteis sobre o Linux ou seus programas.

Também tenho interesse em mais artigos sobre o ambiente TCP/IP, assim como funções de gerenciamento por SNMP. Vocês já estão falando sobre esses tópicos.

Antonio Moura Gomes

Salvador, BA

Obrigado por seus comentários. Temos abordado especialmente o Vista devido às questões que ele, enquanto novidade nos atuais ambientes de rede, pode levantar. Entendemos que há diversas revistas sobre os sistemas Microsoft, porém nossa percepção é de que todas contam com informações fornecidas e tópicos estimulados pela própria fabricante do Windows. Enquanto isso, nós oferecemos uma visão real do Windows Vista, a partir da perspectiva do Linux.

De resto, nossos autores citam o Windows quando julgam ser importante para a aplicação adequada das informações contidas em seus artigos, pois é muito comum o uso de ambos os sistemas numa mesma rede corporativa. ■

Linux PowerPC

Tenho um servidor onde hospedo o site de uma instituição pública. Aguardo ansiosamente sua revista todos os meses, e freqüentemente releio números antigos. Tento também baixar distribuições de todos os cantos, só para conhecer e “brincar”.

Pelo que constatei, o *Yellow Dog 3* funciona direito em PowerPCs G3, mas não nos G4. Agora estou esperando a versão 5, para o Playstation 3.

Uso tanto sistemas x86 quando PowerPC, e vejo que todos os DVDs que a revista publica ou vende são exclusivos para máquinas x86. Será que não é possível fazer pelo menos um DVD para PPC a cada ano?

Roberto Gianpaolo

São Paulo, SP

Já pensamos muitas vezes na possibilidade de oferecer alguma distribuição para PPC em nossos DVDs. O problema é que a maioria dos nossos leitores não poderia usá-la, já que preferem a arquitetura x86. Muitos observadores estão inclusive duvidosos quanto ao futuro do PPC na computação pessoal desde que a Apple decidiu adotar processadores x86 em seus sistemas.

Já publicamos artigos sobre PowerPC no passado, e continuaremos cobrindo essa arquitetura enquanto ela permanecer uma plataforma viável para o Linux. No entanto, no momento um DVD para PowerPC não está em nossos planos. ■

Errata

Na última edição, a figura 5 do artigo *Insigne representante*, à página 47, possui um erro na legenda. O conteúdo correto da legenda é “Pacotes extras proprietários são instalados com o *Insigne Mágico*”.



Itautec

SEJA LIBRIX NA RUA, SEJA LIBRIX EM CASA, SEJA LIBRIX NO TRABALHO.

Agora, além do Librix (Linux da Itautec), a sua empresa pode contar com o melhor e mais estável pacote de hardware e software do mercado, testado e homologado pela Itautec.

Toda a **liberdade** que você precisa para trabalhar com mais mobilidade, usando a internet sem fio, e ainda operar com software livre.

É mais **segurança**, porque a Itautec oferece suporte técnico especializado via internet ou pelo telefone, serviços de tuning e configuração e ainda atendimento nacional on site.

Tem alta **tecnologia** para os aplicativos como editor de textos, planilha eletrônica, editor de imagens e apresentações. É mais facilidade e maior flexibilidade no seu dia-a-dia. Na hora de trabalhar, não se sinta preso. Seja Librix.



Itautec InfoWay Minitorre

IDEAL PARA ENTRETENIMENTO
E ESTAÇÃO DE TRABALHO.

Código da oferta: IN-579

- Processador Intel® Celeron® D 315 (256 KB L2 cache, 2.26 GHz, 533 MHz)
- Librix - Distribuição Linux Itautec
- 512 MB de memória • Monitor de 17" • HD de 40 GB
- Combo (gravador de CD + leitor de DVD)
- Floppy, teclado em português e mouse
- Placa de rede integrada
- Placa de áudio e vídeo integrada
- Fax/Modem 56 Kbps
- 1 ano de garantia balcão****

10x R\$ 109,90

ou **36x R\$ 36,32**
pelo cartão BNDES*
ou R\$ 1.099,00 à vista



Servidor Itautec LX201

PERFORMANCE E SEGURANÇA
PARA A SUA EMPRESA.

Código da oferta: SI-310

- Processador Intel® Xeon® 5030 (2 x 2 MB L2 cache, 2.67 GHz, 667 MHz)
- Librix Server - Distribuição Linux Itautec**
- 1 GB de memória com ECC
- 2 HDs SATA de 200 GB
- CD-RW (gravador de CD)
- 2 interfaces de rede integradas
- Controladora 6 canais SATA integrada
- Teclado e mouse
- Gabinete-pedestal
- 3 anos de garantia on site***

36x R\$ 155,28
pelo cartão BNDES*
ou R\$ 4.699,00 à vista



PRESENTE EM MAIS
DE 2.700 CIDADES.

www.itauteshop.com.br
COMPRE DIRETAMENTE DO FABRICANTE

0800 121 444

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

Ofertas válidas até 7/6/2007 ou enquanto durarem os estoques. Celeron, Celeron Inside, Centrino, o logotipo Centrino, Core Inside, Intel, o logotipo Intel, Intel Core, Intel Inside, o logotipo Intel Inside, Intel Viiv, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, Xeon e Xeon Inside são marcas comerciais ou marcas registradas da Intel Corporation ou de suas subsidiárias nos Estados Unidos ou em outros países. Consulte nossa Central de Atendimento para informações sobre outras condições de financiamento para pessoa física ou jurídica pelo telefone 0800-121-444. *Financiamento para pessoa jurídica através do cartão BNDES, com taxa de 1,03% a.m. Necessário possuir o cartão de crédito citado, sujeito à confirmação da disponibilidade da linha de crédito para as localidades e limite para operação. **Suporte telefônico para o Sistema Operacional Librix - 8 x 5, de segunda a sexta-feira, das 9h às 18h. ***Garantia de três anos on site, de segunda a sexta-feira, das 8h30 às 18h, em um raio de 50 km do Centro de Serviços Itautec mais próximo. ****Garantia balcão de um ano para partes, peças e serviços. A velocidade de comunicação de 56 Kbps depende e pode variar de acordo com o tipo e a qualidade da linha telefônica utilizada. Para possibilitar o acesso à internet são necessários uma linha telefônica ou banda larga e um provedor à sua escolha. Preços com impostos incluídos para São Paulo. Frete não incluído. Demais características técnicas e de comercialização estão disponíveis em nosso site e no Televidas. Fica ressalvada eventual retificação das ofertas aqui veiculadas. Quantidade: 10 unidades de cada. Empresa/produto beneficiado pela Lei de Informática. Fotos meramente ilustrativas.

© Linux New Media do Brasil Editora Ltda.



Certificação LPI

Augusto Campos

Todo administrador de sistemas deve conhecer as certificações disponíveis e a sua importância para a empregabilidade.

por Augusto Campos

Esta edição da Linux Magazine traz o último artigo da série que nos meses recentes deu uma interessante amostra dos temas abordados no exame da certificação LPI nível 1, voltado para administradores de sistemas Linux nível júnior. O LPI foi fundado em 1999, na forma de uma organização sem fins lucrativos, dedicada à certificação de profissionais do Linux, e tem como diferencial o posicionamento de ser independente de distribuição e fornecedor – o que significa que na mesma prova você pode ter de resolver questões sobre pacotes *DEB* e *RPM*, por exemplo.

O posicionamento do LPI varia ao longo do tempo: originalmente, as certificações valiam por prazo indefinido. Em 2006 decidiu-se que elas passariam a valer por apenas cinco anos. Mesmo quem obteve cer-

estudo de fato está relacionado às habilidades e talentos exigidos de um administrador de sistemas Linux.

Diversos brasileiros fizeram e ainda fazem sua parte para apoiar os colegas que estão em busca de obter sua certificação. Merece destaque o exemplo de Bruno Gomes Pessanha, que, mesmo trabalhando como administrador de sistemas em uma empresa de grande porte (e numa rede com necessidades complexas), desde 2002 encontrou tempo e oportunidade para colaborar diretamente com o LPI – especialmente nas atividades de tradução de material – e mais recentemente foi co-autor do livro “Linux Certification in a Nutshell”, que cobre os níveis 1 e 2 do LPI, e foi escrito pensando em servir como guia de administração, e não apenas para passar nos exames. O livro foi publicado internacionalmente pela prestigiada editora O’Reilly, e ganhou o prêmio da escolha dos editores do Linux Journal em 2006, na categoria de livros de administração de sistemas.

Bruno certamente não é o único: Gleydson Mazioli, o autor do Guia Foca Linux[2] – um dos mais conhecidos manuais livres sobre Linux em nosso idioma – também adaptou sua documentação ao conteúdo programático das provas do instituto, e coleciona relatos de leitores que o procuram para contar que passaram no exame graças ao seu excelente material.

Obter uma certificação profissional é importante para a sua empregabilidade, e o LPI pode ser uma opção digna do seu esforço. A comunidade Linux já se encarregou de disponibilizar uma série de guias, livros, manuais e até provas simuladas para que você possa se preparar adequadamente – mas o próximo passo precisa ser seu. ■

Mais Informações

[1] Comunicado da LPI Brasil: <http://www.lpi.org.br/>

[2] Guia Foca Linux: <http://www.guiafoca.org/>

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.



Uma característica persistiu: o LPI continua sendo uma certificação independente de fornecedores.

tificação antes da alteração passou a ter de se certificar novamente a cada cinco anos, caso queira continuar contando com o título.

Outra mudança ocorreu na gestão da operação brasileira do LPI, que até 2006 era responsabilidade do LPI Brasil, entidade integrada por uma série de participantes da comunidade Linux brasileira (eu entre eles). A partir de agosto de 2006, por decisão do LPI mundial, passou a ser realizada pela empresa 4Linux. No processo, a ONG LPI Brasil foi extinta, emitindo um comunicado[1] em que divulgou não achar adequado aceitar outro papel que não permitisse manter a coordenação das ações da certificação LPI e nem as políticas existentes à época para os preços das provas no Brasil – que, no fechamento desta coluna, estão na faixa dos US\$ 130.

Uma característica persistiu: o LPI continua sendo uma certificação independente de fornecedores, com boa visibilidade no mercado, e conteúdo programático cujo

PORTA 25,
AGORA NA
VERSÃO 2.0.
ENTRE E FIQUE
À VONTADE.

O blog do Open Source Software Lab da Microsoft está de cara nova.

Quem quer saber mais sobre open source não pode ficar de fora do Porta 25. Agora na versão 2.0, o site está ainda mais interativo e aberto à sua participação. Ele tem novas funcionalidades e a navegação está mais completa, com mais espaço para as iniciativas do mercado brasileiro. Entre agora mesmo: **www.porta25.com.br**



CGI:IRC

Charly Kühnast

Seu firewall frustra suas tentativas de conexão ao IRC? Com o CGI:IRC, apenas um navegador web é necessário.

por Charly Kühnast

Em algumas situações, prefiro conversar *on-line* do que telefonar para as pessoas. Meu cliente IRC preferido é o *Irssi* [1]. Ele roda em uma sessão de tela num servidor que consigo acessar por SSH de qualquer lugar.

Às vezes, SSH simplesmente não é uma opção, como nos casos em que o firewall de um cliente está muito restrito, ou quando utilizo algum cybercafé nas férias. Uma ferramenta com o tipograficamente desafiador nome de CGI:IRC [2] pode ser a solução. O programa oferece uma interface web que passa a entrada recebida para o servidor IRC (figura 1).

O que eu gosto no CGI:IRC é sua instalação fácil e rápida, sem no entanto restringir as opções de configuração. Para a instalação, apenas é necessário um servidor web com CGI ativado, além da versão 5 da linguagem *Perl*.

Apenas faça o *upload* do script para o servidor, e coloque os arquivos de configuração no diretório CGI deste. A página de instalação [3] dá dicas úteis a respeito desses passos.

O CGI:IRC utiliza uma abordagem incomum, porém inteligente, em seus dois arquivos de configuração. Um deles contém as configurações críticas, que podem ser feitas em poucos minutos para que você já comece a usá-lo imediatamente. O outro arquivo, *cgiirc.config.full*, contém exemplos de configurações mais complexas.

Comecei verificando a configuração básica: o item *default_server* abriga o nome do meu servidor IRC, enquanto *default_port* guarda o número da porta.

A porta padrão é 6667, apesar de servidores em portas diferentes estarem crescendo bastante devido ao bloqueio das portas de IRC por parte de vários provedores de hospedagem.

A variável *default_channel* contém uma lista de canais, separados por vírgulas, que o usuário do CGI:IRC tem permissão de usar. O usuário não pode acessar nenhum canal ausente nessa lista.

Ao entrar no CGI:IRC, é possível escolher um apelido. Se o usuário preferir não escolher nenhum, o programa simplesmente atribui um nome com base no esquema especificado na variável *default_nick*. O padrão, nesse caso, é *CGIxxx*, onde *xxx* é substituído por um número, após o login.

Controle de acesso

O arquivo *ipaccess* lida com o controle de acesso. O CGI:IRC simplesmente ignora quem não possuir uma entrada nesse arquivo, da seguinte forma:

```
ip_access_file = ipaccess
```

Para suportar qualquer número de conexões a partir do *localhost*, é possível apenas acrescentar uma entrada para 127.0.0.1 ao arquivo *ipaccess*. Para restringir a 50 o número de conexões simultâneas, a entrada seria: 127.0.0.1 50 .

Para impedir o acesso a partir de uma rede específica, como 10.0.0.0/8, por exemplo, a entrada seria simplesmente: 10.0.0.0/8 0 .

Após terminar a configuração, é possível conversar infinitamente e de forma imediata, independente de onde se esteja. ■

Mais Informações

[1] Irssi: <http://www.irssi.org>

[2] CGI:IRC: <http://cgiirc.sourceforge.net>

[3] Dicas de instalação (em inglês): <http://cgiirc.sourceforge.net/docs/install.php>

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.

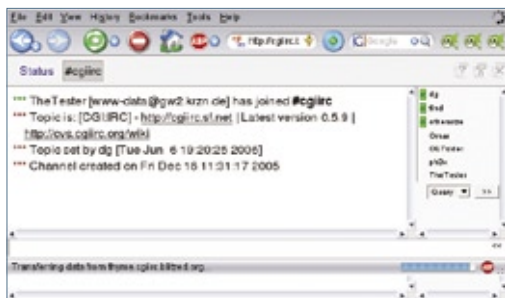
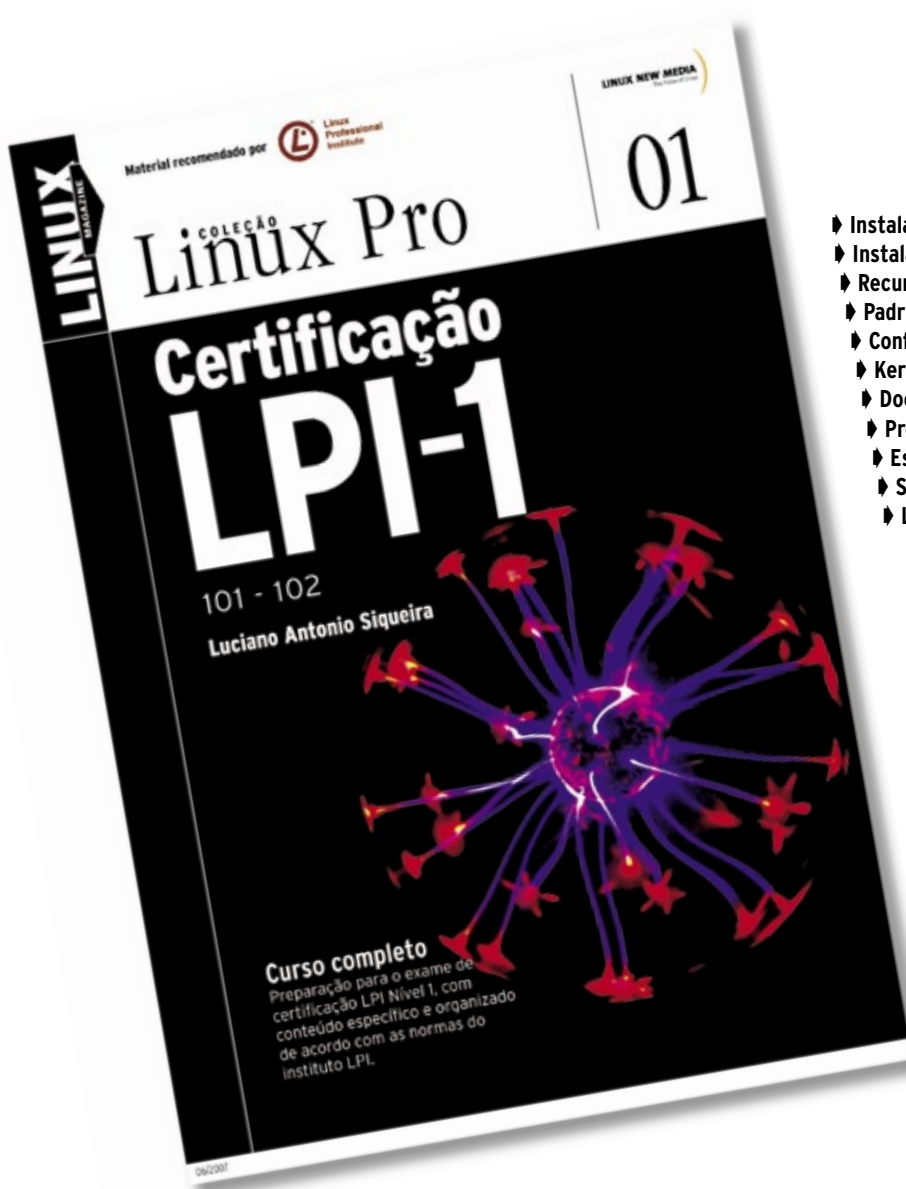


Figura 1 Conversa com um diferencial – o CGI:IRC fornece um cliente IRC acessível de qualquer local, através de um servidor web.

Conheça a nova coleção Linux Pro

Prepare-se para a principal certificação profissional do mercado Linux!



- ♦ Instalação e configuração de hardware
- ♦ Instalação de programas (pacotes Debian e RPM)
- ♦ Recursos avançados do Shell e comandos GNU/Linux
- ♦ Padrões Linux e manutenção do sistema
- ♦ Configurações do servidor X
- ♦ Kernel e carregamento do sistema
- ♦ Documentação oficial e sistemas de impressão
- ♦ Programação shell script
- ♦ Estruturas de redes e servidores (Apache, ssh, [x]inetd, etc)
- ♦ Segurança: restrições de acesso a recursos
- ♦ Livro recomendado pelo LPI



Estude para a prova de acordo com o conteúdo programático estabelecido pelo LPI.

Em breve nas livrarias ou no site www.linuxmagazine.com.br

Pergunte ao Klaus!

Klaus Knopper

Esta coluna é baseada na seção "Ask Klaus!", publicada na Linux Magazine International.

por Klaus Knopper

Redetecção

Sou relativamente novo no uso do Linux. Já experimentei muitas distribuições, e o Suse 10.2 me deu uma ótima impressão. Finalmente consegui ativar os efeitos 3D (graças ao YaST).

Tenho uma máquina com uma placa-mãe com chipset Nvidia, 1 GB de memória, placa de vídeo ATI X700 Pro e um Athlon64 3500+. Porém, acho que chegou a hora de trocar por um modelo mais novo.

Comprei um Athlon64 X2 5200+ com 1 GB de memória e uma placa-mãe com chipset ATI com Crossfire, mantendo a placa de vídeo antiga.

Depois de atualizar meu hardware e colocar meus discos rígidos SATA no novo computador, o Suse 10.2 vai reeditar a nova configuração e configurar tudo como for necessário, ou eu precisarei reinstalar o sistema?

Resposta

Se você modificar os itens de hardware necessários durante a inicialização, provavelmente será necessário refazer o *ramdisk* inicial (*initrd*) que foi criado de forma personalizada para seu antigo sistema durante a instalação inicial.

Nesse caso, seu novo sistema simplesmente não iniciará mais a partir do disco rígido, informando-o que não consegue encontrar nenhuma partição. Para contornar isso, talvez se possa incluir todos os drivers necessários no *initrd* de seu sistema antigo, antes de trocar os discos rígidos de placa-mãe.

Exemplo 1: fixipw2100.sh

```
01 #!/bin/bash
02
03 # Mude isso de acordo com sua placa WiFi
04 WIFIDEV="eth1"
05
06 while true; do
07   LANG=C iwconfig "$WIFIDEV" | grep -q
08   unassociated
09   if [ "$?" = "0" ]; then
10     echo "`date`: Reconectando $WIFIDEV"
11     iwpriv "$WIFIDEV" reset
12     sleep 10
13   fi
14 done
```

Também deve ser possível realizar uma "instalação rápida" em modo de recuperação, usando o DVD de instalação, apenas para recriar o sistema de inicialização e preservar o conteúdo das partições do disco rígido. Lembre-se que é importantíssimo verificar

se você possui algum backup funcional dos dados importantes contidos no disco rígido, antes de deixar o instalador ou o procedimento de recuperação fazerem algo nos discos.

Conexão WLAN instável

O chipset WLAN *ipw2100* de meu notebook está funcionando com o driver contido no kernel 2.6.19. No entanto, após algum tempo, principalmente sob tráfego intenso, a conexão com o ponto de acesso falha, e eu recebo um status de *unassociated* no *iwconfig*. Após descarregar e recarregar o módulo *ipw2100* do kernel, a placa volta a funcionar, mas tenho que digitar novamente os parâmetros do *iwconfig*. Existe alguma falha no driver *ipw2100* ou as minhas configurações estão erradas?

Resposta

Creio que o problema possa ser tanto um bug no driver quanto no *firmware* que é passado para a placa e reiniciado a cada recarregamento do módulo. Parece que a placa se confunde quando o tráfego é muito grande ou a qualidade do sinal é baixa por algum tempo. Às vezes, nem se consegue identificar o motivo.

Embora eu não possa dizer o que exatamente tem de errado com o driver ou *firmware* *ipw2100*, aqui está uma forma conveniente de contornar isso, que tenho usado com sucesso em vários notebooks.

Esse pequeno script, iniciado pelo usuário root e em segundo plano, ordena que a placa faça um *reset* interno sem você precisar informar toda a configuração novamente. Ele apenas verifica a visibilidade do ponto de acesso a cada dez segundos, e faz a reconexão em caso de queda, o que costuma levar dois segundos.

O script do exemplo 1 pode ser executado com um `./fixipw2100.sh &` depois de sua placa ter sido iniciada. Ele não sobrescreve nenhuma configuração já existente. ■

O autor

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



ESMAGADORA!

É A SUA VANTAGEM EM HOSPEDAR SITES COM A GENTE,
E A NOSSA VANTAGEM SOBRE A CONCORRÊNCIA.



Plano Standard

Transferência: 50GB • Espaço: 500MB

R\$ 25,70



Plano SQL

Transferência: 100GB • Espaço: 1GB

R\$ 36,10



E-mail 1GB

A partir de

R\$ 0,90



Plano Terabyte

Transferência: 1TB • Espaço: 3GB

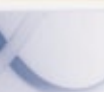
R\$ 135,00



Plano Ilimitado

Transferência: ilimitada • Espaço: 5GB

R\$ 250,00



ILIMITADA É A VANTAGEM DE CONTAR COM A PLUG IN.

Somente uma empresa como a PLUG IN, uma das líderes do mercado de webhosting no Brasil, pode oferecer aos profissionais de internet as melhores opções para hospedagem de sites com preços e franquias imbatíveis. Oferece ainda Data Centers de última geração e uma equipe 100% focada em atender as demandas do mercado digital.

Plugⁱⁿ

Internet para Profissionais de Internet

Capitais e Regiões Metropolitanas: 4003 1001

Outras Regiões: 0800 881 1001

www.plugin.com.br

Crônicas do kernel

Zack Brown

Rótulos de maturidade do código, JFFS e uma alternativa à proposta de Syslets. Veja as últimas invenções dos desenvolvedores do kernel.

por Zack Brown

Maturidade de código no sistema de configuração

Robert P. J. Day sugeriu a adição de alguns novos níveis de maturidade de código à estrutura *kbuild*: *DEPRECATED* e *OBSOLETE*. Infelizmente, a discussão acabou se concentrando em determinar o significado preciso de cada um desses termos. A idéia de Day era que “obsolete” significa que o código está completamente morto e sem suporte, enquanto “deprecated” é válido para aqueles códigos que ainda funcionam, embora exista ao menos uma

... nesse sentido, podemos esperar mais níveis de maturidade na interface de configuração do kernel, no futuro.

alternativa completamente viável. Outros desenvolvedores enxergavam a questão exatamente da forma oposta. Bartłomiej Zolnierkiewicz, por exemplo, considera “deprecated” como indicativo de que não há qualquer alternativa disponível, mas que o código é ruim e deveria ser substituído, enquanto “obsolete” significa que há uma alternativa, e portanto não é mais necessário usar o código antigo.

Tentativas de resolver a questão não tiveram sucesso algum – havia grande margem para interpretação. Por um lado, parecia que todos concordavam que esses níveis de maturidade seriam úteis; então, nesse sentido, podemos esperar mais níveis de maturidade na interface de configuração do kernel, no futuro. Sam Ravnborg e Day também discutiram formas de indicar o nível de maturidade no próprio nome da opção, durante a configuração. Atualmente, o único nível de maturidade disponível é *EXPERIMENTAL*, e a única forma de identificarmos uma opção experimental é procurando um grande “EXPERIMENTAL” ao final do nome da opção.

Adeus, JFFS

A já anunciada remoção do sistema de arquivos *JFFS*, superado pelo *JFFS2*, finalmente aconteceu! O *JFFS* foi retirado da árvore principal do kernel, e Adrian Bunk postou um patch para retirar também a respectiva entrada em *MAINTAINERS*.

David Brownell postou outro patch para marcar o código da porta paralela como não-mantido no arquivo *MAINTAINERS*, pois nenhum dos quatro desenvolvedores listados nele parece estar mantendo-o ativamente. Jean Delvare e Randy Dunlap concordaram com isso, e Delvare pediu encarecidamente que Andrew Morton se encarregasse do patch.

Joern Engel postou mais um patch para retirar completamente a entrada do *DevFS* do arquivo *MAINTAINERS* (ele já havia sido listado como obsoleto).

O *DevFS*, mais do que qualquer outro recurso removido, já causou muitas dores para que os desenvolvedores o retirassem do kernel completamente.

Syslets? Threadlets

Mês passado discuti o novo subsistema de *Syslets* de Ingo Molnar, que oferecia uma forma engenhosa de iniciar chamadas de sistema em segundo plano. Após Linus Torvalds declarar que achou a interface complicada e difícil demais para o usuário comum, Molnar mostrou um sistema modificado, introduzindo a idéia de *threadlets*. Elas são um complemento à idéia original de *syslets*, porém com uma interface muito mais simples. As *threadlets* são basicamente uma forma de iniciar funções arbitrárias em segundo plano com o recurso adicional de criar uma nova thread somente se a *threadlet* for bloqueada por algo; senão, o contexto permanece aquele do programa-pai. A desvantagem das *threadlets* é que são bem mais lentas que as *syslets*. ■

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.



nova regra do mercado

dividir para multiplicar



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

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

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

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

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



PARANÁ
PLATAFORMA DE
DESENVOLVIMENTO
DE SISTEMAS

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

Veja alguns exemplos das soluções desenvolvidas pela Celepar:

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

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

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

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

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



CELEPAR
INFORMÁTICA
do PARANÁ

Software Livre: o Paraná usa e abusa

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

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

© Linux New Media do Brasil Editora Ltda.



OpenOffice.org

Vários problemas de segurança foram descobertos no *OpenOffice.org*, um conjunto de aplicativos de escritório livres.

O *parser* do *Calc* contém um estouro de pilha facilmente explorável por um documento especialmente criado para executar código arbitrário. (CVE-2007-0238)

O *Openoffice.org* não escapa metacaracteres de *shell*, e é vulnerável à execução de comandos de *shell*

arbitrários através de um documento especialmente criado após o usuário clicar em um link preparado. (CVE-2007-0239) ■

Referência no Debian: DSA-1270-2

Referência no Mandriva: MDKSA-2007:073

Referência no Red Hat: RHSA-2007:0033-4

Referência no Suse: SUSE-SA:2007:023

Referência no Ubuntu: USN-444-1

XMMS

Sven Krewitt, da Secunia Research, descobriu que o XMMS (*X Multimedia System*) não lidava corretamente com imagens BMP ao carregar *skins* para sua interface gráfica. Um estouro de inteiros no XMMS 1.2.10, e possivelmente também em outras versões, permitia que agressores remotos, auxiliados por usuários locais, executassem código arbitrário através de informações maliciosas em uma imagem bitmap de skin, a qual causava a corrupção da memória. (CVE-2007-0653) ■

Referência no Mandriva: MDKSA-2007:071

Referência no Ubuntu: USN-445-1

File

O *file* é um utilitário que adivinha o formato de arquivos através de padrões dos dados binários. Um agressor remoto poderia convencer um usuário a executar o *file* em um arquivo especialmente criado, o que acionaria um estouro de *buffer* baseado em fila, possivelmente levando à execução de código arbitrário com os direitos do usuário que estivesse executando o *file*. Essa vulnerabilidade também poderia ser desencadeada através de um analisador automático de

arquivos, como o *amavisd-new*. (CVE-2007-1536) ■

Referência no Gentoo: GLSA 200703-26/file

Referência no Mandriva: MDKSA-2007:067

Referência no Red Hat: RHSA-2007:0124-2

Referência no Ubuntu: USN-439-1

Libwpd

A *Libwpd* é uma biblioteca para leitura e conversão de documentos do *WordPerfect*. A iDefense relatou várias falhas de estouro de inteiros na *Libwpd*. Agressores eram capazes de explorá-las com arquivos *WordPerfect* especialmente criados, os quais poderiam fazer um aplicativo linkado à biblioteca travar ou simplesmente executar código arbitrário. (CVE-2007-0002, CVE-2007-1466) ■

Referência no Debian: DSA-1268-1

Referência no Red Hat: RHSA-2007:0055-5

Referência no Slackware: SSA:2007-085-02

Referência no Ubuntu: USN-437-1

Biblioteca do KDE

O arquivo *ecma/kjs_html.cpp*, no *KDEJavaScript* (KJS), conforme usado no *Konqueror* do KDE 3.5.5, permite que agressores remotos causem uma negação de serviço (travamento) ao acessarem o

conteúdo de uma *iframe* com uma URI *ftp://* no atributo *src*, provavelmente devido a um direcionamento a um ponteiro nulo. Se um usuário for convencido a visitar um site malicioso, o *Konqueror* pode travar, resultando em uma negação de serviço. (CVE-2007-1308)

Foi descoberta também uma falha na forma como o *Konqueror* lida com respostas PASV de FTP. Se um usuário for convencido a visitar um servidor FTP malicioso, um agressor remoto poderia realizar uma varredura das portas das máquinas localizadas na mesma rede que o usuário, levando à divulgação de dados privados. (CVE-2007-1564) ■

Referência no Mandriva: MDKSA-2007:072

Referência no Ubuntu: USN-447-1

Squid

Foi descoberta uma vulnerabilidade no *Squid*, um servidor proxy multi-protocolo livre.

A função *clientProcessRequest()* em *src/client_side.c* no *Squid* 2.6 anterior ao 2.6.STABLE12 permite que agressores remotos causem uma negação de serviço (fechamento do *daemon*) através de requisições TRACE especialmente criadas

para gerar um erro de asserção. (CVE-2007-1560) ■

Referência no Gentoo: GLSA 200703-27/squid

Referência no Mandriva: MDKSA-2007:068

Referência no Ubuntu: USN-441-1

► Evolution

Um erro de formatação de cadeia de caracteres na função `write_html()` em `calendar/gui/e-cal-component-memo-preview.c`, ao exibir as categorias de uma nota, pode ser explorado para executar código arbitrário através de uma nota compartilhada especialmente criada contendo especificadores de formato. (CVE-2007-1002) ■

Referência no Mandriva: MDKSA-2007:070

Referência no Ubuntu: USN-442-1

► Firefox

Uma falha foi descoberta na forma como o *Firefox*, um navegador web de código aberto, lidava com respostas PASV de FTP.

Se um usuário for enganado de forma a visitar um servidor FTP

malicioso, um agressor remoto poderia realizar uma varredura de portas nas máquinas da rede do usuário, levando à divulgação de dados privados. (CVE-2007-1562) ■

Referência no Slackware: SSA:2007-066-03

Referência no Ubuntu: USN-443-1

► NAS

Foram descobertos vários problemas no *daemon* do NAS (*Network Audio System*). Agressores remotos podem enviar requisições de rede especialmente criadas, de forma a causar uma negação de serviço ou a execução de código arbitrário. (CVE-2007-1543, CVE-2007-1544, CVE-2007-1545, CVE-2007-1546, CVE-2007-1547) ■

Referência no Mandriva: MDKSA-2007:065

Referência no Ubuntu: USN-446-1

► Inkscape

Foi descoberta uma falha no uso que o *Inkscape*, um aplicativo de desenho vetorial de código aberto,

faz de cadeias de caracteres de formato. Se um usuário for enganado de forma a abrir no Inkscape uma URI especialmente criada, um agressor remoto poderia executar código arbitrário com os privilégios desse usuário. (CVE-2007-1463) ■

Referência no Mandriva: MDKSA-2007:069

Referência no Ubuntu: USN-438-1

► Apache JK Tomcat Connector

O *Apache Tomcat Connector (mod_jk)* contém uma vulnerabilidade de estouro de buffer que poderia resultar na execução remota de código arbitrário.

Um agressor remoto pode enviar uma requisição de URL longa para um servidor Apache, o que pode acionar a vulnerabilidade e levar a um estouro de inteiros baseado em pilha, resultando, assim, na execução de código arbitrário. (CVE-2007-0774) ■

Referência no Gentoo: GLSA 200703-16/mod_jk

Postura das principais distribuições Linux quanto à segurança

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

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

Microsoft: Linux viola patentes

A gigante do software proprietário anunciou em maio que há diversas patentes suas sendo violadas por softwares de Código Aberto. Somente o kernel Linux, segundo reportagem publicada na revista Fortune, violaria 42 patentes, enquanto os ambientes desktop livres contariam com 65 violações, e o *OpenOffice.org* com mais 45.

Apesar da alegada seriedade das violações, a empresa de Steve Ballmer informou que não pretende divulgar quais seriam essas patentes, assim como não disse o que fará a respeito das “contravenções”. Há que se ressaltar que, ainda que fosse divulgada a lista de patentes, a empresa de Redmond, EUA teria de provar sua validade nos tribunais.

Como era de se esperar, os analistas foram velozes em caracterizar a acusação como ato de desespero da Microsoft, ou como estratégia de extorsão para agregar mais parceiros

em esquemas semelhantes ao acordo da empresa com a Novell, cobrando dos supostos contraventores a imunidade aos processos. Muitos apontaram ainda para o fato de que muitas das empresas a serem processadas são também clientes da própria Microsoft, mostrando que a estratégia de acionar judicialmente os usuários realmente não seria positiva.

Pouco depois, o vice-presidente para assuntos de propriedade intelectual e licenciamento da MS, Horacio Gutierrez, afirmou que o objetivo de sua empresa é, de fato, angariar mais acordos como o firmado com a Novell no final de 2006, embora ele afirme não haver a intenção de processar usuários. ■



▶ Notebooks para todos

O Governo Federal ampliou no mês de maio seu programa de inclusão digital. O programa Computador Para Todos, em vigor desde 2005, já foi responsável por baixar significativamente os preços de computadores, além de oferecer financiamento para facilitar a compra das máquinas por pessoas de menor poder aquisitivo. Como reflexo, diversas famílias finalmente puderam adquirir seu primeiro computador.

Desde maio, a isenção tributária e a facilidade de concessão de linhas de crédito passou a valer também para computadores portáteis. No entanto, enquanto a margem de preços dos desktops foi reduzida de R\$ 1400 para R\$ 1200, os laptops favorecidos pelo programa devem obrigatoriamente ter preço máximo de R\$ 1800.

A expectativa é que sejam ofertados no mercado, assim como ocorreu com os desktops, diversos computadores portáteis por preços ainda menores que o patamar estabelecido pelo governo. ■



▶ Easy Linux está de volta

A revista **Easy Linux**, publicada pela Linux New Media do Brasil – responsável também pela **Linux Magazine** –, voltará a ser publicada a partir do mês de junho.

Com periodicidade mensal, a **Easy Linux** é destinada aos usuários iniciantes, domésticos e pequenas empresas. A revista esteve suspensa desde dezembro do último ano, devido a uma importante reestruturação, e terá como tema de capa, na edição 9, que circulará em junho, os jogos para Linux e aqueles executáveis sob o tradutor de APIs Wine. ■

▶ Gaim vira Pidgin

Após uma longa disputa judicial com a americana AOL, detentora da marca “AIM”, os desenvolvedores do mensageiro instantâneo multi-protocolo Gaim viram-se obrigados a mudar o nome do software. A empresa alega que o antigo nome do mensageiro instantâneo de código aberto era demasiadamente semelhante ao nome de seu próprio programa de mensagens instantâneas, o AIM (*AOL Instant Messenger*).

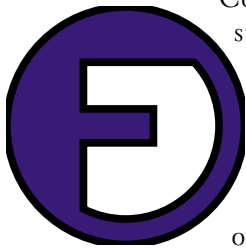
Os novos nomes escolhidos para os componentes do software são *Pidgin* para o programa em si, *Libpurple* para a antiga *Libgaim*, e *Finch* para o ex-*gaim-text* (cliente do software em modo texto).

O anúncio da mudança nos nomes veio junto com o da nova versão do programa, 2.0, que trouxe marcantes mudanças visuais e algumas melhorias de usabilidade. ■

Debates sobre o formato ODF

A Associação Brasileira de Normas Técnicas, órgão responsável pelo estabelecimento de regras e normas para diversos processos industriais e tecnológicos e único representante brasileiro na ISO (*International Organization for Standardization*), realizará ao longo do mês de junho algumas reuniões para debater a respeito dos formatos de documentos ODF e OpenXML.

A agenda dos encontros ainda não estava pronta no momento do fechamento desta edição, mas isso ocorrerá até o início do referido mês.



Como os debates estarão sujeitos ao acompanhamento público, é importante a participação de pessoas interessadas nesse processo, de forma a fazer valer sua opinião. ■

De iniciante a "power user" em um livro

Livros sobre Linux costumam sofrer de um problema dentro de dois: ou são exageradamente superficiais, para cobrir todos os assuntos pretendidos dentro dos limites de espaço disponíveis, ou focam-se em apenas alguns aspectos, deixando os outros, muitas vezes fundamentais, sem cobertura.

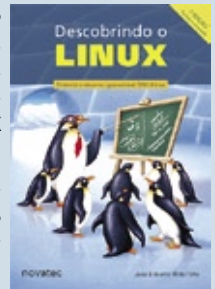
João Eriberto Mota Filho, co-autor do IPS de camada 2 HLBR e mantenedor de alguns pacotes do projeto *Debian*, no entanto, mostra grande perícia ao conseguir informar de forma consistente e ao mesmo tempo concisa, em aproximadamente 500 páginas, muito do que um usuário Linux iniciante necessita para se tornar um *power user*.

Começando pela história do projeto *GNU*, João Eriberto discute sobre todos os assuntos imprescindíveis aos usuários iniciantes, como a escolha de uma distribuição, o particionamento de discos, sistemas de arquivo e *runlevels*.

De forma leve e dinâmica, sem no entanto ser superficial, o livro fornece uma maior compreensão dos fundamentos técnicos do sistema. O leitor chega à página 300 apto a gerenciar múltiplas versões de kernel instaladas no mesmo sistema.

Nas páginas seguintes, João Eriberto acerta ao tocar no processo de compilação de programas, baseando-se em um exemplo real. Mais adiante, explica conceitos de redes ethernet antes de introduzir a configuração do GNU/Linux como cliente nessas redes, além de ADSL, e Wi-Fi.

Para finalizar, uma seção adicionada na segunda edição lembra que, quando passar a empolgação com as linhas de código subindo na tela durante a compilação ou com o acompanhamento do *MRTG*, pode-se lançar mão dos diversos jogos disponíveis para o GNU/Linux. Os melhores de cada estilo são mostrados com capturas de tela e um breve texto descritivo.



LINUX IMPACTA

"O mercado de Linux vai movimentar US\$19 milhões até 2007"*

Confira os melhores treinamentos do Brasil!

Preparatório para a Certificação LPI

Linux LPI 101 - Fundamentos | Linux LPI 101- Implementação e Adm. | Linux LPI 102 - Gerenciamento e Manutenção | Linux LPI 102 - Impl. de Infra-estrutura de Redes

Avançado:

Linux Shell Script | LDAP | Apache | Samba | Firewall

25% de desconto + camiseta



Participe do evento Linux Day. Data: 23/06. Inscreva-se no site: www.impacta.com.br



IMPACTA
TECNOLOGIA
Divisão Networking



Av. Paulista, 1009 - 9º andar
Tel: (11) 3254-2200 | www.impacta.com.br
*fonte: IDC

Virtualização mudará cenário de TI, diz Gartner

Um estudo do grupo de pesquisas de mercado Gartner concluiu que a virtualização será responsável por mudanças radicais na infra-estrutura de TI nos próximos anos. Segundo o estudo, não apenas o uso da tecnologia da informação sofrerá alterações, mas também a forma como os departamentos de TI gerenciam, compram, planejam e cobram por seus serviços. Até 2010, de acordo com o Gartner, a virtualização será a tecnologia mais importante na área de infra-estrutura de TI.

Thomas Bittman, vice-presidente e analista do grupo, afirmou durante uma conferência em Sidney, Austrália, que a virtualização requer mudanças mais culturais do que tecnológicas dentro das empresas. Ainda segundo o analista, o número de máquinas virtuais instaladas no mundo todo, estimado em 540 mil ao final de 2006, deve chegar a 4 milhões até 2009, representando, ainda assim, apenas uma fração do mercado potencial.

Em relação às vendas de servidores, Bittman afirmou que “cada servidor virtual tem o potencial de tirar do mercado mais um servidor físico”, pois “atualmente, mais de 90% dos usuários de máquinas virtuais têm como motivação a redução do número de servidores, do espaço físico e do custo energético de máquinas x86 em suas empresas. Acreditamos que o mercado de servidores já diminuiu 4% em 2006 devido à virtualização, que terá um impacto bem maior em 2009”.

No mercado de virtualização de desktops, que se encontra “dois anos atrasado em relação ao de servidores”, segundo o vice-presidente, “mas será ainda maior que este”, a motivação é outra: isolamento e criação de um ambiente de gerenciamento intangível pelo usuário, com o potencial de “mudar o paradigma de gerenciamento de desktops corporativos”. ■

▶ Insigne investe em relacionamento e busca novos parceiros

A Insigne Free Software do Brasil, fabricante da distribuição Insigne Linux, que equipa diversos computadores incluídos no programa Computador Para Todos, está buscando fortalecer a confiança do usuário no sistema operacional. Para isso, a empresa investiu, ao longo de todo o primeiro ano de implantação do programa do Governo, na capacitação dos vendedores e integradores de sistemas responsáveis pelas vendas do Computador Para Todos. Segundo uma pesquisa realizada pela própria Insigne, essas máquinas foram o primeiro computador da maioria dos compradores atendidos pelo programa de inclusão digital.

A criação de um departamento de ouvidoria na Insigne foi responsável pelo estreitamento da relação entre o usuário e a fabricante do sistema operacional, mantendo o contato da empresa com o cliente e também recebendo sugestões e reclamações acerca de todos os aspectos do sistema e da empresa.

A participação em desktops domésticos e corporativos na América Latina também está nos planos da empresa, que está em busca de novos parceiros comerciais e técnicos no continente. O objetivo, de acordo com a Insigne, é credenciar ao menos um parceiro em cada um dos países vizinhos ao Brasil, de forma a garantir a distribuição e suporte aos usuários dessas localidades. ■

▶ Ponto Frio economiza 20% com Linux

A rede varejista Ponto Frio, segunda maior do Brasil, divulgou o resultado de sua adoção inicial do Librix, distribuição Linux da brasileira Itautech.

Segundo a empresa, o diferencial da solução adotada é o alto índice de estabilidade e a qualidade comprovada. Ao final dessa primeira fase de adoção do Linux, mais de três mil estações de trabalho pelo Brasil foram substituídas por máquinas Linux, renovando-se também o parque.

Segundo o diretor de tecnologia do Ponto Frio, Paulo Sanz, apenas o custo total de propriedade (TCO, na sigla em inglês) está incluído no cálculo dessa economia. Portanto, e tendo em conta os ganhos indiretos, como a segurança, por exemplo, pode-se chegar a uma economia ainda maior.

A parceria entre as duas empresas envolve não apenas o fornecimento de software e hardware, mas também a consultoria técnica, configuração de pacotes, implementação e homologação, além do suporte técnico. ■



Linux em appliance da SanDisk

A SanDisk, maior fornecedor mundial de dispositivos *flash* USB, anunciou o lançamento da *appliance TrustWatch*, para controle de drives *flash*. Segundo o anúncio da empresa, com o TrustWatch os dispositivos *flash* móveis, como pen drives, por exemplo, deixam de ser uma ameaça às redes corporativas.

A *appliance* realiza a criptografia e o controle das informações contidas nos dispositivos *flash* em toda a rede, e com isso obtém maior segurança contra o vazamento de informações confidenciais da empresa. ■



Novo VP da Novell para América Latina

Camillo Speroni é o novo vice-presidente e gerente geral da americana Novell para a América Latina. Após atuar na empresa por mais de quinze anos, nas áreas de vendas e marketing ao redor do planeta, além de ocupar cargos executivos regionais e globais, Speroni terá como responsabilidade focar os recursos da companhia e da região para conquistar consumidores nos mercados de gerenciamento de identidade e Linux. ■



Red Hat e IBM pelo mainframe

As americanas Red Hat e IBM firmaram uma aliança relativa ao desenvolvimento e comercialização de aplicações para mainframes. O *Red Hat Linux Enterprise* será vendido pela *big blue* em sua poderosa linha de servidores System z, e as parceiras farão um esforço conjunto na identificação de aplicações ainda não cobertas pelas ofertas já existentes.

Considerada um ataque à Novell, principal concorrente direta da Red Hat no mercado de sistemas Linux, a manobra impede que acordo semelhante seja realizado entre a IBM, maior fabricante de mainframes para esse mercado, e a dona do Suse Linux, embora tal parceria já tenha sido firmada no passado. ■



redhat.

Workstation HP com Linux a preços reduzidos

A HP do Brasil deseja mostrar aos consumidores que uma workstation pode ser mais valiosa que um desktop *high-end*. Para isso, reduziu o preço de sua workstation xw4400 de R\$ 6000,00 para R\$ 3900,00, que será vendida, a partir do terceiro trimestre, com o sistema operacional *Red Hat Enterprise Linux*. ■



Notas

Novo servidor da Bull para HPC

A Bull lançou recentemente o servidor NovaScale R422, capaz de atingir o dobro do desempenho de seu antecessor, ocupando o mesmo espaço. Com um pico de processamento de 5,4 Tflops (trilhões de operações de ponto flutuante por segundo), um dos diferenciais do lançamento é sua fonte de alta eficiência, que chega a 92%.

Comodo para RHEL e CentOS

A Comodo, fornecedora de soluções de certificação digital e gerenciamento de identidade, anunciou a nova versão de seu conjunto de aplicativos para gerenciamento completo de servidores *Zero Touch Linux (ZTL)*. Como novidade, os aplicativos agora rodam também em sistemas operacionais *Red Hat Enterprise* e *CentOS*. O ZTL está disponível gratuitamente, e pode ser baixado em <http://ztl.comodo.com>.

Recuperação de dados em Linux

A CBL Tech, empresa canadense especializada na recuperação de dados, está ampliando seu laboratório em Curitiba. Com o número de pedidos crescendo rapidamente, o antigo laboratório terá de ser ampliado, e está prevista uma área dedicada exclusivamente a sistemas Linux, devido ao aumento da demanda específica nessa área.

SLED em estações Sun

A Sun divulgou a nova oferta de sistema operacional em suas workstations Ultra 20 e Ultra 40. As máquinas, equipadas com processadores AMD Opteron, já estão sendo comercializadas com o *Suse Linux Enterprise Desktop 10*, da Novell, além das opções *Solaris 10*, *Red Hat Enterprise Linux 3* e 4, e *Windows XP*.

O mercado brasileiro de Software Livre e de Código Aberto

1º Seminário Linux Park 2007

Pela primeira vez fora de São Paulo, o Linux Park 2007 reuniu no Rio de Janeiro os principais players do mercado nacional de SL/CA, além de um público qualificado e participativo.

por Pablo Hess

LINUXPARK

Os seminários Linux Park, organizados pela Linux New Media do Brasil, já se consagraram no cenário corporativo nacional do Software Livre e de Código Aberto (SL/CA). Nas últimas edições do evento, ao todo centenas de executivos de TI reuniram-se para trocar experiências a respeito do uso do SL/CA em suas empresas.

A primeira edição dos seminários Linux Park 2007 ocorreu dia 26 de abril, pela primeira vez fora da cidade de São Paulo. A sala de convenções do Hotel Sofitel, no movimentado bairro de Copacabana, no Rio de Janeiro, foi ocupada pelo público numeroso e altamente qualificado (figura 1).

Novidade entre os participantes, instituições de ensino fundamental,

médio e superior estiveram presentes, mobilizadas pela Abrasol (Associação Brasileira de Software Livre). Representantes de diversos setores também marcaram presença, como varejo, Telecomunicações, Forças Armadas, Transportes, Indústria e Comércio de petróleo, Administração Municipal, Energia, Governo e, naturalmente, Tecnologia.

Às 9:00, Rafael Peregrino da Silva, Diretor Geral da Linux New Media do Brasil, iniciou seu *keynote* de abertura (figura 2) do primeiro Linux Park do ano. Após explicar os benefícios que a tecnologia do Software Livre e de Código Aberto (SL/CA) pode trazer às empresas, Rafael apresentou a Linux New Media, mencionando a atuação internacional da editora, que publica conteúdo específico sobre SL/CA em 67 países.

Em seguida, o Diretor Geral apresentou os resultados de uma pesquisa realizada pela Linux New Media do Brasil em parceria com a Intel, a respeito do mercado de Linux e SL/CA no Brasil, reforçando o conceito e a importância do ecossistema no contexto do mercado de TI. Inicialmente, Rafael listou as inúmeras plataformas em que o Linux está apto a rodar, incluindo o segmento de

dispositivos embarcados, no qual o sistema do pingüim oferece maiores margens de lucro em comparação às soluções proprietárias já existentes. Os modelos de distribuição de software também foram abordados, assim como as categorias de serviços possibilitadas pelo modelo aberto de desenvolvimento. A íntegra da apresentação, incluindo os resultados da pesquisa sobre o mercado nacional de SL/CA, pode ser obtida em [1].

Finalizando o *keynote*, Rafael exibiu as estatísticas da empresa de pesquisas de mercado Chadwick Martin Bailey, obtidas a partir de questionários respondidos por gerentes de TI, nas quais é possível constatar que o preço não é mais o principal fator na aquisição de soluções de TI.

O público respondeu ao *keynote* com perguntas também de alto nível. Ao ser questionado a respeito de quais necessidades ainda não estão supridas pelo SL/CA, Rafael foi rápido em citar os softwares de frente de caixa, automação comercial e outros dos quais as pequenas e médias empresas ainda dependem, e que atualmente não possuem exemplares livres. Peregrino aproveitou para nomear algumas formas de se de-



Figura 1 Como nas outras edições, o evento contou com a presença de um público altamente qualificado.

envolver software multiplataforma, através do uso de compiladores livres para as linguagens mais usadas em plataformas Windows®, e também com a adoção do *Java*, agora livre, que tende a aumentar.

Varejo

O primeiro case do evento foi apresentado por Marco Fragni, Gerente de Serviços de TI da rede varejista Ponto Frio (figura 3). Após corroborar as observações expostas por Rafael Peregrino minutos antes, afirmando que o fator decisivo na escolha do Linux no Ponto Frio não foi a ideologia ou o preço, Fragni relatou a história da segunda maior rede varejista do Brasil. Com 61 anos de existência e R\$ 3,8 bilhões de faturamento em 2006, os 3,2 milhões de clientes ativos da rede distribuem-se por todos os estados das regiões Sul, Sudeste e Centro-Oeste, à exceção do Mato Grosso do Sul.

Listados pelo gerente, os motivos para a adoção do Linux nos 400 servidores e mais de 8 mil estações

do parque de TI foram sua proteção contra vírus, estabilidade muito superior à solução proprietária anterior, portabilidade – o sistema é utilizado desde os PDAs até os mainframes – e flexibilidade.

A distribuição empregada para essa hercúlea tarefa foi o *Librix*, de fabricação do próprio parceiro de tecnologia do Ponto Frio, a Itautec. Na realidade, segundo relatou Fragni, o conceito de *single point of contact* foi fundamental nesse aspecto, pois uma mesma empresa é responsável pelo hardware e software.

Por enquanto, apenas as lojas com maior volume de vendas foram migradas, com ótima aceitação por parte dos usuários; o restante será migrado na segunda fase da operação, em 2008.

Games

Se a oferta de jogos sofisticados para Linux é limitada, o uso da plataforma livre no desenvolvimento desses softwares é ainda mais raro. A Hoplon, fabricante de jogos sediada em Florianópolis, SC, ousa desbravar esse terreno.

Como mostrou Tarquínio Teles (figura 4), presidente da empresa, o maior desafio enfrentado no desenvolvimento de seu primeiro game, o *Taikodom*, é a infraestrutura de TI.

Como ocorre com qualquer MMOG (*massively multimedia on-line game*), o *Taikodom* será acessado por centenas, talvez dezenas de milhares de usuários; ao mesmo tempo. Como a interatividade é a base do jogo, poder



Figura 3 Marco Fragni demonstrou os resultados e a motivação para a migração para Linux no Ponto Frio.

de processamento e latência são os principais aspectos da operação da infra-estrutura.

A solução ideal, segundo o presidente, foi utilizar SOA (arquitetura orientada a serviços), servindo o jogo através de máquinas virtuais Linux dentro de mainframes IBM, também rodando o sistema aberto.

“O desempenho sob demanda oferecido pela virtualização é fundamental”, disse o empolgado Tarquínio. “Por exemplo, um cinema superlotado representa redução dos lucros para seus donos, pois há espectadores potenciais que não conseguem comprar suas entradas. Com o *Taikodom*, temos que estar preparados tanto para um estrondoso sucesso, com grande presença do público, quanto para uma sala praticamente vazia. Esperar um público de tamanho pré-definido certamente representaria perda financeira.”

O executivo da Hoplon ainda discorreu brevemente sobre a capacidade de produção de softwares de qualidade internacional no Brasil. Segundo ele, um bom game requer quatro fatores (os quatro Cs): criatividade, computadores, competência técnica e capital. “Felizmente, temos os três primeiros no Brasil, e a Hoplon conseguiu o capital”, afirmou Tarquínio.

Os padrões abertos também foram uma importante escolha da empresa, pois evitam o aprisionamento ao fornecedor de software.



Figura 2 Rafael Peregrino apresentou em seu keynote os resultados da pesquisa da Linux New Media do Brasil em parceria com a Intel, a respeito do mercado brasileiro de SL/CA.



Figura 4 Tarquínio Teles discorreu sobre as vantagens de desenvolver jogos extremamente exigentes sobre plataformas abertas.

As excelentes ferramentas livres utilizadas na criação do Taikodom compõem mais um beneficiado pela Hoplon, no mais puro espírito colaborativo. As melhorias à *IDE Eclipse*, desenvolvidas pelos criadores do game para permitir a realização de praticamente qualquer tarefa relacionada ao jogo a partir da própria IDE, serão retornadas à comunidade, incrementando assim a qualidade do Eclipse. “Queremos que as universidades brasileiras disponham dessas tecnologias e facilidades”, afirmou Teles.

Governo

Após o almoço, o Serpro (Serviço Federal de Processamento de Dados) marcou a presença do Governo Federal no primeiro Linux Park de 2007. Em sua apresentação, Márcio Campos (**figura 5**) detalhou a relação e a história do órgão com o SL/CA.

Vinculado ao Ministério da Fazenda, o Serpro tem nove mil usuários distribuídos pelo Brasil. Por ser o responsável pela declaração on-line do imposto de renda no país, os computadores do órgão processam 3 bilhões de transações anuais, além de fornecer as soluções de TI e comunicações para a realização de políticas públicas.

O Linux começou a ser utilizado no Serpro em 1999, na unidade de Recife, PE, com a criação do Pro-

grama de Software Livre do Serpro (PSSL). Depois disso, o uso do sistema operacional de código-fonte aberto não parou de crescer, com a criação de um centro de especialização em SL/CA e a adoção do pingüim nas estações dos funcionários.

Nos servidores, o órgão emprega somente SL/CA, tanto como sistema operacional quanto nos serviços oferecidos, que abrangem desde a autenticação até mensagens instantâneas e backup.

Nessa área, há softwares de autoria do próprio Serpro que se destacam, como o *Babassu*, um cliente de mensagens instantâneas para LANs, o *Sagui*, gerenciador de atualização de estações, e a Estação Móvel de Acesso (EMA), um *liveCD* personalizado para cada usuário da rede do órgão.

“O uso do Linux reduziu nossos custos, aumentou nosso controle de mudança de versões e aumentou a inteligência dos funcionários”, relatou Campos. Como resultado, “o Serpro vai licenciar sob a GPL todas as ferramentas que construímos”.

Petróleo

Como não podia faltar numa série de seminários no estado responsável por mais de 70% da produção nacional de petróleo, a Petrobras também esteve presente ao evento, com Luiz Monnerat (**figura 6**) apresentando uma palestra sobre a computação de alto desempenho com clusters Linux na gigante nacional do petróleo.

Primeiramente, o engenheiro de sistemas explicou o uso de HPC (*high-performance computing*) na Petrobras, predominantemente para processamento sísmico e

geofísico, atividade da mais alta importância na exploração petrolífera praticada pela companhia.

Monnerat detalhou a história do envolvimento da empresa com o SL/CA, que, embora tenha sido atrasada pela reserva de mercado, conseguiu alcançar o patamar internacional já em 1997, quando foi desenvolvida, em parceria com a Unicamp, uma aplicação de simulação de reservatórios com emprego de 12 nós computacionais. “Em 2000, a Petrobras já se adiantava às tendências”, afirmou Luiz. “Desde o início dependemos de nossa equipe interna, movida por entusiasmo e criatividade – e tivemos sucesso”.

O interesse em clusters Beowulf de fato aumentou na empresa, com um cluster de 72 nós montado em 1999. “Já em 2004, 90% do processamento por HPC da Petrobras era realizado por Beowulfs”, afirmou Luiz.

No entanto, esse crescimento da HPC na empresa não foi sempre fácil. “Houve um momento em que nosso edifício atingiu seu limite de energia, e tivemos que alugar um CPD externo para nossos clusters”, descreveu o palestrante. “A solução usou processamento remoto, realizado pelas CPUs do CPD, enquanto os dados permaneciam no edifício original”. Em 2004, esse CPD abrigava o maior supercomputador do Brasil, com 1300 nós de processamen-



Figura 5 Márcio Campos anunciou que o Serpro vai lançar os softwares desenvolvidos internamente sob a licença livre GPL.

to, e hoje já possui 4600 CPUs e 9 TB de memória, rodando *Red Hat Enterprise Linux* e *CentOS*.

Painel sobre interoperabilidade

O final do evento foi marcado pelo memorável painel de interoperabilidade – executado pela primeira vez na história. Executivos dos mais importantes *players* do mercado nacional de SL/CA debateram sobre o assunto durante mais de uma hora (figura 7), respondendo primeiro às perguntas do moderador, Rafael Peregrino, e em seguida dando respostas às perguntas do público.

Respondendo à primeira pergunta, “O que a interoperabilidade representa para sua empresa?”, Cezar Taurion, Gerente de Novas Tecnologias Aplicadas da IBM, apontou as múltiplas formas de interoperabilidade, ressaltando a atuação da *big blue* nesse sentido.

A Itaútec foi representada por Isabel Lopes, Gerente de Análise e Suporte da empresa brasileira, e acrescentou que a demanda pela interoperabilidade vem do mercado, tornando-a essencial para a sobrevivência das empresas.

O Gerente de Estratégias de Mercado da Microsoft Brasil, Roberto Prado, enfatizou que o centro de

desenvolvimento de Código Aberto da empresa surgiu em resposta à demanda de seus clientes.

A Novell, segundo seu Consultor Sênior Ricardo Palandi, já se preocupa com interoperabilidade e padrões abertos desde o fim da década de 90, e ressurgiu no início do século atual graças às aquisições relacionadas ao SL/CA.

Por último, Alejandro Choclat, Country Manager da Red Hat Brasil, levantou uma importante questão: “Como podemos saber como será, no futuro, o uso dos dados gerados hoje?”. Segundo Choclat, a adoção de SL/CA e padrões abertos levará ao crescimento dos serviços em TI, o que é altamente positivo, na visão da Red Hat.

Posteriormente, cada um dos representantes respondeu a uma pergunta específica do moderador. Falando sobre o formato *ODF*, a IBM reforçou a ideia de que é importante utilizarmos um formato aberto para documentos, a fim de garantir sua compatibilidade com leitores no futuro. A Microsoft foi questionada a respeito do acordo com a Novell, respondendo que a parceria garantiu à empresa uma aproximação de clientes antes inatingíveis, por estarem “fechados com o Linux”, nas palavras de Prado, que também apontou que o *OpenXML* há de se tornar um padrão aberto após aprovação pela ISO.

A pergunta dirigida à Novell fazia menção à sua estratégia para virtualização, defendida pela companhia como vantajosa econômica, ambiental e tecnicamente. O acordo Novell-Microsoft também foi tema da pergunta à Red Hat, que afirmou que integrará todos os avanços provenientes deste.



Figura 7 Pela primeira vez, representantes dos principais *players* do mercado de SL/CA reuniram-se para debater sobre a interoperabilidade.

Por último, o ansioso público finalmente pôs suas perguntas aos presentes. Interpelada por Julio Cezar Neves, professor universitário e analista de suporte de sistemas da Dataprev, a representante da Itaútec afirmou que, como fornecedora de soluções proprietárias e livres, a empresa permite que o cliente defina a opção mais vantajosa para seu negócio. Em seguida, o executivo da Microsoft, ao ser questionado a respeito do uso futuro dos códigos abertos que sua empresa vier a disponibilizar, confirmou que a licença *Shared Source*, semelhante à *BSD*, será respeitada em sua totalidade.

Experiência

Ao término do evento, o público agraciou os palestrantes e organizadores com calorosos aplausos, reafirmando a aceitação e a importância do Linux Park para o cenário do SL/CA nacional.

Pode-se esperar, portanto, que a próxima edição do evento, dessa vez na capital mineira, tenha igual ou maior sucesso. ■

Mais Informações

- [1] Apresentação de Rafael Peregrino, incluindo pesquisa realizada pela Linux New Media do Brasil:
http://www.linuxpark.com.br/arquivos/LP07-1/Mercado_Linux_e_SL_no_Brasil.pdf



Figura 6 Luiz Monnerat demonstrou como a Petrobras se beneficia, desde 1997, de clusters Beowulf com Linux.

Ron Hovsepian, CEO da Novell

Cliente em foco

Meses após o polêmico acordo entre a Novell e a Microsoft, muitos ainda têm dúvidas quanto aos assuntos que este engloba. Ron Hovsepian está à frente das negociações, e pode explicar com clareza o que o acordo diz e não diz.

por Rafael Peregrino da Silva

Novell®

Linux Magazine» Embora muito já tenha sido dito a respeito do acordo entre a Novell e a Microsoft, muitas dúvidas ainda persistem. Você poderia explicar um pouco melhor como surgiu a idéia desse acordo?

Ron Hovsepian» No início de maio de 2006, telefonei para Kevin Turner, Chief Operating Officer da Microsoft e ex-CIO da rede Walmart, onde foi meu cliente. Falei sinceramente: “Kevin, acho que a Microsoft deveria pensar seriamente em comercializar o Linux”. Após o choque inicial, expliquei a ele o motivo dessa colocação, do ponto de vista do cliente, especialmente em relação à interoperabilidade, e ele compreendeu de verdade.

No dia seguinte, recebi um telefonema de Kevin, extremamente interessado em formular um acordo para que esses planos se concretizassem.

Então, tudo foi pensado tendo em vista o favorecimento do cliente.



Figura 1 Ron Hovsepian, CEO da Novell.

LM» Quanto às indenizações por patentes, o que exatamente o acordo pretende cobrir?

RH» Novamente o foco é o cliente. O acordo diz que, caso haja litígios legais quanto à violação de patentes de alguma das empresas pela outra, nenhum cliente será envolvido na disputa. As duas companhias ainda têm o direito de processar uma à outra por qualquer motivo que seja, porém os clientes de cada uma não serão envolvidos.

Esse não é um acordo de troca de licenças. Isso é o que eu mais desejo que os leitores compreendam. A Novell e a Microsoft não têm, e provavelmente jamais terão, um acordo de troca de patentes.

Acreditamos que envolver nossos clientes em questões judiciais faz mal à imagem de todas as empresas envolvidas na disputa. Um exemplo disso foi o que ocorreu à SCO, que saiu extremamente prejudicada de suas batalhas contra clientes e fornecedores.

LM» Atualmente, as patentes de software são uma das maiores ameaças ao Software Livre e de Código Aberto. Qual a posição da Novell a esse respeito?

RH» Há dois aspectos nessa discussão. O primeiro é a realidade de cada autoridade reguladora (governos, em última instância), com importantes diferenças entre os diversos países do globo. O segundo é o que nós, como empresa, estamos fazendo.

Nós afirmamos, logo após fechar o acordo, que usaríamos em nossa defesa as patentes que possuímos. Com o surgimento, logo em seguida, da Open Invention Network (OIN), nós inserimos nossas patentes nessa realidade, justamente com o objetivo de protegê-las.

O acordo com a Microsoft simplesmente cria mais uma proteção, dessa vez para o cliente. Portanto, é mais um motivo para o cliente não precisar se preocupar com questões de patentes.

Em parte, é por isso que a comunidade e o Linux não crescem mais rápido; as empresas e desenvolvedores envolvidos não conseguem por à parte suas diferenças e trabalhar para o bem comum. É muito mais fácil criar forks e dividir os desenvolvedores e usuários.

LM» Concorrentes da Novell, no Brasil, afirmaram que a empresa vendeu sua alma à Microsoft. Além disso, especula-se bastante que a Novell esteja apenas atuando como um “emissário” da Microsoft no mercado do SL/CA. Por último, fala-se que a Microsoft cogitou adquirir sua empresa. Você poderia esclarecer essas questões?

RH» A aquisição pela Microsoft é completamente especulativa. Não posso garantir que seja impossível, pois ambas são empresas de capital aberto, com seus próprios conselhos diretores e estruturas administrativas. Mas posso dizer que acho muito improvável.

Quanto a vender a alma, volto a afirmar que busco representar os clientes.

Meus clientes desejam uma melhor interoperabilidade, e querem ter apenas uma empresa à qual recorrer para o fornecimento e suporte tanto ao Windows quanto ao Linux. O acordo é a manifestação disso. Nós não vamos vender nossas almas a ninguém.

LM» *A Microsoft não agiu sempre de forma ética para eliminar a concorrência, e a própria Novell já foi prejudicada por isso. Isso não indicaria algum tipo de risco em acompanhar a empresa nesse tipo de acordo?*

RH» A Microsoft vai competir honestamente em qualquer mercado. Portanto, eu enxergo essa questão como: “é possível ter uma relação com uma empresa tão competitiva?”, e acho que a resposta é “sim”.

Creio que o desejo da Microsoft de entrar no mercado de Linux é pequeno, se é que existe. Porém, o que a motiva é aumentar sua presença frente ao cliente. Então, se ela puder unir-se a nós em favor do cliente, sua estratégia pode ficar melhor fundamentada. Além disso, outra consequência é a melhora da percepção da empresa por parte dos clientes.

LM» *Aparentemente, a GPLv3, ainda em formulação, incluirá cláusulas que impedem a distribuição de seus softwares mediante acordos como o da Novell com a Microsoft. Como a Novell pretende abordar essa limitação, especialmente em relação ao Samba, que provavelmente a adotará?*

RH» Estamos obviamente bastante atentos a isso. Temos participado no Comitê B da formulação da GPLv3. Estamos aguardando versões públicas dos outros comitês, para decidirmos como agir. Claro que há algumas opções técnicas e de negócios das quais podemos lançar mão. O que podemos garantir é que a Novell permanecerá profundamente comprometida com o Linux e seu mercado.

LM» *Steve Ballmer, da Microsoft, afirmou que a empresa está disposta a*

fazer com outras companhias acordos semelhantes ao que fez com a Novell. Entretanto, a Novell vinha tratando o acordo, ao menos no início, como algo exclusivo. Houve erros de interpretação por alguma das partes?

RH» De minha parte, não vejo qualquer problema em acordos que envolvessem afastar os clientes dos processos por violação de patentes. Realmente não me importo se a Microsoft quiser fazer acordos semelhantes com nossos concorrentes, ou até mesmo outros acordos, de troca de licenças, por exemplo.

No caso da Novell, especificamente, nós possuímos um grande arsenal de patentes de alta importância, o que dá um tom diferente às negociações com a Microsoft. No entanto, nós jamais usaríamos essas patentes contra nossos clientes, embora possamos usá-las como mecanismo de defesa contra outras empresas.

Na realidade, nós discordamos da Microsoft quanto à proteção de direitos de propriedade intelectual, e já informamos a eles que não faremos qualquer tipo de reconhecimento de infração de patentes no Linux.

LM» *Como seus clientes mais importantes reagiram ao acordo? E os novos clientes?*

RH» Evidentemente estou muito feliz em ver a Novell adquirir novos clientes, que encararam o acordo como uma ótima notícia. Como você pôde ver há pouco, eles estão muito satisfeitos com o fato de nós assumirmos a função de buscar a interoperabilidade, em vez de eles próprios terem de se preocupar com isso. Em troca, eles já fizeram pedidos de inclusão de recursos de interoperabilidade, que no momento somam vinte itens. Essa proximidade com nossos clientes é extremamente bem vinda.

A própria Microsoft, na minha visão, tem agido corretamente, ouvindo os pedidos de seus clientes e aproximando-se deles. Sua conversa conosco é totalmente franca. Por exemplo, quando eles propuseram, há pouco, um acordo de patentes, nós educadamente negamos, pois isso não é estrategicamente favorável a nós. E esse fato não perturbou nosso relacionamento.

LM» *O acordo possui cinco pilares, bem definidos, de colaboração entre as duas companhias. Em cada um deles, quais partes já estão em andamento?*

RH» Temos que pensar como se fossem três acordos diferentes. Primeiramente, um acordo na área de negócios, que engloba a participação

A Novell e a Microsoft não têm, e provavelmente jamais terão, um acordo de troca de patentes.

da Microsoft, com várias dezenas de milhões de dólares e um esforço de vendas dedicado ao acordo (em Redmond), além dos US\$ 240 milhões em cupons de serviços Novell que eles adquiriram e vêm distribuindo.

O segundo trata da cooperação técnica, passando por virtualização e ODF. Já publicamos nosso planejamento nessa parte do acordo, e estamos nos primeiros estágios da colaboração. Construímos um tradutor do formato OpenXML para o OpenOffice.org, e vamos continuar avançando nesse campo. No tocante à virtualização, temos que esperar o Vista estabelecer-se e amadurecer para que possamos interagir com ele de forma sólida.

A terceira nuance do acordo é a que trata das patentes, e creio que já falei demais sobre ela. (risos). ■

Simon Phipps, Chief Open Source Officer da Sun Microsystems

Abrindo e aprendendo

Veja o novo posicionamento da Sun no mercado do Software Livre e de Código Aberto.

por Pablo Hess



Linux Magazine» Como a Sun se envolveu com o Software Livre e de Código Aberto?

Simon Phipps» Desde 1982, quando a Sun era a *startup* de Código Aberto do momento, utilizamos o BSD Unix como base para nosso negócio – *workstations* –, mas acrescentamos muitos componentes proprietários nele. Apenas em 2005, quando a Sun lançou o OpenSolaris, voltamos a ter um kernel livre.

Em relação à diferença entre esses termos, para mim, o Software Livre é a base que os desenvolvedores usam para criar softwares que os fazem sentirem-se no controle. E esse software precisa ser licenciado de forma a permitir que eles tenham direito de desenvolvê-lo, e necessita também de regras que facilitem a contribuição por parte dos desenvolvedores. Esse conjunto de regras a respeito da licença e da contribuição é o que eu entendo por Código Aberto, que por sua vez é como os desenvolvedores inteligentes usam o Software Livre.



Figura 1 Simon Phipps, Chief Open Source Officer da Sun Microsystems.

Por esses motivos, creio que é um erro lutar para separar os dois termos.

LM» Qual é o envolvimento da Sun com as distribuições do OpenSolaris?

SP» Temos nossa própria distribuição (*Solaris Express*), feita a partir das mesmas ferramentas abertas que os outros grupos usam. No entanto, achamos melhor não interferir na forma como a comunidade de usuários faz uso das ferramentas que disponibilizamos.

LM» Como a Sun se relaciona com sua comunidade de usuários?

SP» Para responder a essa pergunta, é necessário deixar claro que não existe uma comunidade única de usuários, pois cada um de nossos produtos tem sua própria comunidade. Isso se reflete na forma como lidamos com cada uma delas, incluindo as licenças e regras adotadas para seus respectivos softwares.

LM» Quais são as maiores dificuldades enfrentadas por vocês na abertura de códigos?

SP» Como não existe experiência a esse respeito na indústria, temos que assegurar a qualidade de nosso software, ao mesmo tempo em que garantimos as vantagens e oportunidades que o Código Aberto oferece.

Talvez não pareça, mas é bem complicado (senão impossível) percorrer esse caminho todo sem cometer erros. Então, nós acabamos por avançar um tanto e recuar um pouco, tentando sempre assegurar a qualidade e a liberdade do código.

E quero que os leitores tenham em mente que nós sabemos que vamos errar, mas vamos sempre corrigir nossos erros da melhor forma possível.

LM» A CDDL foi lançada após a GPLv2. Por que houve esse esforço de criação de mais uma licença livre?

SP» Costumo caracterizar nossa licença CDDL como a *Mozilla Public License* (MPL) com falhas corrigidas. Ela não é uma nova licença maligna que faz as pessoas cederem direitos que não desejam, nem tampouco é exclusiva da Sun. A CDDL é uma licença de uso geral, que eu sugiro que se use no lugar da MPL.

Antes de criarmos a CDDL, buscamos os motivos da intensa proliferação de licenças livres, e descobrimos que isso ocorre devido a falhas não intencionais na MPL. Quando advogados corporativos encontram uma dessas falhas, afirmam que é necessário corrigi-la. Porém, recorrentemente, a falha é corrigida apenas para sua própria empresa. Por isso, tivemos o cuidado de corrigir todas essas falhas da MPL para qualquer desenvolvedor ou usuário.

LM» Qual a relação da Sun com o kernel Linux?

SP» Nós sabemos que o Linux roda muito bem em nosso hardware, e muitas vezes ele é o mais apropriado no contexto do usuário.

Separar nossas comunidades é estupidéz, pois temos mais semelhanças do que diferenças. Sabemos que usuários de tecnologia tendem a tornar-se apaixonados pelo que usam, mas isso jamais deve ser transformado em raiva. ■

Xandros contrata no Brasil

A Xandros, Inc. é um fornecedor global de soluções baseadas em Linux com sede em Nova York. A empresa está fortalecendo a sua presença no Brasil e na América Latina com objetivo de melhor atender às demandas do mercado local. Oferece oportunidade para profissionais qualificados com base em São Paulo.

Sales System Engineer Brazil / Latin America

Requisitos:

- Profundo conhecimento em Linux (Debian)
- Experiência com infraestrutura de servidores, desktops e thin clients
- Experiência de no mínimo 2 anos em atendimento ao cliente
- Conhecimento avançado de inglês (conversação e escrita)
- Domínio da língua portuguesa (conversação e escrita)
- Conhecimento de espanhol desejável
- Capacidade de trabalhar sob pressão
- Bom relacionamento interpessoal
- Disponibilidade para viagens
- Automóvel próprio
- Iniciativa

Enviar currículo com pretensão salarial para James D. Largotta:
jamesl@xandros.com / +1-646-747-7648

www.xandros.com

Código Aberto na idade da razão

Cezar Taurion

Nas últimas semanas participei de alguns grandes eventos de Linux e Código Aberto, como o Linux Park e FISL 8.0. E percebi que está cada vez mais latente o amadurecimento da comunidade de Código Aberto. Mesmo no FISL, onde antes havia muito conteúdo ideológico e emotividade, hoje a maioria das discussões e apresentações já são muito pragmáticas. Todos saem ganhando com isso.

A maturidade do movimento de Código Aberto pode ser simbolizada pelo crescimento e maturidade do Linux, que começou sem maiores pretensões. O email de Linus Torvalds, em 25 de agosto de 1991, dizia que seu sistema operacional era apenas um hobby, e não se tornaria nada profissional.

A cada dia diminui o número de críticos que acham que Código Aberto não é sério.

Hoje, Código Aberto é uma realidade. Diversos softwares, como o próprio Linux, *Apache*, *Firefox*, *Eclipse*, *JBoss*, *PostgreSQL*, *MySQL*, *Sendmail* e *PHP*, para citar alguns, já fazem parte do portfólio de software de muitas empresas.

O movimento de Código Aberto tem em seu contexto a inovação do processo de desenvolvimento. Existe uma frase emblemática de Eric Raymond, em seu livro *The Cathedral and the Bazaar*, que diz: “acredito que o golpe mais inteligente e de maior relevância do Linux não foi a construção do próprio kernel Linux, mas a invenção do seu modelo de desenvolvimento”. Este novo modelo de desenvolvimento colaborativo permitiu criar diversos novos e inovadores modelos de negócio que estão afetando e vão afetar ainda mais a indústria de software.

A cada dia diminui o número de críticos que acham que Código Aberto não é sério. Alguns mitos dos seus tempos pioneiros e românticos começam a ser eliminados. Quando começamos a debater Código Aberto com mais intensidade, por volta de 2000 ou 2001, havia quase um consenso de que os desenvolvedores que atu-

avam nos projetos de Código Aberto eram 100% voluntários, o processo de desenvolvimento era anárquico e sem um *road map* claro e nenhuma preocupação com datas para entrega. Havia também a percepção de que os fundamentos econômicos do Código Aberto eram intangíveis, a chamada *gift economy*.

Hoje, sabe-se que nos projetos de maior sucesso, cerca de 90% dos desenvolvedores mais ativos estão na folha de pagamento da própria indústria de software. Também existe uma organização clara, com *road map* definido (os exemplos da Linux Foundation, Eclipse Foundation e Apache Software Foundation são prova disso) e está claro que existem, sim, modelos de negócio que podem ser construídos em cima do contexto de Código Aberto.

A sinergia entre a indústria e a comunidade é positiva para todo mundo. Uma pesquisa, ainda em rascunho, em elaboração por pesquisadores da Universidade de Pisa, na Itália, tem gerado dados muito interessantes. Até o momento, ela está demonstrando que a sinergia indústria-comunidade é altamente positiva. Os projetos que têm apoio da indústria têm, em média, 19 desenvolvedores ativos, contra cinco dos demais projetos. Também apresentam maior atividade e demonstram um viés mais focado na tecnologia *Java* que na família C (C e C++). A pesquisa também mostra um maior pragmatismo quanto à escolha das opções de licenciamento: em 45% dos projetos em que empresas de software participam ativamente, a licença GPL é a escolhida, contra quase 75% quando o projeto é conduzido apenas pela comunidade. As outras licenças mais usadas são basicamente a BSD, Mozilla Public License e a Apache License.

A conclusão a que podemos chegar é que está ocorrendo um maior amadurecimento da comunidade, com conseqüente maior evolução e aperfeiçoamento do modelo de Código Aberto. Acredito que estamos no caminho certo. ■

O autor

Cezar Taurion é gerente de novas tecnologias aplicadas da IBM Brasil. Seu blog está disponível em <http://www-03.ibm.com/developerworks/blogs/page/ctaurion>.



Vigiando os fios

Mantenha-se à frente dos problemas de rede com a versátil ferramenta de monitoramento Nagios.

por Joe Casad e Pablo Hess

CAPA

Se você é responsável por mais de uns poucos PCs, provavelmente já percebeu que seria interessante monitorar o estado da sua rede automaticamente. Você inclusive já deve ter implementado um sistema como esse. Os administradores profissionais já possuem suas próprias ferramentas de monitoramento preferidas, e os usuários domésticos não precisam se preocupar com isso. Então, por que dedicar uma matéria de capa ao Nagios?

O mundo de TI já está cheio de ferramentas comerciais de monitoramento. Na verdade, grande parte do pavilhão de exposições durante a Linux World é dedicado a ferramentas como essas, que monitoram e gerenciam recursos de rede. Muitas delas são bastante eficientes, e não desencorajamos ninguém de usar uma solução comercial, caso ela seja a ferramenta certa para o trabalho.

Entretanto, é possível ir bem longe com o Linux usando produtos livres e gratuitos, e o Nagios é um exemplo de ferramenta extremamente eficiente que não exige pagamento. Se você estiver pensando em adquirir uma solução comercial, você precisa saber quais são as alternativas livres. Visitando os estandes na LinuxWorld, você encontrará inúmeros folhetos, *white papers* e documentos técnicos a respeito de soluções comerciais de monitoramento. Por isso, estamos oferecendo uma contrapartida igualmente técnica a respeito do Nagios.

Se você acredita que não possui qualquer necessidade de usar o Nagios porque só usa o Linux em casa, é melhor pensar novamente. Como mostra nosso especialista em Perl Michael Schilli, na seção de programação, é possível usar o Nagios em uma escala menor, com scripts caseiros para verificar temperaturas e enviar alertas com informações de status.

Incluimos também o *GroundWork*, um aplicativo GPL comercial que facilita a configuração do Nagios e oferece uma interface mais organizada para o usuário.

Na seção de programação, nosso ás do Perl Michael Schilli mostra como criar seus próprios plugins para o Nagios.

Continue lendo e desbrave os detalhes do fabuloso Nagios. ■

Índice

O verdadeiro grande irmão p.32

Trabalho de base p.40

Vigilância de sistemas

O verdadeiro grande irmão

O versátil Nagios monitora sua rede através de plugins, e emite alertas antes que haja problemas com máquinas e serviços. Aprenda em profundidade como instalar, usar e gerenciar esse ícone do monitoramento de redes.

por Julian Hein

Algumas soluções avançadas de monitoramento de redes são vendidas por milhares de reais, e valem o investimento caso sejam capazes de manter a rede de uma empresa funcionando sem interrupções. Porém, se o objetivo for uma ferramenta versátil e confiável que informe o administrador sobre eventos na rede, sem no entanto estourar o orçamento, a ferramenta livre de monitoramento **Nagios** pode ser a solução.

De acordo com o site do Nagios, a proposta desse programa é “...informar ao administrador os problemas de rede antes que seus clientes,

usuários finais ou chefes o façam”. O programa monitora as máquinas da rede, verificando sintomas de possíveis problemas. Pode-se usá-lo para monitorar serviços de rede, recursos das máquinas (como carga do processador e espaço disponível em disco) e fatores ambientais, como a temperatura na sala dos servidores.

O Nagios é facilmente extensível – pode-se fazê-lo monitorar quase todos os problemas de rede potenciais. É possível exibir sua saída em um gráfico ou numa tabela HTML. Até mesmo alertas podem ser enviados através dele, caso apareça algum problema.

O Nagios não é exatamente uma solução de monitoramento completa, mas sim um *daemon* que gerencia o processo de monitoramento (figura 1). A configuração do programa define as máquinas e serviços que ele deve monitorar, e programas pequenos e independentes, conhecidos como *plugins*, obtêm e retornam as informações de status. Vários plugins pré-definidos estão disponíveis no site, e também é possível criar os seus próprios.

As máquinas e serviços monitorados pelo Nagios são todos definidos através dos arquivos de configuração do software. Esses arquivos contêm ainda configurações do daemon do programa propriamente dito, assim como informações sobre os contatos que receberão os alertas dele.

Instalação

No momento da redação deste artigo, a versão estável ideal para redes pequenas e médias mais atual do Nagios era a 2.7. Já para monitorar grandes redes, com 300 ou 400 máquinas, pode ser mais interessante experimentar a próxima versão, 3.0, que promete grandes avanços em desempenho, principalmente em ambientes avantajados.

É possível baixar o Nagios a partir da página do projeto [1]. No entanto, muitas distribuições Linux, como *Debian* [2], *Fedora*, *Red Hat Enterprise* e *Gentoo* incluem uma versão do programa, e pode-se baixar os pacotes do Suse a partir dos populares *mirrors* FTP. Muitos usuários acham mais fácil compilar o progra-

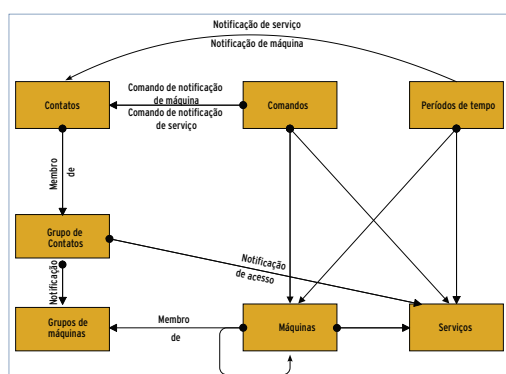


Figura 1 Os arquivos de configuração do Nagios freqüentemente referem-se a outros arquivos de configuração.

ma a partir do código-fonte, pois isso permite uma instalação mais rápida de *patches* de segurança.

Para compilar seu próprio Nagios, é necessário instalar os pacotes *apache*, *apache2*, *libgd*, *libjpeg-devel* e *openssl-devel*, incluindo suas dependências. Os comandos a seguir preparam o servidor para a instalação:

```
#useradd nagios
#groupadd nagios
#mkdir /usr/local/nagios
#chown nagios:nagios
#/usr/local/nagios
#useradd nagcmd
#groupmod -A nagcmd www-data
#groupmod -A nagcmd nagios
```

A etapa a seguir descompacta e instala o código-fonte:

```
#tar zxvf nagios-2.7.tar.gz
#cd nagios-2.7
#./configure --with-command-
#group=www-data
#make all
```

O comando `./configure -help` mostra um panorama dos parâmetros disponíveis para a compilação. Após terminá-la, pode-se instalar o aplicativo digitando-se `make install`. Outros comandos `make` instalam um script de inicialização, um exemplo de configuração e um *pipe* para comunicação entre as interfaces web e o daemon:

```
#make install-init
#make install-config
#make install-commandmode
```

O pacote do Nagios propriamente dito não contém plugins, sendo necessário instalá-los separadamente. É possível baixá-los a partir do site [1]. A versão 1.4.6 dos plugins é a atual. Entretanto, vários plugins não poderão ser compilados, a menos que sejam especificados determinados arquivos de cabeçalho ou bibliotecas clientes instaladas no sistema. Além disso, alguns plugins só estão disponíveis como scripts *Perl*, ou estão

Exemplo 1: Configuração do objeto Timeperiod

```
01 define timeperiod {
02     timeperiod_name nonworkhours
03     alias outside working hours
04     monday 00:00-09:00,17:00-24:00
05     tuesday 00:00-09:00,17:00-24:00
06     wednesday 00:00-09:00,17:00-24:00
07     thursday 00:00-09:00,17:00-24:00
08     friday 00:00-09:00,17:00-24:00
09     saturday 00:00-24:00
10     sunday 00:00-24:00
11 }
```

localizados no subdiretório `contrib` do pacote do plugin. Será necessário copiar esse tipo de plugin para `/usr/local/nagios/libexec`.

Configuração

O arquivo central de configuração, `/usr/local/nagios/etc/nagios.conf`, contém configurações globais do daemon do programa. Um arquivo de configuração de exemplo é gerado automaticamente quando se compila os binários. Quando se utiliza uma versão empacotada do software, ou quando a versão foi pré-instalada no sistema, o arquivo de configuração deve estar localizado nos diretórios do Nagios (veja a seção *Arquivos de configuração*, mais adiante, para mais informações sobre arquivos de exemplo). O arquivo de configuração contém mais opções de configuração do que este artigo pode

cobrir. A documentação completa do arquivo de configuração está disponível em [3].

Uma das configurações mais importantes nesse arquivo de configurações globais é uma referência ao(s) arquivo(s) de definição de objetos que será usado pelo programa:

```
cfg_file = nome_do_arquivo
```

O arquivo de definição de objetos contém a maioria das informações específicas que descrevem as máquinas e serviços a serem monitorados. Dependendo do tamanho e da complexidade da rede em questão, pode ser interessante espalhar essas informações de objetos ao longo de diversos arquivos.

Nesse caso, é possível usar a diretiva de configuração `cfg_file` múltiplas vezes, ou aplicar a diretiva `cfg_dir`

Quadro 1: Objetos do Nagios

O Nagios necessita de ao menos uma entrada de configuração para os seguintes objetos:

- ▶ **Timeperiods**: períodos de tempo para monitoramento e notificação;
- ▶ **Commands**: checagens de monitoração e notificação;
- ▶ **Contacts**: contatos e emails;
- ▶ **Contactgroups**: grupos de contatos;
- ▶ **Hosts**: dispositivos e suas configurações;
- ▶ **Hostgroups**: grupos de hosts;
- ▶ **Services**: configuração de serviços de monitoramento.

Os seguintes objetos não são estritamente necessários, mas são oferecidos como opções de configuração estendidas:

- ▶ **Servicegroups**: grupos de serviços monitorados;
- ▶ **Dependencies**: definição de dependências entre máquinas ou serviços;
- ▶ **Escalations**: regras de escalção para notificações;
- ▶ **ExtendedInformation**: configurações estendidas para a interface web.

Exemplo 2: Definição de comando

```
01 define command {
02     command_name check_smtp
03     command_line $USER1$/check_smtp -H $HOSTADDRESS$ -p $ARG1$ -w
    ➔ $ARG2$ -c $ARG3$
04 }
```

Exemplo 3: Contatos no Nagios

```
01 define contact {
02     contact_name jdoe
03     alias Jon Doe
04     service_notification_period nonworkhours
05     host_notification_period nonworkhours
06     service_notification_options w,u,c,r
07     host_notification_options d,u,r
08     service_notification_commands notify-by-email
09     host_notification_commands host-notify-by-email
10     email jdoe@example.com
11 }
```

Exemplo 4: Definição de Host

```
01 define host {
02     host_name linux1
03     alias Linux Server 1
04     address 192.168.1.254
05     parents main-switch
06     check_command check-host-alive
07     max_check_attempts 5
08     check_period always
09     contact_groups linux-admins
10     notification_interval 30
11     notification_period always
12     notification_options d,u,r
13 }
```

Exemplo 5: Configuração de checagem de serviço

```
01 define service {
02     service_description smtp check
03     host_name linux1
04     check_command check_smtp!25!10!20
05     max_check_attempts 3
06     normal_check_interval 5
07     retry_check_interval 1
08     check_period always
09     notification_interval 30
10     notification_period always
11     notification_options w,c,r
12     contact_groups linux-admins
13 }
```

para especificar um diretório com os arquivos de definição de objetos:

```
cfg_dir = nome_do_diretorio
```

Essencialmente, um objeto do Nagios é qualquer elemento que o programa precise conhecer, como um serviço que deva ser monitorado, um comando a ser executado, uma máquina em operação na rede ou um

contato selecionado para receber notificações em caso de emergências.

O **quadro 1** lista alguns dos possíveis objetos no arquivo de definição de objetos. O site oferece uma descrição completa de objetos pré-definidos[4]. A seguir estão descritos alguns dos mais importantes.

As configurações de *Timeperiod* (período de tempo) definem quando monitorar ou notificar. O objeto *Ti-*

meperiod mostra as informações de período de tempo (**exemplo 1**).

A propriedade mais importante associada a ele é *timeperiod_name*, que é consultada por várias outras funções de configuração do Nagios. A interface web utiliza o apelido estendido (*extended alias name*). Valores de tempo individuais sempre referem-se a um dia da semana.

É preferível usar um arquivo de configuração separado para períodos de tempo, como `/usr/local/nagios/etc/objects/timeperiods.cfg`. Inicialmente, serão necessárias três definições das situações mais comuns, como por exemplo, *always*, *workhours* e *nonworkhours*.

O Nagios refere-se a qualquer tipo de definição combinada que chame um programa ou script de shell como um *comando*. No **exemplo 2**, o objeto de comando manda-o chamar o plugin `check_smtp` com parâmetros específicos. `$HOSTADDRESS$` refere-se a uma macro que recebe os dados apropriados ao ser chamada. O parâmetro de plugin `-p` significa o número da porta SMTP, e `-w` e `-c` introduzem os limites *WARNING* e *CRITICAL*.

A informação passada para o plugin depende de qual esteja sendo usado. O monitoramento HTTP exige parâmetros como o nome do servidor, caminho, nome do usuário e senha, enquanto uma verificação por *ping* apenas requer um endereço IP. A forma mais fácil de descobrir quais parâmetros são necessários para um plugin do Nagios é executar o plugin com o parâmetro `--help`.

O programa define as pessoas e endereços de contato com o objeto *Contacts* (veja o **exemplo 3**). Os contatos são usados principalmente em caso de problemas, mas também são utilizados para atribuir privilégios de acesso à interface web.

Quadro 2: Monitoramento de servidores Windows com o Nagios

Obviamente o Nagios oferece várias soluções para monitorar servidores Windows. Além do *NRPE*, que possui uma versão para Windows, o *NsClient* faz referência ao nome *NetSaint*, que era como o Nagios se chamava até 2001. O *NsClient++* é um sucessor que combina as funcionalidades das duas alternativas em um único agente.

A instalação é extremamente simples: após descompactar o arquivo ZIP, só é necessário copiar os arquivos para um local adequado no servidor Windows, como *C:\Arquivos de Programas\NsClient*, e modificar as configurações presentes em *@NSC.ini* para refletirem as exigências locais. Em particular, é necessário ativar os módulos individuais no início do arquivo de configuração. Feito isso, o administrador do Windows precisa reiniciar o serviço através do *Iniciar | Executar*, digitando *C:\Arquivos de Programas\NsClient++ /install* e, em seguida, *net start nsclient++*.

Como o agente contém ambos seus antecessores, é possível utilizar qualquer um dos dois plugins no servidor Nagios, ou seja, *check_nt* ou *check_nrpe*. O primeiro possui valores para os parâmetros *CLIENTVERSION*, *CPULOAD*, *UPTIME*, *MEM-USE*, *USEDISKSPACE*, *SERVICE-STATE* e *PROCSTATE*, além de todos os contadores *PerfMon* do Windows. Uma chamada para consultar o status de um serviço do Windows é assim:

```
./check_nt -H <endereço_da_máquina> -p <porta> -s <senha> -v SERVICESTATE -l <serviço>
```

A forma mais fácil de se descobrir o nome dos serviços consultados no Windows é através das propriedades do gerenciador de serviços do Windows, que fica em *Iniciar | Administração | Serviços*. Enquanto a maioria dos outros parâmetros é auto-explicativa, os contadores de performance, ou *performance counters*, precisam de alguma explicação. O monitor de desempenho do Windows é uma interface central para valores de desempenho. Os administradores podem usá-lo tanto para consultar dados internos de desempenho do Windows quanto para dados de várias outras aplicações do servidor, como o *Exchange Server* ou o *SQL Server*. Para isso, a sintaxe é:

```
#./check_nt -H <endereço_da_máquina> -p <porta> -v COUNTER -l "\\Performanceobject(Instance)\\Indicador"
```

O valor de retorno pode ser reformatado para a saída no plugin.

O **exemplo 3** é o primeiro relacionado a um objeto definido com outro objeto: por exemplo, *nonworkhours* é definido no objeto *Timeperiods* (**exemplo 1**). *notify-by-email* e *host-notify-by-email* representam comandos que o Nagios utiliza para passar mensagens.

Para evitar a necessidade de listar grandes números de contatos

individuais, pode-se acrescentar os contatos aos grupos:

```
define contactgroup {
    contactgroup_name linux-admins
    alias Linux administrators
    members jdoe,mtestmann,wadmin
}
```

Qualquer dispositivo que deva ser monitorado precisa ser definido como uma máquina (**exemplo 4**).

As propriedades mais importantes de uma máquina são seu nome e endereço IP. A variável *max_check_attempts* define com que frequência se deve repetir uma verificação antes de o Nagios considerar uma falha e notificar o administrador. Enquanto isso, *contact_groups* especifica grupos a notificar em caso de falha. Nosso exemplo utiliza um grupo de contato que configuramos antes. Máquinas individuais podem ser coletadas em grupos arbitrários de máquinas para um gerenciamento facilitado:

```
define hostgroup {
    hostgroup_name linux-servers
    alias Linux Server
    members linux1,linux2,tux,webserver,mybox
}
```

Assim que tiverem sido definidas as configurações de tempo, máquinas e contatos, já será possível definir os serviços. Uma definição de serviços especifica os recursos a serem monitorados. É aí que tudo que especificamos começa a se unir (**exemplo 5**).

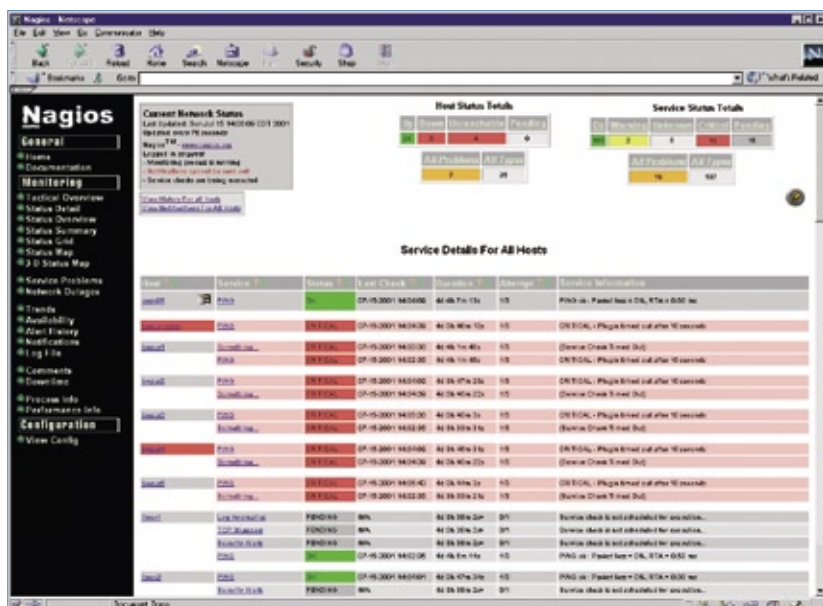


Figura 2 O Nagios fornece resumos detalhados das informações de status.

Exemplo 6: Configuração da interface web do Nagios

```
01 ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
02
03 <Directory "/usr/local/nagios/sbin">
04     Options ExecCGI
05     AllowOverride None
06     Order allow,deny
07     Allow from all
08     AuthName "Nagios Access"
09     AuthType Basic
10     AuthUserFile /usr/local/nagios/etc/htpasswd.users
11     Require valid-user
12 </Directory>
13
14 Alias /nagios /usr/local/nagios/share
15
16 <Directory "/usr/local/nagios/share">
17     Options None
18     AllowOverride None
19     Order allow,deny
20     Allow from all
21     AuthName "Nagios Access"
22     AuthType Basic
23     AuthUserFile /usr/local/nagios/etc/htpasswd.users
24     Require valid-user
25 </Directory>
```

O exemplo 5 também demonstra como passar parâmetros para um comando de verificação. É importante notar que os parâmetros ficam separados por `!`. Isso passa os valores para as macros `$ARG1$`, `$ARG2$` e assim por diante, que em seguida são passados para o plugin.

Em operações normais, faz sentido distribuir a configuração do Nagios através de múltiplos arquivos individuais e, dependendo dos requisitos do projeto, organizar os arquivos em vários subdiretórios. Por enquanto, provavelmente um arquivo único deve ser suficiente. As fontes do Nagios incluem um arquivo chamado `localhost.cfg` ou `minimal.cfg`, que é perfeito para seus primeiros passos.

Após criar ou modificar os arquivos de configuração do programa, é possível realizar uma verificação da configuração. A opção `-v` o faz verificar a configuração completa para erros de sintaxe e, sobretudo, certificar-se de que as referências a outros objetos possam ser resolvidas da forma cor-

reta. Como argumento, o Nagios espera apenas o nome do arquivo de configuração principal:

```
/usr/local/nagios/bin/nagios -v
➔ /usr/local/nagios/etc/nagios.cfg
```

Em caso de sucesso, a verificação da configuração exibe uma mensagem: *Things look okay. No serious problems were detected during the pre-flight check.*

Iniciando o daemon

É possível iniciar o daemon com o seguinte comando: `/etc/init.d/nagios start`. Se o daemon já estiver rodando, pode-se simplesmente mandá-lo recarregar-se, para que ele utilize a nova configuração `/etc/init.d/nagios reload`.

Presumindo que o Nagios não exiba mensagens de erro, agora o daemon foi iniciado para monitorar as máquinas e serviços que foram configurados. Para descobrir quais etapas o programa está realizando no momento, pode-se verificar o arquivo de log `tail -f /usr/local/nagios/var/nagios.log`.

Interface web

Em controles normais e, acima de tudo, para verificar o status atual de todos os servidores monitorados, o Nagios traz uma interface web (figuras 2 e 3) integrada, que deve ser integrada à instalação local do Apache. Se o Apache estiver sendo utilizado, a melhor forma é criar um arquivo chamado `/etc/apache2/conf.d/nagios` com as entradas mostradas no exemplo 6.

Para permitir que os usuários entrem na interface web do programa, é necessário definir entradas de conta em `htpasswd.users`. Se esse arquivo não existir, será necessário criá-lo utilizando o `htpasswd`:

```
touch /usr/local/nagios/etc/
➔ htpasswd.users
htpasswd /usr/local/nagios/etc/
➔ htpasswd.users jdoe
```

Os nomes de usuários precisam estar de acordo com os contatos criados anteriormente, para que a interface web possa identificar os usuários corretos e mostrar-lhes apenas as máquinas atribuídas a eles. O arquivo `cgi.cfg` lida com outras funções da interface web e configurações de privilégio.

Plugins

Um plugin do Nagios é essencialmente um pequeno utilitário que obtém informações do sistema. Como mencionado antes, há toda uma coleção de plugins disponíveis para download no site. Num site do *SourceForge* dedicado ao desenvolvimento de novos plugins[5], existem links para plugins de terceiros e informações sobre a criação de seus próprios plugins.

Como os plugins são programas independentes, pode-se simplesmente rodar um plugin na linha de comando para testá-lo. É bom trabalhar sob a conta de usuário

do servidor do Nagios, já que será ela a executar os plugins. A linha de comando é diferente para cada plugin, como cada tipo de verificação pode demandar parâmetros diferentes. Dito isso, todos os plugins devem possuir uma opção `-h` ou `--help` implementada. Chamar a ajuda oferece um breve resumo das várias opções.

Considerando o plugin `check_disk`:

```
nagios# ./check_disk -w 50% -c
➔20% -p /$$
```

```
DISK OK - free space: / 45256 MB
➔(64% inode=98%); | /=25137MB;37080
➔;59328;0;74160
```

Os plugins fornecem um valor de código de retorno que não fica diretamente visível por padrão. Pode-se mostrar o código de retorno digitando-se `echo $?`. Os códigos de retorno numéricos representam os seguintes resultados: 0 para OK, 1 para WARNING, 2 para CRITICAL e 3 para UNKNOWN.

A segunda parte da saída do plugin são os resultados visíveis exibidos na interface web. Vários plugins traduzem o valor de retorno para uma mensagem clara, como a `DISK OK` mostrada acima. Entretanto, não se deve confiar cegamente nisso – em caso de dúvida, é importante verificar o código de retorno.

A terceira parte dos resultados fica separada do resto por um pipe (`|`). O Nagios chama essa seção de “dados de performance”. Os plugins processam esses valores, convertendo-os em tabelas ou gráficos que demonstram as mudanças.

Se o programa não conseguir encontrar o plugin, ou se este não for executável, ou ainda se o plugin não retornar a resposta correta para o daemon, a interface web exibe um status de UNKNOWN (desconhecido) e uma mensagem de erro *Return Code of 127 is out of bounds*.

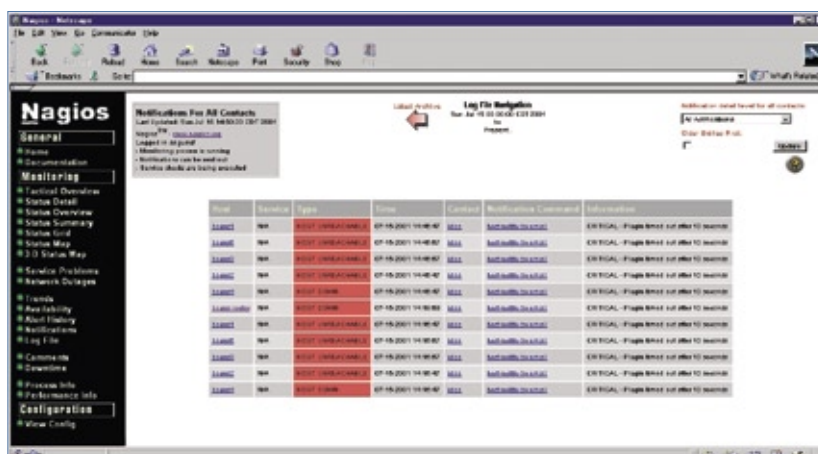


Figura 3 O Nagios mantém um resumo dos eventos de notificação.

Os parâmetros listados anteriormente, `-w` e `-c`, estão definidos para a maioria dos plugins, pois também estabelecem os limites para WARNING e CRITICAL. Nosso exemplo especifica o limite de espaço livre em disco em 50 ou 20%. Ao testar um plugin na linha de comando, é necessário escolher um limite bem baixo, exatamente para verificar se o plugin realmente retorna o status esperado.

Se os resultados da preparação e das checagens estiverem a contento, pode-se acrescentar uma entrada referente ao plugin na configuração do Nagios:

```
define command {
command_name check_disk
command_line $USER1$/check_disk -
➔w $ARG1$ -c $ARG2$ -p $ARG3$
}
```

Não é típico fixar os limites de valores de alerta ou os nomes das partições no arquivo de configuração; em vez disso, normalmente é recomendável especificar esses valores ao definir o serviço.

Para preservar o máximo possível de flexibilidade, o Nagios utiliza

macros, que são cadeias de caracteres iniciadas pelo símbolo `$`; a cadeia é substituída pelos dados em tempo de execução do programa. Macros do tipo `$ARGx$` são mais importantes, pois são utilizadas para armazenar parâmetros de definições de serviço.

Monitoramento remoto

Ao monitorar recursos remotos, o Nagios diferencia as checagens diretas das indiretas. As diretas são iniciadas localmente no servidor Nagios. Quase todas as verificações relacionadas a protocolos de rede, como ping, DNS, SMTP e HTTP, são feitas como checagens diretas que simulam o acesso como qualquer cliente normal:

```
nagios# ./check_http -H
➔linuxmagazine.com.br -w 5 -c 10
HTTP OK HTTP/1.1 200 OK - 78673
➔bytes in 0.366 seconds
```

Checagens indiretas são usadas caso o plugin precise requisitar dados de uma máquina remota.

Então, o programa precisa conectar-se à máquina antes de exe-

Exemplo 7: Exemplos do NRPE

```
01 command[check_users]=@libexecdir@/check_users -w 5 -c 10
02 command[check_load]=@libexecdir@/check_load -w 15,10,5 -c 30,25,20
03 command[check_disk1]=@libexecdir@/check_disk -w 20 -c 10 -p /dev/hda1
04 command[check_disk2]=@libexecdir@/check_disk -w 20 -c 10 -p /dev/hdb1
```

cutar o plugin diretamente nela. Para isso, a forma mais fácil é criar conexões SSH entre o servidor Nagios e os clientes, sem atribuir senhas, e usar o SSH para chamar os plugins. O pacote de plugins fornece um plugin chamado *check_by_ssh* para esse propósito.

Para iniciar o plugin *check_disk* remotamente em outro servidor, é necessário encapsulá-lo no *check_by_ssh*. A definição na linha de comando fica assim:

```
define command {
    command_name check_ssh_disk
    command_line $USER1$/check_by_
    ssh -t 60 -H $HOSTADDRESS$ -C
    "$USER2$/check_disk -w $ARG1$ -c
    $ARG2$ -p $ARG3$"
```

O comando *check_by_ssh* é iniciado localmente. Ele estabelece uma conexão com o servidor, e em seguida executa o plugin *check_disk*, que se encontra instalado no servidor.

O caminho dos plugins em servidores remotos é guardado na variável *\$USER2\$*, para que não seja necessário especificá-lo.

Outra opção é o *Nagios Remote Plugin Executor* (NRPE), um programa cliente-servidor para o Nagios que executa plugins remotos. Para usá-lo é necessário instalar o servidor NRPE, assim como

os plugins nos servidores a serem monitorados. O NRPE consiste em um daemon para os clientes Nagios e um plugin de checagem para o servidor.

É interessante compilar o plugin diretamente no servidor Nagios. Após descompactá-lo, digite simplesmente *./configure && make all*. Isso cria o arquivo *check_nrpe*, que depois pode ser copiado para o diretório local com os outros plugins, antes de se prosseguir à configuração de um comando respectivo:

```
define command{
    command_name check_nrpe
    command_line $USER1$/check_nrpe
    -H $HOSTADDRESS$ -c $ARG1$
}
```

Para economizar esforço, pode-se instalar o serviço NRPE nos clientes a partir dos pacotes, ou copiá-lo do servidor Nagios.

Recomenda-se executar o NRPE com o *inetd* ou *xinetd*, e usar um *TCP wrapper*. O arquivo *README* do pacote NRPE contém instruções.

Ao final, deve-se informar as checagens que se deseja que o NRPE faça remotamente, em *nrpe.cfg* (exemplo 7). O arquivo *sample* contém exemplos (veja o exemplo 6).

Embora o NRPE seja a ferramenta oficial para checagens remotas, ele possui algumas desvantagens em comparação com o SSH; por exemplo, ele necessita de um daemon adicional, e também exige a abertura de mais uma porta.

SNMP

O SNMP é a ferramenta ideal para coletar informações de hardware remoto. Existe um pacote de plugin para o Nagios que fornece o *check_snmp*.

Pode-se usar o *check_snmp* para se obter valores através do *OID* do *MIB* do vendedor. Seguindo o padrão familiar de outros plugins

do programa, a linha de comando para isso é *nagios# ./check_snmp -H <endereço_ip> -o <OID> -w warning -c critical -m :*. O último argumento, *-m :*, é importante, mas mal documentado. Ele impede que o plugin tente carregar MIBs instalados localmente. Isso ocasiona mensagens de erro com todas as versões do plugin. Entretanto, é necessário encontrar os OIDs certos manualmente, seja verificando os MIBs do vendedor ou por tentativa e erro com o *snmpwalk*.

Todo esse monitoramento de rede é inútil se o administrador não for notificado em caso de problemas. Mais uma vez, o Nagios possui uma coleção de sofisticadas funções de alerta. A cada vez que um erro é detectado em algum local do sistema, ele inicia um complexo processo de análise. O software começa verificando se alguém está ciente do erro (veja *max_check_attempts*), se a parada do serviço foi planejada pela interface web e se o alerta está ativado para a hora atual do dia (veja *notification_interval*).

Contatos

Após fazer isso, o Nagios descobre os contatos atribuídos à máquina, e confere suas configurações de notificação para saber se os contatos devem ser notificados; em caso positivo, que tipo de notificação é esperado (veja *notification_options*).

Finalmente, o programa verifica se o contato deseja ser avisado imediatamente (veja *notification_period*). Graças a esse esquema, ele suporta um controle altamente granular das notificações.

Dependendo da máquina, hora e contato, pode-se enviar diferentes mensagens através de canais distintos. Para enfocar esse mecanismo ainda mais, as escalas oferecem aos administradores a possibilidade de alterar a forma como os alertas subsequentes para programas já existentes serão feitos.



Figura 4 A interface WAP do Nagios é capaz de enviar um alerta para telefones celulares aptos a acessar a Internet.

Para enviar de fato um alerta, o Nagios manda um comando similar aos de checagem. Em outras palavras, as notificações não estão fixadas no Nagios. Em vez disso, o programa executa um comando ou script de shell (**exemplo 8**).

A parte importante da configuração do alerta são os dados enviados ao programa de email. Mais uma vez são usadas macros para transmitir os dados. A documentação do Nagios inclui uma lista completa de macros disponíveis.

Arquivos de configuração

Como ponto de partida para nossos experimentos, o Nagios inclui vários arquivos de exemplo. O arquivo `minimal.cfg` simplesmente implementa algumas checagens para o localhost, enquanto `bigger.cfg` possui exemplos mais sofisticados. Entretanto, mesmo que só se queira monitorar uma pequena rede, faz sentido dedicar-se à organização de sua configuração de objetos.

Distribuir os objetos ao longo de arquivos separados de acordo com o tipo de objeto é altamente recomendável. Por exemplo, pode-se usar os arquivos `maquinas.cfg`, `servicos.cfg`, `contatos.cfg`. Todavia, até mesmo essa abordagem pode rapidamente tornar-se difícil de acompanhar, e não há motivos reais para se manter tipos de objetos individuais separados.

O Nagios encontra os objetos independentemente de quantos arquivos (ou até diretórios) separados estejam em uso, contanto que seu arquivo `nagios.cfg` aponte para os locais corretos.

É interessante usar subdiretórios para estruturar logicamente uma con-

Exemplo 8: Configuração de notificação

```
01 define command {
02     command_name notify-by-email
03     command_line /usr/bin/printf "%b" $$
04     "***** Nagios 1.0 *****\n\n" $$
05     Notification Type: $NOTIFICATIONTYPE$\n\n $$
06     Service: $SERVICEDESC$\n $$
07     Host: $HOSTALIAS$\n $$
08     Address: $HOSTADDRESS$\n $$
09     State: $SERVICESTATE$\n\n $$
10     Date/Time: $DATETIME$\n\n $$
11     Additional Info:\n\n $$
12     $OUTPUT$ | /usr/bin/mail -s $$
13     "** $NOTIFICATIONTYPE$ alert -$HOSTALIAS$/$SERVICEDESC$ $$
14     is $SERVICESTATE$ **" $CONTACTEMAIL$
15 }
```

figuração. Por exemplo, guardar as configurações globais e de rede nos níveis mais altos. O nível seguinte conteria, então, subdiretórios individuais para cada cliente, departamento ou tipo de dispositivo.

Então, pode-se incluir no arquivo de configuração os objetos relacionados, como uma máquina, junto com os serviços e contatos associados a ela. O melhor método é organizar os objetos de forma a facilitar sua procura.

Conclusões

O Nagios oferece muito mais do que se pode descrever em um artigo. Inúmeros recursos e projetos adicionais oferecem aos administradores a possibilidade de acrescentar funções de monitoramento para qualquer cenário plausível. Ele também suporta sistemas de notificação alternativos que usem SMS, e pode até realizar chamadas telefônicas (**figura 4**). O portal de programas adicionais (*add-ons*) [3] é o melhor lugar para se procurar extensões e plugins do programa.

Não importa quão incomuns sejam suas necessidades, há um plugin

adequado para elas, ou ao menos um que possa ser usado como ponto de partida para a criação da sua própria solução personalizada. Não se esqueça, é claro, de compartilhar seu novo plugin com a comunidade. ■

Mais Informações

- [1] Página do Nagios: <http://www.nagios.org>
- [2] Repositório do Debian com pacotes do Nagios: <http://www.backports.org>
- [3] Documentação do arquivo de configuração do Nagios: http://nagios.sourceforge.net/docs/2_0/configmain.html
- [4] Objetos do Nagios: http://nagios.sourceforge.net/docs/2_0/xodtemplate.html
- [5] Plugins do Nagios: <http://nagiosplug.sourceforge.net/>
- [6] Plugins e add-ons: <http://www.nagiosexchange.org>

O autor

Julian Hein é o fundador e CEO da empresa alemã NETWAYS (<http://www.netways.de>), que atua na implementação e operação de redes complexas há mais de dez anos.

PostgreSQL



dextra
Coding your Business

Fone: (19) 3256-6722
contato@dextra.com.br
www.dextra.com.br/postgres

GroundWork

Afonso Lima - www.sxc.hu

Trabalho de base

O Nagios possui uma interface web bastante básica. O GroundWork é uma interface mais amigável e com visual profissional para essa ferramenta.

por James Mohr

Ao instalar um sistema Nagios[1], uma solução para facilitar o trabalho de configuração é usar um script para adicionar as máquinas e serviços aos arquivos responsáveis por isso. Esse método é rápido e fácil para administradores experientes que preferem trabalhar com o vi do que clicar em uma interface gráfica.

Porém, se a única necessidade for realizar uma pequena mudança, pode ser deveras incômoda a obrigatoriedade de se fazer login na máquina e caminhar pelos diretórios até encontrar um arquivo de configuração específico. Nesses casos, uma interface gráfica é muito útil, principalmente quando depende apenas de um navegador web.

Vários projetos já tentaram criar uma interface assim para o Nagios, com variados graus de sucesso. Infelizmente, alguns desses projetos perderam força e não conseguiram acompanhar o desenvolvimento dessa grande ferramenta de monitoramento.

Uma interface para o Nagios que ainda está em desenvolvimento ativo é o GroundWork[2]. Esse software é, ao mesmo tempo, uma empresa e um projeto de software de código aberto. Como empresa comercial, a GroundWork naturalmente tem como meta o lucro. Eles oferecem duas versões comerciais de seu produto, além da versão de código aberto disponível para download a partir do SourceForge[3].

Leitores cautelosos devem estar céticos quanto a um projeto de código aberto que também está disponível como produto comercial, pois, nesses casos, a versão livre costuma ser apenas uma amostra da versão comercial, com funcionalidade bastante reduzida. Porém, felizmente o GroundWork Monitor não se enquadra nessa descrição. Ele oferece toda a funcionalidade necessária para configurar e gerenciar a sua instalação do Nagios.

No núcleo do sistema fica a plataforma de aplicação Guava, que suporta a interação com usuários através de AJAX. Isso significa que as páginas são atualizadas sem a necessidade de serem comple-

tamente recarregadas. O Guava também fornece os aspectos de apresentação do sistema, assim como os recursos relacionados à segurança do usuário. O Guava propriamente dito é um projeto de código aberto disponível no SourceForge[4].

A versão atual do GroundWork baseia-se no Nagios 2.5. Além de oferecer uma interface de usuário, o GroundWork traz um banco de dados MySQL para informações sobre eventos, em contraste com a solução baseada em texto puro oferecida pelo Nagios “pelado”. Além disso, o GroundWork inclui o pacote de plugins do Nagios, que costuma exigir o download em separado.

Fácil Instalação

As várias fontes de documentação do GroundWork listam requisitos mínimos de hardware diferentes, e muitas vezes até contraditórios. Por exemplo, um local informa que a versão de código aberto exige apenas um único processador de 2,8 GHz, enquanto outro afirma que são necessários dois desse. Naturalmente, a quantidade de memória e CPUs exigida depende do número de dispositivos que se deseja monitorar, e com que frequência. Entretanto, seria interessante ter orientações mais consistentes.

A versão aberta do programa está disponível em[3] como um pacote RPM normal, uma imagem ISO de CD, ou uma “appliance” do VMware. A versão baixada para nossos testes foi a 5.0.5, tanto da imagem ISO quanto dos pacotes RPM. Iniciando a partir do CD, o usuário precisará informar sua configuração de rede, e logo em seguida já poderá utilizar o GroundWork.

A versão em pacote RPM só é compatível com o *Red Hat Enter-*

prise, o *Suse Linux Enterprise* e o *CentOS 4*.

Em nossos testes, a instalação pareceu transcorrer direito, porém, como a versão do Suse usada não era a Enterprise, não foi possível iniciar o GroundWork devido a vários problemas com bibliotecas.

É incômodo o fato de até mesmo a versão de código aberto exigir um produto comercial, com apenas uma única distribuição não comercial sendo suportada.

O GroundWork instala sua própria versão do Apache. Caso se possua um servidor Apache em execução, ele será parado e desativado pelo GroundWork – mas nada será apagado ou alterado. A documentação diz que “todo o conteúdo exibido será servido pela versão do Apache incluída no GroundWork”.

O processo não é automático, e ao final é necessário realizar algumas configurações manuais para disponibilizar seu conteúdo.

Além disso, não é possível atualizar o Apache pelos meios

normais, pois qualquer mecanismo de atualização instalará a versão original do Apache. Para evitar tais complicações, a documentação sugere que se instale o GroundWork em um sistema independente.

Rodando

Quando conseguimos executá-lo, o programa exibiu uma aparência bastante profissional. A estrutura do menu é lógica, e a navegação através deste é fácil – especialmente para usuários experientes no uso do Nagios.

Pode-se baixar um guia de avaliação que leva o usuário, passo a passo, através diversas configurações básicas do GroundWork. O guia de avaliação não presume muito a respeito dos conhecimentos do leitor, e não tivemos problemas para instalar o produto e fazê-lo funcionar com ajuda do guia.

Será necessária uma versão funcional do MySQL. O guia de avaliação inclui algumas informações básicas sobre a conexão com o banco de dados. Quando o usuário entrar pela primeira vez,

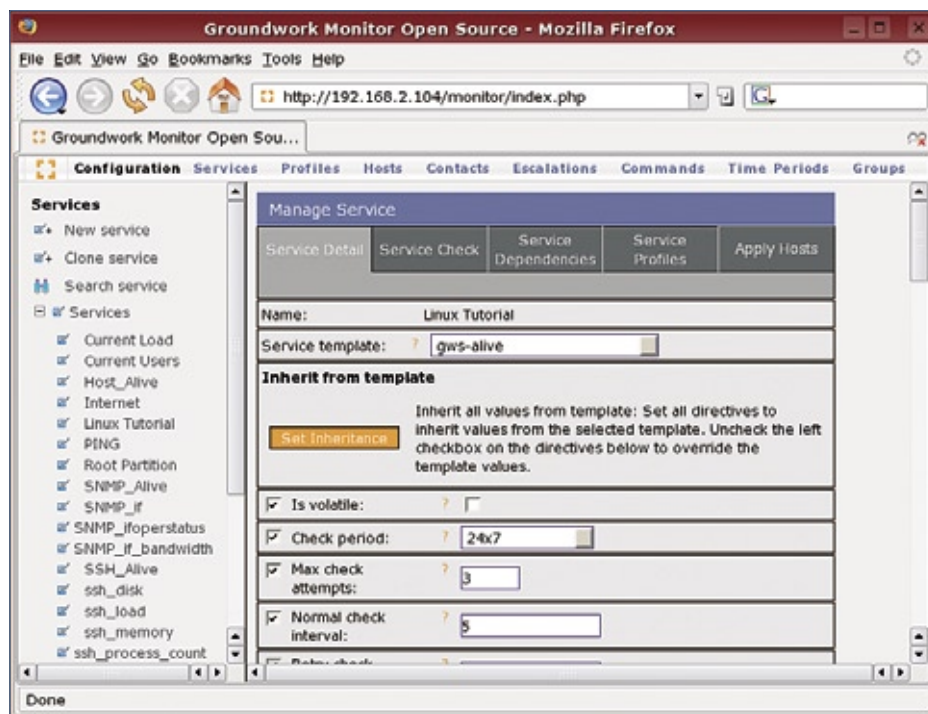


Figura 1 Janela de definição de serviço no GroundWork.

verá uma animação na página inicial apontando para o *Configuration EZ*, que oferece uma forma facilitada de acrescentar máquinas à rede rapidamente, através da descoberta automática de serviços e máquinas. É possível atribuir nós a grupos de nós existentes, ou deixá-los sem atribuição (“*unassigned*”).

O *Configuration EZ* bloqueia as configurações mais detalhadas, mostrando apenas as opções mais básicas. Com algumas exceções, fica-se limitado a atribuir configurações pré-existentes (como verificações de serviços) a novas máquinas. Em redes onde se deseja somente acrescentar novos nós ou outros dispositivos, e não um novo serviço ou monitor, essa interface espartana é muito útil.

Embora a configuração do monitoramento básico seja bem fácil com o GroundWork, deve-se estar ciente de que a tecnologia subjacente ainda é o Nagios. Administradores experientes compreenderão o modo de operação do GroundWork com bastante facilidade. Entretanto, os iniciantes devem dedicar algum tempo a adquirir uma maior familiaridade com o Nagios antes de usar o GroundWork de forma eficiente.

O GroundWork opera por uma interface web. O *frame* esquerdo da janela abriga o menu de navegação, e a área de trabalho propriamente dita fica à direita (**figura 1**).

No alto da janela fica a barra de navegação (chamada de *menu* em vários pontos). Ela se modifica de acordo com a parte do sistema que estiver sendo visualizada.

Ao entrar no sistema, o administrador começa na página identificada como *Home* no canto superior esquerdo da tela. Ao clicar no logo do GroundWork, um menu se abre, mostrando as principais áreas, como *Administra-*

tion e *Configuration*, por exemplo. Quando se seleciona um item, o painel esquerdo de navegação muda de acordo.

Para inserir dados no sistema GroundWork, pode-se iniciar do zero ou carregar uma instalação pré-existente do Nagios. Em nossa máquina de testes, ainda não havíamos instalado o Nagios, então escolhemos uma instalação do zero (*fresh install*); mas também testamos a instalação em uma máquina já com o Nagios.

Não encontramos problemas ao carregar os arquivos de configuração pré-existentes. Apesar de a versão do GroundWork testada ser baseada na versão 2.5 do daemon de monitoramento, ainda é possível utilizar arquivos da versão 1.x a partir da interface do GroundWork.

Se alguma diretiva estiver faltando no Nagios 2.x, a verificação inicial mostrará o problema, possibilitando a adição dessas diretivas a partir da interface gráfica.

Se for preferível carregar uma instalação pré-existente do Nagios, pode-se atualizar a configuração atual do GroundWork com objetos de sua configuração do Nagios, ou limpar (ou dar um *purge*) nas informações relacionadas ao Nagios no banco de dados do GroundWork, substituindo todo o conteúdo do arquivo de configuração do Nagios.

Ao adicionar nós pela descoberta automática, pode-se selecionar uma rede inteira, ou simplesmente um bloco de endereços IP. Como a rede usada no teste era relativamente pequena, configuramos o GroundWork para varrer apenas os primeiros 50 endereços IP, o que foi completado em menos de um minuto.

Cada nó encontrado pelo GroundWork é listado na interface gráfica; depois, é possível se-

leccionar os nós e adicioná-los ao sistema (ou não). Caso seja necessário, pode-se carregar nós a partir de um arquivo externo, em vez de passar pela potencialmente demorada descoberta automática.

Um dos maiores problemas da interface aparece ao se adicionar nós. A lista de nós não é atualizada automaticamente. Em vez disso, parece ser necessário fechá-la e depois abri-la novamente para que sejam mostrados os novos nós.

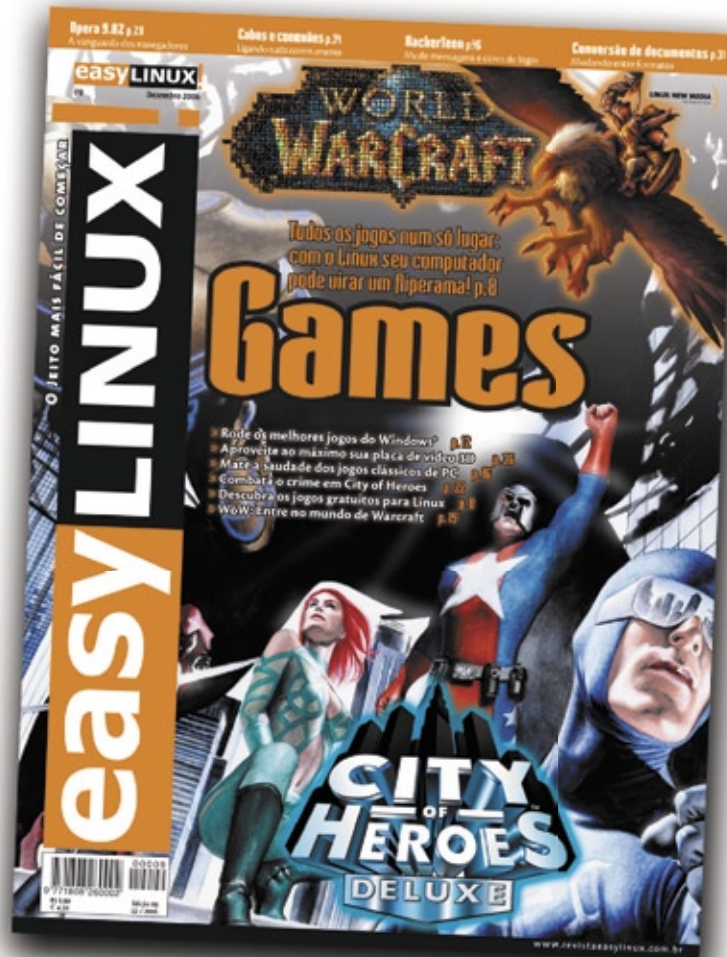
O GroundWork alega fazer uso de AJAX para efetuar a atualização automática das páginas sem interação com o usuário, o que torna esse comportamento ainda mais decepcionante.

Após executarmos a descoberta automática, todas as máquinas Linux foram corretamente identificadas. Apesar de o GroundWork ter reconhecido as estações Windows, ele foi incapaz de identificar seus sistemas operacionais, o que rendeu, ao final, apenas um grupo: “Linux Servers”. Todavia, pode-se acrescentar grupos de máquinas literalmente em alguns segundos, o que reduz bastante esse problema.

Administração

O GroundWork foi feito para administração. É possível criar grupos de usuários, o que dá acesso ao sistema. Os privilégios depois são determinados pelos papéis. Para cada papel, são definidas *subscriptions*. Embora os papéis sejam cumulativos, eles definem somente as aplicações (porções do sistema) que o usuário pode acessar. Por exemplo, pode-se conceder a um papel acesso à interface do Nagios, permitindo que ele veja o status das máquinas e serviços, mas impedindo que ele faça alterações.

Em junho nas bancas por apenas R\$8.90 !!!



Easy Linux traz todos os meses notícias, tutoriais de programas e jogos, dicas e tudo que o usuário iniciante precisa saber para usar **Linux** em casa e no trabalho. Com linguagem simples e abrangente, **EasyLinux** é a leitura obrigatória para quem quer “desbravar” o **software livre**!

EasyLinux: leia para saber!

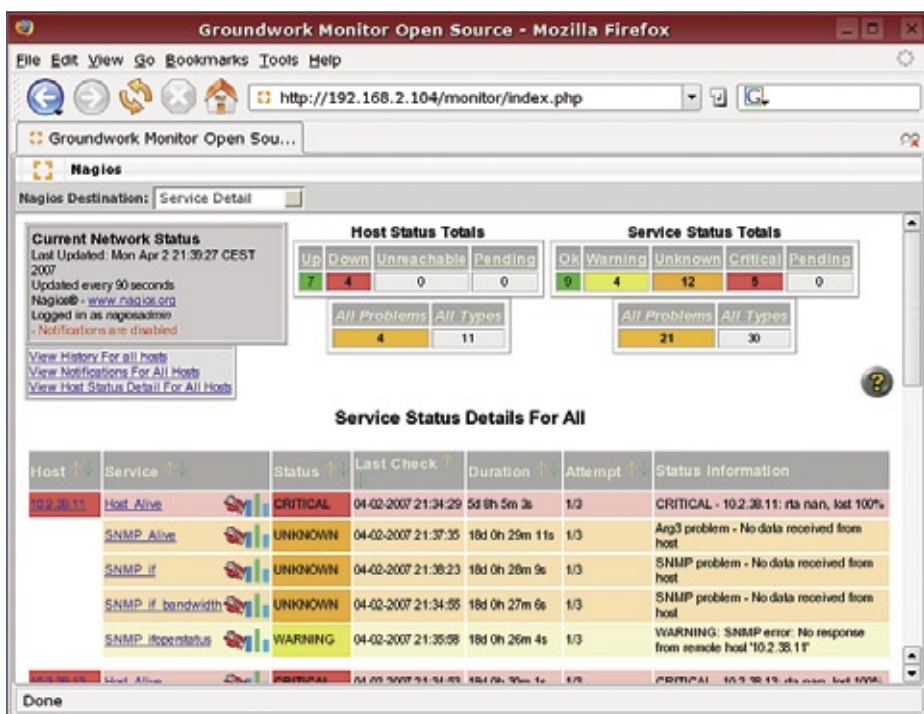


Figura 2 Interface do Nagios no GroundWork.

Na seção de administração, pode-se instalar pacotes e, em alguns casos, configurá-los. Os pacotes podem ser acrescentados ao sistema através do item de menu chamado *Wrappit*. Esse recurso de gerenciamento de pacotes permite a integração de aplicações web pré-existent à estrutura de menu do GroundWork.

O menu *Configuration* fornece acesso a todas as configurações que normalmente o Nagios ofereceria. As configurações primárias do Nagios são acessíveis pela barra de menu (figura 1).

A opção *Control* representa a configuração geral do Nagios. Nela, é possível definir vários diretórios, além do usuário sob o qual o GroundWork será executado, e o comportamento padrão do Nagios. As opções em *Control* são os valores que normalmente seriam encontrados no arquivo de configuração do Nagios (*nagios.cfg*, normalmente). Como há opções demais, o GroundWork as divide em múltiplas telas, obrigando o administrador a salvar cada tela

antes de prosseguir à próxima. Isso significa que, se houver algo que se deseje acessar na última tela, será necessário carregar e salvar cada uma das anteriores.

A opção *Tools* possibilita que se apague máquinas ou serviços com base em caracteres curinga. Não é possível definir seu próprio curinga. Em vez disso, o GroundWork já traz uma lista de padrões que parecem cobrir todas as possíveis combinações iniciais.

Além de oferecer seu próprio conjunto de diálogos de configuração, o GroundWork oferece acesso à interface tradicional do Nagios (figura 2). Nela, pode-se visualizar os serviços, agendar tarefas e períodos de manutenção, desativar verificações e tudo o que for possível fazer com a interface gráfica do Nagios.

Útil, mas imperfeito

Definitivamente, o custo (zero) da versão de código aberto do GroundWork é um importante

fator, difícil de ser ignorado ou superado. Mesmo sem os recursos extra da versão comercial, a facilidade de uso do programa merece reconhecimento.

Infelizmente, o GroundWork não se comportou como esperado em várias ocasiões. Em algumas situações, o programa não nos permitiu realizar nada ao fazer seleções. Por exemplo, ao clicar nos links da barra de ferramentas ou selecionar valores dos menus *drop-down*, com frequência o programa simplesmente pára. Entretanto, atualizar a página ou ir para outra área do programa corrige o problema, quando ocorre.

O GroundWork parece ter problemas ao se usar múltiplas abas no *Firefox*. Aparentemente, ele guarda a página na última aba que tiver sido aberta e, se recarregarmos alguma das abas anteriores, ela carregará a página mais nova naquela onde se estava trabalhando.

Parece-nos que o GroundWork está tentando em demasia ter um visual “avançado” atraente para administradores sem familiaridade com o Nagios ou com o monitoramento de sistemas. O site do produto e a documentação são cheios de hipérboles de marketing que desviam a atenção em relação à real funcionalidade do produto. Ainda assim, a versão de código aberto do software é um produto sólido e recomendável. ■

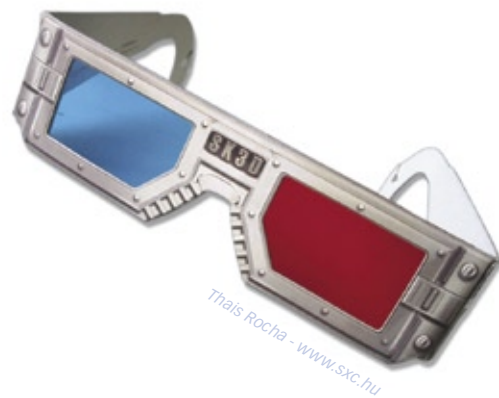
Mais Informações

- [1] Nagios: <http://www.nagios.org>
- [2] Versão de código aberto do GroundWork: <http://www.groundworkopensource.com>
- [3] Download do GroundWork: http://www.groundworkopensource.com/downloads/full_download.html
- [4] GroundWork Guava: <http://guava.sourceforge.net/>

Outra visão

O ambiente desktop 3D Looking Glass oferece uma nova visão da área de trabalho.

por Fabrizio Ciacchi



Os ambientes desktop 3D, como *Compiz*^[1] e *Beryl*^[2], são um novo tópico popular na comunidade Linux. Porém, esses dois softwares apenas começaram a explorar as possibilidades de uso da terceira dimensão para exibir e organizar informações.

Um dos primeiros – e mais sofisticados – projetos de desktop 3D é o *Looking Glass*^[3] (LG3D), criado por um programador da Sun, Hideya Kawahara. Após mostrar seu passatempo a seus superiores, Hideya foi agraciado com uma equipe de desenvolvedores para auxiliá-lo na criação do LG3D.

O Looking Glass teve sua primeira versão estável (1.0) liberada recentemente. Vamos analisar alguns de seus recursos mais interessantes.

Usuários do *Ubuntu* têm pacotes individuais para cada componente disponível no mesmo site, e outros usuários podem usar o pacote genérico para Linux.

Após instalar o Looking Glass através do script de instalação contido no pacote baixado, é possível executá-lo de três formas diferentes. A primeira requer que já haja um gerenciador de janelas em execução, e abrirá o LG3D com o comando `lg3d-app`, digitado em um terminal. A segunda forma é semelhante, porém abre o gerenciador da Sun em tela cheia, com o comando `lg3d-app-full`. Por último, para incluir no GDM ou KDM a opção de iniciar o LG3D, são necessários os comandos:

```
# ln -s /caminho/até/o/lg3d /usr/
# share

/usr/share/lg3d/bin
./postinstall
```

Instalação

Por ser inteiramente feito em Java, o LG3D pode rodar em Linux, Windows e Solaris. Para apenas conhecer o ambiente, é possível utilizar o *LiveCD* disponível em ^[4]. Os nada modestos requisitos mínimos de instalação incluem um processador de 1.4 GHz, 512 MB de memória e uma placa aceleradora 3D com 128 MB de memória, além de um driver de vídeo (no Linux) com suporte a *OpenGL* 1.2 (sendo a versão 1.3 a recomendada).

Também é possível baixar o *Mega Bundle*^[5], um pacote espaçoso (aproximadamente 150 MB) que inclui a *JDK*, as bibliotecas *java3d* e o *LG3D*, e deve funcionar em qualquer distribuição.

Visual

Na parte de baixo da tela do Looking Glass fica a barra de tarefas (**figura 1**). À esquerda localiza-se o menu do LG3D, oferecendo o acesso a aplicativos da mesma forma que qualquer ambiente desktop. Ao lado do menu há ícones para as ferramentas mais usadas, seguidos dos ícones dos aplicativos abertos. No canto direito da barra fica a bandeira pirata usada para sair do LG3D.

Um recurso muito interessante desse ambiente desktop é o suporte ao papel de parede panorâmico. Múltiplas áreas

de trabalho podem habitar regiões de uma única imagem panorâmica (**figura 2**). Clicando-se com o botão esquerdo no lado direito ou esquerdo da área de trabalho, o usuário é levado à parte adjacente da imagem. Um clique direito na barra de tarefas mostra a imagem inteira, a partir da qual é possível escolher uma área de trabalho (como mostra a **figura 2**).

O uso da perspectiva é mais um recurso interessante do LG3D. Não apenas os objetos possuem profundidade, como também a própria área de trabalho. O eixo Z acrescentado à área de trabalho



Figura 1 A barra de tarefas fica localizada no centro do ambiente do Looking Glass.

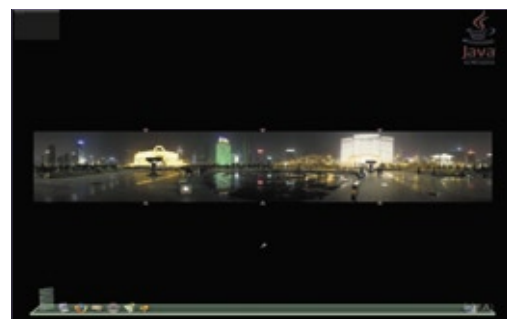


Figura 2 É possível selecionar uma área de trabalho movendo-se entre as regiões de uma única imagem panorâmica.

(figura 3) permite que o tamanho dos objetos varie conforme sua “distância” do usuário. As janelas geralmente são abertas em uma distância padrão. Com a tecla **[Ctrl]** pressionada, basta usar a rodinha do mouse, com o cursor localizado em sua barra de título, para aproximar e afastar a janela.

Uma das possibilidades mais inovadoras oferecidas pelo desktop 3D da Sun é a escrita de notas no verso das janelas (figura 4). Pode-se usar isso para registrar uma observação sobre o conteúdo da janela, por exemplo. Para criar uma nota, basta clicar com o botão direito na barra de título, o que faz a janela girar 180° horizontalmente. Todas as janelas já possuem automaticamente uma área para notas no verso, e basta digitar nela a nota.

Até mesmo as bordas das janelas são usadas pelo LG3D: ao rotacionar as janelas, o título de cada uma é mostrado nelas (figura 5), o que facilita a organização das janelas, especialmente quando há muitas delas abertas.

Os ícones das janelas abertas, na barra de tarefas, também não são estáticos como nos outros ambientes desktop, mas miniaturas das janelas. Um filme reproduzido em uma janela minimizada, nesse caso, continua sendo mostrado, porém em miniatura, na barra de tarefas.

Na realidade, toda a área de trabalho pode ser rotacionada. Clicando-se com o botão esquerdo sobre o logo do Java, no canto superior direito da área de trabalho, o arrastar do mouse faz a área de trabalho girar de.

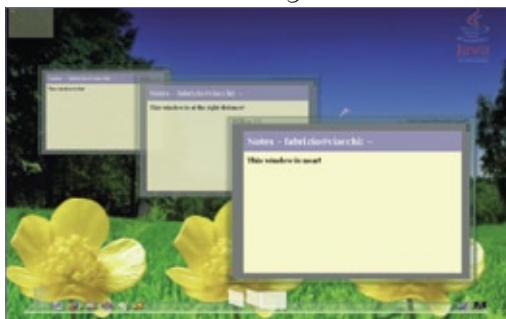


Figura 3 Os objetos parecem menores ou maiores de acordo com sua posição no espaço tridimensional.

Aplicativos

O Looking Glass pode executar tanto aplicativos do Linux quanto programas em Java nativos. Essas últimas empregam as bibliotecas 3D em Java e classes especializadas do LG3D. Todos os aplicativos 2D do Linux são renderizados em três dimensões por uma camada de abstração oferecida pelo *X11* [6]. A versão 1.0 do desktop da Sun conseguiu eliminar os problemas que o impediam de funcionar em harmonia com alguns programas populares do Linux, como *Firefox* e *Evolution*.

Evidentemente, os aplicativos escritos especificamente para o Looking Glass, como o reprodutor de músicas *Trumplayer*, o visualizador de fotos *Zoetrope* e o gerenciador de fotos *LgScope 3D* apresentam o melhor visual, pois fazem uso dos atraentes recursos visuais desse desktop.

Conclusões

O Looking Glass é um projeto impressionante e inovador, mas talvez ainda não esteja pronto para o uso diário. Apesar de o sistema já estar bastante estável, ele mostrou problemas com a atualização da imagem no monitor, em nossos testes.

Os gráficos são realmente impressionantes, mas eventualmente uma imagem simples, ou até mesmo alguns papéis de parede, mostraram resoluções inesperadamente baixas. Talvez essas simplificações melhorem o desempenho, mas alguns usuários podem ficar muito frustrados com elas. Apesar disso tudo, o Looking Glass é um projeto muito importante e com uma nova abordagem para o desktop 3D. ■



Figura 4 O Looking Glass permite a escrita de notas no verso das janelas.



Figura 5 É possível alinhar as janelas do Looking Glass como livros em uma prateleira.

O autor

Fabrizio Ciacchi (<http://fabrizio.ciacchi.it>) é estudante de Ciências da Computação na Universidade de Pisa. Trabalha como consultor para diferentes companhias e escreve artigos para a edição italiana da Linux Magazine (www.linux-magazine.it).

Mais Informações

- [1] Compiz: <http://www.go-compiz.org>
- [2] Beryl: <http://www.beryl-project.org>
- [3] Looking Glass: http://www.sun.com/software/looking_glass/
- [4] LiveCD do Looking Glass: <http://lg3d-livecd.dev.java.net>
- [5] Pacotes binários do Looking Glass: <http://lg3d-core.dev.java.net/binary-builds.html>
- [6] Panorama do LG3D (inglês): <http://lg3d-core.dev.java.net/files/documents/1834/30923/LG3D-Overview.pdf>

Sexta e última aula da preparação LPI

LPI nível 1: Aula 6

Configure compartilhamentos de rede e aprenda a administrar a segurança do sistema na última aula da série de preparação para a certificação LPI nível 1.

por Luciano Siqueira



The Linux
Professional
Institute

TUTORIAL



Objetivo 1.113.4: Administração Apropriada dos Daemons NFS e SAMBA

NFS

Através do NFS – *Network File System* – é possível montar diretórios compartilhados remotos como se fossem dispositivos locais. O NFS precisa estar habilitado no kernel, seja nativo ou carregado como módulo, tanto no servidor quanto na máquina cliente.

Para montar dispositivos remotos, é necessário que o *daemon* `/sbin/rpc.portmap` esteja ativo no cliente e no servidor. Sua execução é controlada através do script `/etc/init.d/portmap start|stop|restart` ou `/etc/rc.d/rc.portmap start|stop|restart`.

Para que um host possa servir diretórios através do NFS, é necessário ativar os daemons:

- ▶ `/usr/sbin/rpc.rquotad`
- ▶ `/usr/sbin/rpc.nfsd`
- ▶ `/usr/sbin/rpc.mountd`
- ▶ `/usr/sbin/rpc.lockd`
- ▶ `/usr/sbin/rpc.statd`

A execução de todos esses daemons é unificada através do script `/etc/rc.d/`

`init.d/nfs start|stop|restart` ou `/etc/rc.d/rc.nfsd start|stop|restart`.

Os compartilhamentos são configurados através do arquivo `/etc/exports`. Cada linha contém um diretório compartilhado seguido de uma lista, separada por espaços, dos hosts que poderão montá-los. Cada host pode estar acompanhado de parênteses imediatamente a sua direita, sem que haja espaço depois dele, contendo opções de acesso para o mesmo.

Exemplo de compartilhamento em `/etc/exports`:

```
/mnt/hdb1 192.168.1.0/26(ro)
```

O diretório local `/mnt/hdb1` poderá ser montado por todos os hosts da subrede local `192.168.1.0/26`, apenas em modo somente leitura (`ro`, de *read only*). Uma opção de acesso importante é `no_root_squash`, que permite que o usuário remoto de ID 0 (`root`) monte o compartilhamento. Essa opção é especialmente útil quando o diretório local compartilhado é o diretório raiz no cliente remoto. Há várias opções de controle de acesso que podem ser consultadas através de `man 5 exports`.

Para atualizar as alterações feitas ao arquivo `/etc/exports` no servidor NFS ativo, é necessário executar o comando `exportfs -a`. Para desativar

os compartilhamentos em `/etc/exports`, executa-se `exportfs -ua`.

No cliente, o próprio comando `mount` é usado para montar o diretório remoto. Por exemplo, montar o diretório compartilhado no exemplo anterior num host da subrede local `192.168.1.0/26`:

```
# mount -t nfs 192.168.1.1:/mnt/  
hdb1 /mnt/remoto
```

Esse exemplo presume ser `192.168.1.1` o IP do servidor do compartilhamento, e existir no cliente o diretório alvo `/mnt/remoto`.

O comando `nfsstat` mostra estatísticas de uso dos compartilhamentos NFS no servidor.

SAMBA

Máquinas rodando Linux podem acessar e fornecer recursos compartilhados a máquinas rodando MS-Windows®, como arquivos e impressoras.

Os daemons responsáveis são `/usr/sbin/smbd` (cliente/servidor *SMB*) e `/usr/sbin/nmbd` (cliente/servidor *NetBIOS*). Ambos são geralmente disparados pelos scripts de inicialização do sistema. As configurações de acesso e compartilhamento do SAMBA são feitas no arquivo `smb.conf`, geralmente em `/etc/samba/` ou em `/etc`.

Exemplo 1: arquivo smb.conf

```
[global]
server string = Slackware Samba Server
log file = /var/log/samba.%m
max log size = 50
dns proxy = No

[homes]
comment = Home Directories
read only = No
browseable = No

[printers]
comment = All Printers
path = /var/spool/samba
printable = Yes
browseable = No

[Montados]
comment = Dispositivos Montados no servidor
path = /mnt
```

O **exemplo 1** demonstra o conteúdo do arquivo `smb.conf`. Há três seções básicas no arquivo `smb.conf`:

- ♦ **[global]**: Define o comportamento geral do samba, como o nome do grupo de trabalho, redes permitidas, tipo de acesso aos recursos etc;
- ♦ **[homes]**: Permite que cada usuário acesse seu diretório pessoal no servidor. Pode conter opções restritivas e outras. Conseqüentemente, este compartilhamento pressupõe que o usuário logado no cliente tenha uma conta no servidor;
- ♦ **[printers]**: Compartilha as impressoras instaladas no servidor com os clientes. O funcionamento da impressora no servidor não depende de configuração no samba.

Outros compartilhamentos podem ser criados por meio de seções específicas para cada um. Diretórios e impressoras podem ser compartilhados e configurados individualmente dessa forma.

O SAMBA pode ser configurado através de uma interface web chamada `swat`. Para poder usar o `swat`, é necessário que o daemon `inetd/xinetd` esteja ativo e o `swat` liberado em `/etc/services`. A porta do `swat` é

a 901. Para acessá-lo, portanto, basta apontar um navegador, no servidor, para <http://localhost:901>.

Os recursos compartilhados numa máquina MS Windows podem ser acessados usando-se o comando `smbclient`.

O **exemplo 2** mostra como listar recursos disponíveis ao usuário *administrador* numa máquina MS-Windows 2000, através do `smbclient`.

Montar o diretório compartilhado pela máquina `pc-w2k`:

```
# mount -t smbfs //pc-w2k/fonts /
➔usr/share/fonts -o
➔username=administrador
```

ou

```
# smbmount //pc-w2k/fonts /usr/
➔share/fonts -o
➔username=administrador
```

A entrada em `/etc/fstab` para essa montagem poderia ser:

```
//pc-w2k/fonts /usr/share/fonts
➔smbfs credentials=/etc/passwd-pc-
➔w2k 0 0
```

A opção `credentials` especifica um arquivo protegido contendo o usuário e a senha para montar o diretório compartilhado. Dessa forma, evita-se deixar a senha à mostra em `/etc/fstab`.

Um usuário comum poderá montar recursos remotos com `smbclient` ou `mount`, se esses comandos tiverem as permissões adequadas (SUID: 1000,1000).

Objetivo 1.113.5: Configurar um Serviço Básico de DNS

Em redes pequenas, é possível que os hosts resolvam (convertam) os nomes de máquinas para números IP e vice-versa, apenas através do arquivo `/etc/hosts`, demonstrado no **exemplo 3**.

DNS

Para grandes redes, no entanto, é muito mais prático, e até necessário, o uso de um servidor *DNS – Domain Name System* – que converte remotamente nomes de máquinas para seus respectivos números IP e vice-versa. A correspondência entre

Exemplo 2: Listar recursos disponíveis para o usuário administrador com o smbclient

```
$ smbclient -L pc-w2k -U administrador
Domain=[PC-W2K] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]
```

Sharename	Type	Comment
IPC\$	IPC	IPC remoto
Fonts	Disk	Fontes True Type
DOCS	Disk	Meus Documentos
ADMIN\$	Disk	Administração remota
C\$	Disk	Recurso compartilhado padrão

```
Domain=[PC-W2K] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]
```

Server	Comment
Workgroup	Master

Exemplo 3: /etc/hosts

```
127.0.0.1      localhost
192.168.1.1    slack102
192.168.1.6    debian
192.168.1.20   pc-w2k
```

Exemplo 4: /etc/named.conf

```
options {
    directory "/var/named";
};

zone "." IN {
    type hint;
    file "root.hints";
};
```

o nome e o número IP é chamada mapeamento, e é organizada de forma hierárquica.

Em outras palavras, um domínio como `howtos.linux.com` será quebrado e resolvido começando por `com`, depois `linux`, e finalmente `howtos`, itens chamados respectivamente *top-level domain*, *second-level domain* e *third-level domain*. É nessa ordem que o endereço IP para `howtos.linux.com` será obtido. Os top-level domains mais comuns são `.com`, `.org` e `.net`, mas há outros.

Servidor DNS

O programa servidor responsável pelo mapeamento é o `/usr/sbin/named`, que é parte do pacote chamado *BIND*, cujas especificações são definidas pelo *Internet Systems Consortium*. Seu arquivo de configuração é `/etc/named.conf`. Em versões anteriores ao BIND 8, o arquivo de configuração chama-se `/etc/named.boot`. O exemplo 4 mostra as configurações para um servidor cache de DNS.

Com essa configuração, o servidor local propriamente não mapeará nenhum nome, mas resgatará os

pedidos de servidores principais e os armazenará temporariamente, para que seus clientes os acessem mais rapidamente. Zonas convencionais têm seções definidas de forma semelhante, como por exemplo, zone `"localhost IN {..."`, e é importante que, para cada uma delas, haja uma zona para DNS reverso

(Exemplo: zone `"0.0.127.in-addr.arpa IN {..."`). O DNS reverso é responsável por converter números IP para seus respectivos nomes.

Voltando ao exemplo 4, na seção `options` é indicado onde estão os arquivos de mapeamento (`directory "/var/named";`). Está definido apenas o mapeamento para `.`, que será consultado caso nenhum outro mapeamento seja encontrado (é esse o caso do exemplo).

No arquivo `/var/named/root.hints` (exemplo 5) está uma lista com os servidores de nomes principais da internet, obtidos através do comando `dig`.

Após alterar os arquivos de configuração, será necessário reiniciar o daemon `named`.

Cliente DNS

O arquivo `/etc/nsswitch.conf` (exemplo 6) determina de que maneiras, e em que ordem, o host local tentará resolver os nomes de endereços.

Os termos que precedem o caractere `:` especificam o tipo dos nomes procurados (`hosts`, `networks` etc.). Os

Exemplo 6: arquivo nsswitch.conf

```
hosts:          files dns
networks:       files
services:       files
protocols:      files
```

termos que sucedem o `:` indicam de que forma o tipo de nome em questão deverá ser resolvido. O termo `files` determina o uso de arquivos locais (como o `/etc/hosts` ou `/etc/networks`) enquanto `dns` determina o uso de um servidor DNS.

O servidor DNS a ser utilizado é especificado através do arquivo `/etc/resolv.conf` (exemplo 7).

A entrada fundamental é `nameserver`, que define o servidor DNS. Outros `nameserver` podem ser especificados para serem servidores DNS secundários.

Registro de Domínios

Um nome de domínio é registrado para uso na internet através de autoridades competentes, como a Internic[1] e a Fapesp[2]. Após o registro, é necessário fornecer os endereços DNS para onde serão direcionadas as solicitações para o domínio em questão.

Objetivo 1.113.7: Utilização do Shell Seguro (OpenSSH)

O *OpenSSH* é o substituto para ferramentas de acesso remoto, como `telnet`, `rlogin`, `rsh` e `rcp`. No host de destino (que aceitará conexões externas), o daemon `/usr/sbin/sshd` deverá estar ativo para possibilitar que clientes se conectem. O `sshd` geralmente é disparado por um script de inicialização do sistema, situado em `/etc/rc.d/rc.sshd` ou `/etc/init.d/sshd`. O daemon `sshd` utiliza a porta 22 para aguardar pedidos de conexão. O comando usado pelo cliente para se conectar é `ssh`. O comportamento do `sshd` pode ser modificado através do arquivo de configuração `/etc/ssh/sshd_config`. Personalizações do comando `ssh` podem ser feitas nos arquivos `/etc/ssh/ssh_con-`

Exemplo 5: arquivo root.hints

```
Trecho de /var/named/root.hints:
(...)
D.ROOT-SERVERS.NET. 3600000 IN      A      128.8.10.90
A.ROOT-SERVERS.NET. 3600000 IN      A      198.41.0.4
H.ROOT-SERVERS.NET. 3600000 IN      A      128.63.2.53
C.ROOT-SERVERS.NET. 3600000 IN      A      192.33.4.12
(...)
```

Exemplo 7: arquivo /etc/resolv.conf

```
nameserver 200.230.1.1
nameserver 200.230.1.2
```

fig, /etc/sshrc ou apenas por usuário, em ~/.ssh/config. Outros comandos úteis do ssh são scp (copiar através de ssh), sftp-server (servidor FTP por ssh) e sftp (cliente FTP por ssh).

Conectar-se como usuário root no host 192.168.1.1:

```
$ ssh root@192.168.1.1
```

Como outros serviços de rede, o ssh está sujeito ao controle via *tcpwrappers*, através dos arquivos /etc/hosts.allow e /etc/hosts.deny. E, por tratar-se de uma forma de login de usuário na máquina em questão, é respeitado o bloqueio a usuários comuns imposto pelo arquivo /etc/nologin. Se o arquivo /etc/nologin existir, apenas o root pode entrar no sistema; aos demais usuários, é vetado o login, e apenas mostrado o conteúdo de /etc/nologin.

Existem dois protocolos de chaves criptográficas usados pelo ssh, o RSA (protocolo 1) e DSA (protocolo 2). Dependendo do protocolo usado, os arquivos de chaves receberão o nome de ssh_host_rsa_key ou ssh_host_dsa_key. Para cada chave, há uma chave pública usada para autenticação por terceiros, armazenada num arquivo de mesmo nome, seguido do sufixo .pub. Por padrão, os arquivos ssh_host_rsa_key e ssh_host_dsa_key terão permissão -rw-----, e seus respectivos arquivos .pub terão permissão -rw-r--r--.

Na primeira vez que o cliente ssh conecta-se a um host, ele é questionado sobre aceitar uma chave pública. Se for aceita, ela será armazenada em ~/.ssh/known_hosts e garantirá a confiabilidade da conexão entre os dois hosts. O conteúdo desse arquivo pode ser incluído em /etc/ssh/ssh_known_hosts, para que a chave passe a valer para os demais usuários. Ainda assim será necessário que o usuário forneça sua senha ao host de destino.

Para evitar a necessidade de digitação da senha a cada login, pode-se criar um arquivo chamado authorized_keys, para que o ssh realize a autenticação de usuário via chave, no lugar de senha. O arquivo authorized_keys deve existir no host de destino, e pode conter uma ou mais chaves que foram criadas no host de origem através do comando ssh-keygen.

Para gerar uma chave DSA de 1024 bits:

```
$ ssh-keygen -t dsa -b 1024
```

Esse comando gerará as chaves id_dsa e id_dsa.pub em ~/.ssh/ no host de origem. O conteúdo de id_dsa.pub poderá então ser incluído em ~/.ssh/authorized_keys para o usuário específico no host de destino. Supondo que o host de destino tenha IP 192.168.1.1 e uma conta para o usuário com o mesmo nome, o arquivo pode ser copiado através do comando:

```
$ scp ~/.ssh/id_dsa.pub
➔ 192.168.1.1:~/.ssh/authorized_keys
```

Por questão de segurança, é importante que todos os arquivos contendo chaves em /etc/ssh/ e ~/.ssh/ tenham permissão 600 – escrita e leitura apenas para o dono do arquivo.

Tópico 114: Segurança

Objetivo 1.114.1: Tarefas Administrativas de Segurança

TCP wrappers

Daemons de serviços de rede compilados com suporte à biblioteca *Libwrap* podem utilizar-se do mecanismo chamado *TCP wrappers* para controlar o acesso por hosts na rede. Esse controle é estabelecido através de regras criadas nos arquivos /etc/hosts.allow e /etc/hosts.deny.

O arquivo /etc/hosts.allow contém as regras para os hosts que poderão acessar a máquina local. Se um host corresponder a uma regra em /etc/hosts.allow, o mesmo será liberado, e o arquivo /etc/hosts.deny não será consultado.

O arquivo /etc/hosts.deny contém as regras para os hosts que não poderão acessar a máquina local. Se um host não constar em /etc/hosts.allow nem em /etc/hosts.deny, o mesmo será liberado.

Cada regra é escrita em uma linha, com o mesmo formato (serviço: host:comando) para /etc/hosts.allow e /etc/hosts.deny: , onde:

- ◆ **serviço** é um ou mais nomes de daemons de serviço, ou instruções especiais;
- ◆ **host** é um ou mais endereços, ou instruções especiais, e;
- ◆ **comando** é um comando opcional a ser executado no caso de cumprimento da regra.

Hosts podem vir na forma de domínios, IPs de rede ou IPs incompletos. Caracteres curinga ? e * podem ser utilizados.

Instruções especiais são ALL, LOCAL, KNOW, UNKNOWN e PARANOID. O operador EXCEPT exclui um host ou grupo hosts de uma determinada regra.

Em /etc/hosts.allow, liberar todos os serviços a todos os hosts da rede 192.168.1.0, com exceção do 192.168.1.20:

```
ALL: 192.168.1.* EXCEPT
➔ 192.168.1.20
```

Bloquear todos os serviços a todo host que não constar em regra de /etc/hosts.allow, em /etc/hosts.deny:

```
ALL: ALL
```

A documentação completa para a criação de regras do *tcpwrappers* pode ser encontrada na página manual *hosts_access(5)*.

Exemplo 8: Encontrando arquivos SUID e SGID com o find

```
find / -perm -4000 -or -perm -2000
/bin/su
/bin/ping
/bin/mount
/bin/ping6
/bin/umount
(...)
```

SUID/SGID

Arquivos com permissão SUID e SGID garantem privilégios especiais a quem os executa. Portanto, é importante monitorar quais arquivos detêm essas permissões, para evitar que programas estranhos ou alterações nos programas conhecidos com essa permissão possam possibilitar a invasão ou dano ao sistema.

O exemplo 8 demonstra como encontrar arquivos SUID e SGID com o `find`, enquanto o exemplo 9 apresenta uma forma de se gerar uma lista detalhada no mesmo comando. Essa lista pode ser salva diariamente (provavelmente por um agendamento no `crontab`) através do comando:

```
# find / \( -perm -4000 -or -perm
# -2000 \) \
<del>exec ls -l '{ }' \; > /var/
# log/setuid</del>$(date +%F)
```

Esse comando gerará um arquivo de nome `setuid-ano-mês-dia`, que poderá ser comparado ao arquivo do dia anterior através do comando `diff`:

```
# diff /var/log/setuid-2006-05-02
# /var/log/setuid-2006-05-03
2c2
< <del>rws</del>-x--x 1 root bin
# 29364 2005-09-07 17:46 /bin/ping
---
> <del>rws</del>-x--x 1 root bin
# 29974 2005-09-07 17:46 /bin/ping
```

Essa saída mostra que o arquivo `/bin/ping` mudou de tamanho em relação ao registro anterior. Supõe-se que tenha sido substituído por um programa malicioso, devendo

Exemplo 9: Detalhando a lista gerada pelo exemplo 8

```
find / \( -perm -4000 -or -perm -2000 \) -exec ls -l '{ }' \;
-rws--x--x 1 root bin 35780 2004-06-21 16:20 /bin/su
-rws--x--x 1 root bin 29364 2005-09-07 17:46 /bin/ping
-rwsr-xr-x 1 root bin 61308 2005-09-13 01:42 /bin/mount
-rws--x--x 1 root bin 26764 2005-09-07 17:46 /bin/ping6
-rwsr-xr-x 1 root bin 32212 2005-09-13 01:42 /bin/umount
(...)
```

ser excluído e reinstalado adequadamente. É importante rastrear os logs do sistema atrás de possíveis origens dessa alteração.

Outras buscas por brechas no sistema podem ser realizadas pelos seguintes comandos:

```
# find / -path /dev -prune -perm -
# 2 -not -type l
```

Esse comando procura arquivos com permissão de escrita para todos os usuários, com exceção do diretório `/dev`. Arquivos de configuração do sistema poderiam ser alterados com intuito de viabilizar invasões ou danos ao sistema.

Para procurar arquivos sem dono ou sem grupo, que sugerem que o sistema tenha sido invadido, o comando apropriado seria:

```
# find / \( -nouser -o -nogroup \)
```

Verificação de pacotes

Semelhantemente à verificação nativa de pacotes `.deb` e `.rpm`, é possível verificar a maioria dos pacotes compilados ou de códigos-fonte fornecidos por um desenvolvedor. As maneiras mais comuns de verificação são a soma MD5 e as assinaturas PGP, cujas ferramentas estão disponíveis na maioria das distribuições.

Praticamente todos os pacotes de programas tradicionais oferecem assinaturas de verificação PGP, como o código-fonte do kernel do Linux, disponível em <ftp://ftp.kernel.org/pub/>. Além do arquivo `.tar.gz` ou `.bz2`, deve ser copiado um arquivo de mesmo nome, acrescido do sufixo

`.sign` (ocasionalmente esse arquivo aparece com o sufixo `.asc`). Para verificação, primeiro é necessário importar a chave pública referente ao kernel:

```
# gpg --keyserver wwwkeys.pgp.net
# --recv-keys 0x517D0F0E
```

Esse procedimento é necessário somente uma vez. A chave pública deve ser obtida somente de fonte confiável, especificada pelo próprio desenvolvedor do programa. Informações sobre obtenção da chave pública do kernel podem ser consultadas em <http://www.kernel.org/signature.html>.

Agora, a verificação do arquivo propriamente dito:

```
# gpg --verify linux-2.6.16.13.
# tar.bz2.sign linux-2.6.16.13.
# tar.bz2
gpg: Signature made Ter 02 Mai
# 2006 19:15:20 BRT using DSA key ID
517D0F0E
gpg: Assinatura correta de "Linux
# Kernel Archives Verification Key
# <ftpadm@kernel.org>"
```

Essa saída informa que o referido arquivo é autêntico.

De maneira mais simples agem as verificações MD5. Um arquivo com sufixo `.md5` correspondente ao arquivo `.tar.gz` ou `.bz2` contém um número referente ao resultado de cálculo envolvendo os bytes contidos no pacote. Para verificar a soma MD5 do pacote copiado `bluefish-1.0.5.tar.bz2`, através do seu arquivo MD5 correspondente `bluefish-1.0.5.tar.bz2.md5`:

```
# md5sum -c bluefish-1.0.5.tar.
# bz2.md5
```


bluefish-1.0.5.tar.bz2: A soma coincide

Como no caso das assinaturas PGP, é fundamental que o arquivo MD5 tenha sido copiado de fonte segura, indicada pelo próprio desenvolvedor do programa.

Senhas

As definições sobre a vida útil de senhas e aspectos relacionados são armazenadas no arquivo `/etc/shadow` (quando usado o sistema de senhas *shadow*). Cada linha corresponde a uma conta, em campos separados por `:`, representando:

- Nome de acesso;
- Senha criptografada;
- Dias decorridos entre 1º de janeiro de 1970 e a última alteração da senha;
- Número de dias até que a senha deva ser alterada;
- Número de dias após o qual a senha deve ser alterada;
- Número de dias antes da expiração da senha quando o usuário será avisado;
- Número de dias após a expiração da senha quando a conta deve ser bloqueada;
- Dias decorridos entre 1 de janeiro de 1970 e a data em que a conta foi bloqueada;
- Campo reservado.

Além de alterar senhas, o comando `passwd` também pode alterar essas definições, através das opções:

- `-x dias`: Número máximo de dias que a senha permanecerá válida;
- `-n dias`: Mínimo de dias até que o usuário possa trocar uma senha modificada;
- `-w dias`: Dias anteriores ao fim da validade da senha, nas quais será emitido um aviso a respeito da expiração de senha;
- `-i dias`: Inatividade, tolerância de dias após a senha ter expirado até que a conta seja bloqueada.

Por exemplo, para alterar as validades de senha para a conta “ataliba”:

```
# passwd -x 30 -n 1 -w 7 -i 7
# ataliba
```

A opção `-e` provoca a expiração imediata da senha e `-d` apaga a senha para a conta especificada.

Quando a opção `-g` é usada, a senha do grupo especificado é alterada; seguido de `-r`, remove a senha e, de `-R`, restringe o acesso a todos usuários. Essa tarefa só pode ser realizada pelo superusuário ou pelo administrador do grupo.

A conta especificada pode ser bloqueada através da opção `-l` e liberada pela opção `-u`. O estado da conta pode ser verificado fornecendo-se a opção `-S`:

```
# passwd -S ataliba
ataliba P 05/03/2006 1 30 7 7
```

Essa saída representa:

- **ataliba**: Login referente à conta;
- **P**: Um **P** significa que o usuário possui uma senha utilizável; **NP** significa que ele não possui qualquer senha; **L** representa uma conta bloqueada;
- **05/03/2006**: Data da última mudança de senha;
- **1**: Limite mínimo de dias da senha;
- **30**: Limite máximo de dias da senha;
- **7**: Dias de aviso
- **7**: Limite de dias de inatividade após a senha ter expirado até a conta ser bloqueada.

Os atributos da senha também podem ser alterados através do comando `chage`, através dos argumentos:

- `-m`: Mínimo de dias até que o usuário possa trocar uma senha modificada;
- `-M`: Número máximo de dias que a senha permanecerá válida;
- `-d`: Número de dias decorridos em relação a 01/01/1970 em que a senha foi mudada. Também pode ser expresso no formato de data local (*dia/mês/ano*);
- `-E`: Número de dias decorridos em relação a 01/01/1970 a partir do qual a conta não estará mais disponível. Também pode ser expresso no formato de data local (*dia/mês/ano*);
- `-I`: Inatividade, tolerância de dias após a senha ter expirado até que a conta seja bloqueada;
- `-W`: Dias anteriores ao fim da validade da senha nos quais será emitido um aviso a respeito.

Por exemplo, para determinarmos a data de bloqueio de uma conta, o comando adequado seria:

```
# chage -E 04/05/2006 ataliba
```

O uso do `chage` é restrito ao superusuário (root). Porém, usuários comuns podem usar o `chage` com a opção `-l` para checar as definições de suas respectivas contas, como mostra o **exemplo 10**.

Tanto `passwd` quanto `chage` entram em modo de configuração interativa se não forem passadas opções. O usuário assumido será sempre o

Exemplo 10: Verificação das definições de conta por um usuário comum

```
$ chage -l ataliba
Maximum:      30
Minimum:      1
Warning:      7
Inactive:     1
Last Change:  Mai 03, 2006
Password Expires: Jun 02, 2006
Password Inactive: Jun 03, 2006
Account Expires:  Abr 05, 2006
```

atual, caso um usuário não seja especificado como argumento.

Atualização de programas

Como nenhum programa é imune a falhas, é recomendado instalar todas as correções disponibilizadas pelos desenvolvedores. Programas desatualizados com falhas conhecidas são alvos fáceis para invasão e possível dano ao sistema.

Todas as principais distribuições mantêm atualizações para seus programas compilados. O anúncio das atualizações geralmente é feito através de email, recebido mediante cadastro no site da distribuição.

Grupos especializados em segurança também informam sobre falhas e procedimentos necessários para correção. O CERT (*Computer Emergency Response Team*) [3] e o BUGTRAQ [4] divulgam questões pertinentes a falhas e correções de sistemas.

Filtragem de Pacotes – iptables

A filtragem de pacotes de dados em rede permite controlar o fluxo das transmissões através de regras específicas. Dessa forma, é possível criar um *firewall* ou um redirecionamento do tipo NAT (*Network Address Translation*).

O programa utilizado para criação dessas regras é o *iptables*. É necessário que o kernel em uso seja capaz de trabalhar com filtragem de pacotes, o que é regra nos kernels recentes. O item de configuração do kernel para filtragem de pacotes é *Network Packet Filtering*.

Para cada tipo de operação há uma tabela específica. Cada tabela contém *chains* (correntes), onde são definidos *targets* (ações) para os pacotes que corresponderem a determinada regra na corrente. São as tabelas naturais *filter*, *nat* e *mangle*:

- ♦ **filter**: É a tabela padrão. Contém as chains embutidas *INPUT* (para pacotes que chegam ao

host local), *FORWARD* (para pacotes sendo roteados pelo host local) e *OUTPUT* (para pacotes gerados no host local). Essa é a tabela utilizada para construção de firewalls;

- ♦ **nat**: Para pacotes que criam novas conexões. Contém as chains embutidas *PREROUTING*, *OUTPUT* e *POSTROUTING*;

- ♦ **mangle**: Para alterações especializadas de pacotes. Contém as chains *INPUT*, *OUTPUT*, *PREROUTING*, *FORWARD* e *POSTROUTING*.

A tabela de atuação é indicada através da opção *-t* do comando *iptables*. Se nenhuma tabela for especificada, a tabela assumida será a *filter*. As operações dentro de uma *chain* são determinadas através dos seguintes argumentos-comando:

- ♦ **-A**: Adicionar regra na chain;
- ♦ **-I**: Inserir regra numa posição específica dentro da chain;
- ♦ **-R**: Substituir regra na chain;
- ♦ **-D**: Apagar chain;
- ♦ **-N**: Criar chain personalizada;
- ♦ **-X**: Apagar chain vazia;
- ♦ **-P**: Definir política para uma chain embutida;
- ♦ **-L**: Listar a(s) regra(s) inscritas em uma chain;
- ♦ **-F**: Apagar todas as regras em uma chain;
- ♦ **-Z**: Zerar os contadores de pacotes.

em todas as regras de uma chain. Especificações de regras (interceptam os pacotes que corresponderem a descrição dada):

- ♦ **-s <endereço>** ou **--source <endereço>**: Endereço de origem do pacote. Pode ser um nome de rede, nome de host, IP de rede/máscara de rede ou simplesmente um endereço IP. Se um endereço for precedido de *!*, a regra intercepta os pacotes que não correspondem à condição;
- ♦ **-d <endereço>** ou **--destination <endereço>**: Endereço de destino do pacote. Mesmo formato de *-s*. Se o endereço for precedido de *!*,

a regra intercepta os pacotes que não corresponderem à condição;

- ♦ **-p <protocolo>** ou **--protocol <protocolo>**: Define o protocolo. Pode ser *tcp*, *udp*, *icmp* ou *all*. Se o protocolo for precedido de *!*, a regra intercepta os pacotes que não corresponderem à condição;

- ♦ **-i <interface>** ou **--in-interface <interface>**: Interface através da qual o pacote chegou. Se o nome da interface for seguido do sinal *+* (*interface+*) aplicará a todas interfaces cujos nomes comecem por *interface*. Se o nome da interface for precedido de *!*, a regra intercepta os pacotes que não corresponderem à condição. Se *-i interface* não existir, todas as interfaces serão assumidas;

- ♦ **-o <interface>** ou **--out-interface <interface>**: Interface através da qual o pacote será enviado. Se o nome da interface for seguido do sinal *+* (*interface+*) aplicará a todas interfaces cujos nomes comecem por *interface*. Se o nome da interface for precedido de *!*, a regra intercepta os pacotes que não corresponderem à condição. Se *-i interface* não existir, todas as interfaces serão assumidas;

- ♦ **-j <ação>** ou **--jump <ação>**: Targets (ações) para o(s) pacote(s) interceptados.

Targets comuns para firewalls são:

- ♦ **ACCEPT**: Permite a passagem normal do pacote;
- ♦ **DROP**: Descarta o pacote;
- ♦ **-m <módulo>** ou **--match <módulo>**: Usar módulo estendido *módulo*. Há muitos tipos de módulos de controle adicionais e opções extras para cada um deles. Um muito usado para firewalls é o módulo *state*, cuja opção **--state <estado>** permite determinar qual a relação de um pacote com as conexões existentes. Possíveis valores para *estado* são *INVALID* (o estado não pode ser determinado), *ESTABLISHED*

SHED (o pacote pertence a uma conexão ativa), **NEW** (indicando que o pacote inicia nova conexão) e **RELATED** (o pacote inicia outra conexão, porém relacionada a uma conexão existente).

O **exemplo 11** demonstra o uso de algumas dessas opções do comando **iptables**, para a criação de um firewall simples. O firewall criado irá descartar qualquer tentativa de conexão por programas remotos, inclusive compartilhadores de arquivos e programas de mensagens instantâneas.

Para voltar à configuração padrão, aceitando indiscriminadamente todas as conexões, o conjunto de comandos a seguir deve ser empregado (respeitando-se as letras maiúsculas e minúsculas nas opções):

```
# iptables -t filter -F INPUT
iptables -t filter -P INPUT ACCEPT
iptables -t filter -F FORWARD
iptables -t filter -P FORWARD
➔ ACCEPT
iptables -t filter -F OUTPUT
iptables -t filter -P OUTPUT
➔ ACCEPT
```

Verificando portas abertas no sistema

O programa **nmap** é utilizado para rastrear sistemas em busca de portas de serviços ativos. Seu uso mais simples é sem argumentos, especificando apenas um nome ou endereço de host a ser rastreado, como mostra o **exemplo 12**.

A saída mostra que as portas 631/tcp (Serviço de impressão do CUPS) e 6000/tcp (servidor de janelas X) estão abertas a conexões. Portanto, é funda-

mental estabelecer restrições ao seu uso através da configuração do **tcpwrapper**, ou através da configuração do próprio **daemon** do serviço.

O **nmap** possui muitas opções de rastreamento que podem ser consultadas através de sua página manual (**man nmap**). É possível, por exemplo, fazer um rastreamento para tentar descobrir as portas passíveis de conexão e qual o sistema operacional do host em questão, conforme mostra o **exemplo 13**.

Um programa que desempenha função semelhante é o **netstat**. Entre outras funções, com o **netstat** é possível monitorar as conexões ativas. Algumas opções do **netstat**:

- **-t**: Mostra todas as conexões TCP ativas;

Exemplo 11: Criação de um firewall simples

Apagar todas as regras da tabela filter:

```
iptables -t filter -F
```

Estabelecer política de descartar todos os pacotes em todas as chains da tabela filters:

```
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT DROP
```

Liberar todos os pacotes (saindo e entrando) da interface local:

```
iptables -t filter -A INPUT -i lo -s 0/0 -d 0/0 -j ACCEPT
iptables -t filter -A OUTPUT -o lo -s 0/0 -d 0/0 -j ACCEPT
```

Liberar todos os pacotes saindo através da interface eth0:

```
iptables -t filter -A OUTPUT -o eth0 -s 0/0 -d 0/0 -j ACCEPT
```

Liberar para entrar pela interface eth0 somente os pacotes pertencentes (ESTABLISHED) ou relacionados (RELATED) a uma conexão existente:

```
iptables -t filter -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED \
-s 0/0 -d 0/0 -j ACCEPT
```

Listando as novas configurações de filtros:

```
iptables -t filter -L -v
Chain INPUT (policy DROP 39 packets, 12431 bytes)
  pkts bytes target    prot opt in     out     source    destination
    0    0 ACCEPT    all  --  lo     any     anywhere  anywhere
    0    0 ACCEPT    all  --  eth0   any     anywhere  anywhere
➔state RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy DROP 12 packets, 816 bytes)
  pkts bytes target    prot opt in     out     source    destination
    0    0 ACCEPT    all  --  any    lo     anywhere  anywhere
    0    0 ACCEPT    all  --  any    eth0   anywhere  anywhere
```


- ▶ -l: Mostra todas as portas abertas a conexões;
- ▶ -c: Execução contínua, renova as informações a cada segundo.

O `netstat` é capaz de obter e mostrar várias outras informações (tabelas de rotas, estatísticas de interface etc.). Mais detalhes sobre sua operação podem ser consultados na página manual (`man netstat`).

Objetivo 1.114.2: Segurança do Host

syslog

Em geral, todas as mensagens do serviço de sistema `syslog` são importantes para checar e garantir o bom funcionamento do sistema. Porém, a facilidade `authpriv` é especialmente importante, pois é responsável por informar questões relativas à mudança e autenticação de usuários. Configuração de `authpriv` no arquivo `/etc/syslog.conf`:

```
authpriv.* /var/log/secure
```

Essa entrada fará com que todas as mensagens relativas a `authpriv` sejam armazenadas no arquivo `/var/log/secure`.

É importante que os arquivos de log críticos em `/var/log/*` não possam ser lidos ou escritos por usuários comuns. Portanto, devem ter a permissão octal 600 (`-rw-----`).

Algumas mensagens mais graves são enviadas por email para o usuário `root`. Para que outro usuário também receba essas mensagens de segurança, basta acrescentá-lo como um alias de `root` em `/etc/aliases` (ou `/etc/mail/aliases`):

```
root: ataliba, palimercio
```

Para que o redirecionamento tenha efeito, deve ser executado o comando `newaliases`.

No exemplo, as mensagens de segurança destinadas a `root` serão enviadas para os usuários `ataliba` e `palimercio`

(que devem ser nomes de contas de usuários existentes no sistema).

Sistema de senhas shadow

O uso do sistema de senhas `shadow` proporciona maior segurança, visto que o arquivo onde as senhas são armazenadas (`/etc/shadow`) não oferece leitura para usuários comuns (`-rw-r-----`) e essas estão sob forte criptografia.

O uso de senhas `shadow` é verificado pela letra `x` no campo de senha do usuário em `/etc/passwd`. Caso o sistema não use senhas `shadow`, é necessário instalar o pacote `shadow password suite` (já presente na grande maioria das distribuições) e executar o comando `pwconv` para converter as senhas antigas para o novo formato.

Desativando serviços de rede

Daemons de serviços de rede que não estão sendo utilizados representam um risco adicional de invasões que pode ser evitado. Uma das maneiras de desativar servidores desnecessários é

Certificação Linux Número 1 no Mundo



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



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



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



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



Linux
Professional
Institute

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

Exemplo 12: Saída do comando nmap

```
$ nmap localhost
```

```
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2006-05-08 01:39 BRT
Interesting ports on localhost (127.0.0.1):
(The 1666 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
631/tcp   open  ipp
6000/tcp  open  X11
```

Exemplo 13: Uso detalhado do nmap

```
# nmap -sS -O localhost
```

```
Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2006-05-08 01:50 BRT
Interesting ports on localhost (127.0.0.1):
(The 1666 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
631/tcp   open  ipp
6000/tcp  open  X11
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.6.3 - 2.6.7 (X86)

Nmap finished: 1 IP address (1 host up) scanned in 3.240 seconds
```

tirar a permissão de execução do script que os inicia. Primeiro, o serviço deve ser terminado, e depois executado o comando `chmod -x script`.

Para serviços disparados pelo servidor *inetd*, basta comentar (acrescentar o caractere `#`) à linha referente ao serviço em `/etc/inetd.conf`.

Por exemplo, para desativar o servidor *telnet* em `/etc/inetd.conf`:

```
#telnet stream tcp      nowait
#root  /usr/sbin/tcpd  in.telnetd
```

De forma semelhante, os serviços controlados pelo servidor *xinetd* podem ser desativados no arquivo de configuração `/etc/xinetd.conf`, na opção `disable` correspondente ao serviço.

Para desativar o servidor FTP em `/etc/xinetd.conf`, a entrada correspondente no arquivo seria:

```
ftp {
    disable = yes
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    server = /usr/sbin/vsftpd
}
```

Objetivo 1.14.3: Segurança a Nível de Usuário

Além do cuidado com as permissões e senhas do usuário, controlados com as ferramentas *passwd*, *usermod*, *umask* etc., outras medidas podem ser tomadas para aumentar a disponibilidade da máquina, seja ela uma estação ou servidor.

Usuários comuns podem provocar lentidão e até panes no sistema se utilizarem exageradamente os recursos da máquina. Semelhante ao controle de espaço em disco exercido através do uso de cotas, os limites de memória, a criação de arquivos e os processos também podem ser limitados através do comando `ulimit`.

O `ulimit` é um comando embutido no *bash*. Os limites são válidos para a sessão do *shell* atual, assim como para sessões e processos disparados a partir dela. Geralmente, os limites são estabelecidos no login, através do arquivo `/etc/profile`.

Para cada recurso, pode ser estipulado um limite *soft* e um limite *hard*, especificados pelas opções `-S` e `-H`, respectivamente. O limite *hard* não poderá ser aumentado, e o limite *soft* poderá ser

aumentado até o limite *hard*. Se não for especificado `-S` ou `-H`, o limite indicado será definido para ambos.

Opções comuns de `ulimit`:

- ◆ `-a`: Mostra os limites atuais;
- ◆ `-f`: Especifica o número máximo de arquivos que poderão ser criados pelo shell;
- ◆ `-u`: O número máximo de processos disponíveis ao usuário;
- ◆ `-v`: O montante máximo de memória virtual disponível ao shell

Para se estabelecer em 100 o limite máximo de processos:

```
ulimit -Su 100
```

Permitir que o usuário acresça esse limite até o máximo de 200:

```
ulimit -Hu 200
```

Se nenhuma opção for fornecida, o recurso assumido será `-f` (limite de arquivos criados). Sem um valor de limite, `ulimit` mostrará o limite *soft* atual para a opção fornecida.

Considerações finais

Apenas as configurações mais fundamentais do Samba serão exigidas para a prova, como compartilhar o diretório do usuário e impressoras. Quanto ao NFS, é necessário conhecer a sintaxe do arquivo `/etc/exports` e a utilização do comando `exportfs`.

Em relação a segurança, aparecerão na prova questões como bloqueio de serviços e inspeção de pacotes instalados. Alguns comandos pouco conhecidos também são abordados, como `chage` e `ulimit`. ■

Mais Informações

- [1] Internic: <http://www.internic.net/>
- [2] Fapesp, Registro-BR: <http://www.registro.br/>
- [3] CERT: <http://www.cert.org>
- [4] BUGTRAQ: <http://www.securityfocus.com>

O novo sistema de arquivos Ext4

Pronto para o futuro

O próximo sistema de arquivos da família Ext oferece melhor desempenho e sistemas de arquivo maiores. Você está preparado para o Ext4?

por Marcel Hilzinger



Daniel Jaeger Vendruscolo - www.sxc.hu

O Linux ganhou muito com a introdução do Ext2, e o Ext3 foi o primeiro sistema de arquivos com *journal* a entrar no kernel. Ao longo dos anos, a família Ext (*Extended*, estendida) de sistemas de arquivo teve um importante lugar no Linux, e continua sendo uma escolha bastante popular por parte dos usuários ao redor do mundo. Porém a venerável base de código por trás do Ext está mostrando sinais da idade. Vários meses atrás, desenvolvedores começaram a debater o problema de acrescentar novos recursos ao Ext3, mantendo sua estabilidade e a compatibilidade com códigos mais antigos[1].

Enquanto isso, diversas iniciativas ofereciam a esse sistema de arquivos avanços fundamentais demais para serem facilmente integrados ao código, porém importantes demais para serem ignorados.

A solução proposta pelos desenvolvedores foi a realização de

um *fork* do código, com a consequente criação do Ext4. Essa estratégia permite que os usuários por todo o mundo continuem usando o Ext3 estável, enquanto os desenvolvedores integram e testam uma nova rodada de melhorias. O Ext4, próxima geração

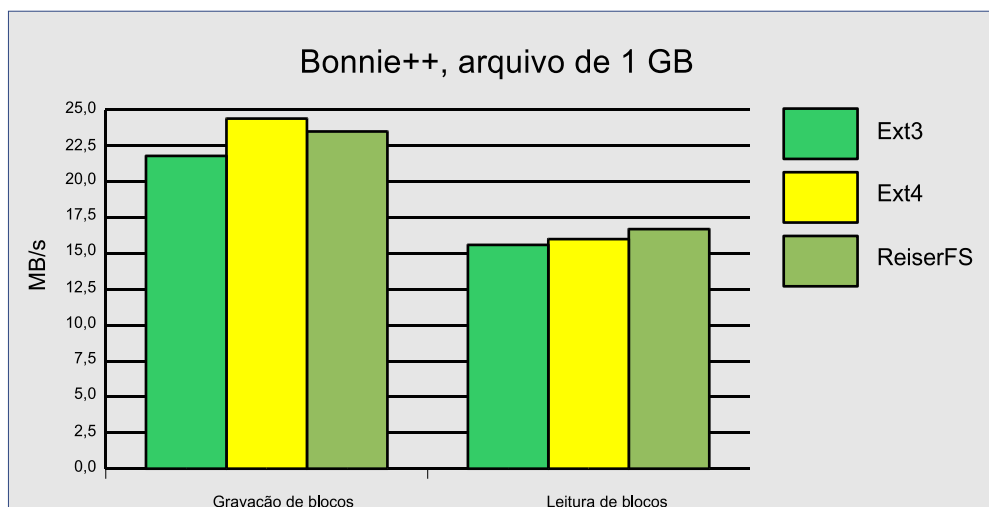


Figura 1 O Ext4 grava um arquivo de 1 GB mais rápido que o ReiserFS em uma operação de gravação em bloco. O Ext4 é bem mais rápido que o Ext3.

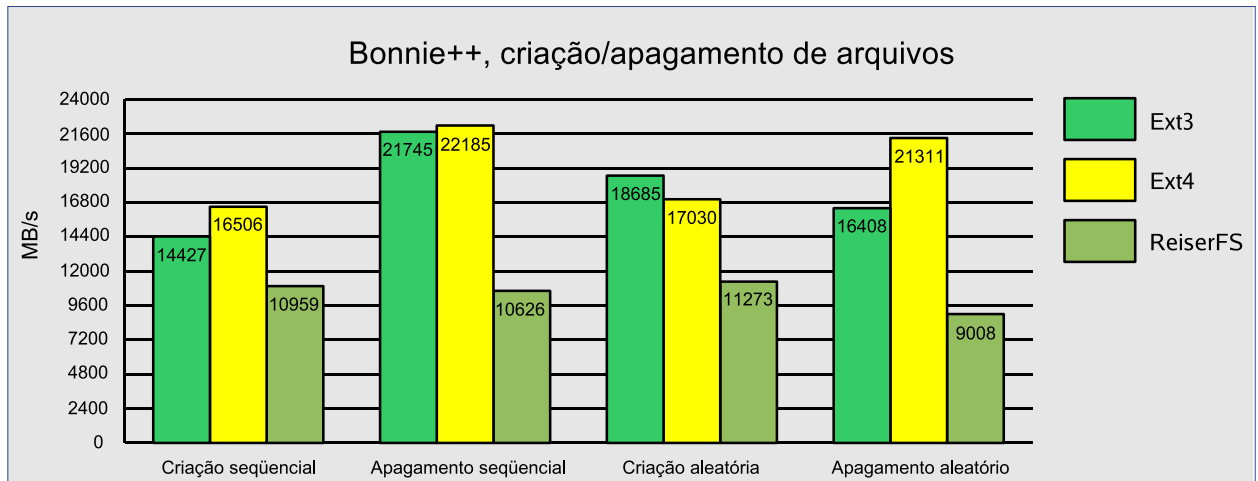


Figura 2 Um teste de resistência da *Bonnie++* avalia quantos arquivos o sistema de arquivos consegue criar ou apagar em um segundo. O Ext4 alcança as melhores marcas.

do *Extended filesystem*, agora já está disponível para os usuários. Nós avaliamos como ele se compara a outras opções populares de sistemas de arquivos.

O que muda?

O Ext4 se encaminha a um melhor suporte a ambientes de 64 bits, o que leva a várias outras melhorias. Um importante benefício mostrado por ele é o aumento no tamanho máximo de arquivo. No Ext3, esse valor era de 8 TB (com um tamanho de bloco padrão, com 4 KB), que um dia já foi considerado gigantesco. No entanto, o hardware atual aceita maiores valores com folga. O Ext4 agora suporta sistemas de arquivos com até 1024 PB (petabytes).

Outra importante mudança no Ext4 é seu uso de *extents*, áreas contíguas de espaço de disco adicional que contêm arquivos. O propósito de um extent é garantir que alterações subseqüentes ao arquivo sejam armazenadas na mesma localização que o arquivo original. Os extents reduzem a fragmentação e melhoram a velocidade de gravação. Vários outros sistemas de arquivos populares, como *Reiser4*, *NTFS* e o *HFS* da Apple já oferecem esse suporte.

A retrocompatibilidade também foi um dos objetivos dos desenvolvedores do Ext4: é possível montar partições Ext4 como Ext3, e também se pode montar uma Ext3 como Ext4 (com *ext4dev* como sistema de arquivos). Infelizmente, para atingir esse nível de compatibilidade, é necessário desativar o recurso de extents do Ext4, que é um de seus maiores benefícios de desempenho.

Os interessados em testar o novo sistema de arquivos necessitarão de um kernel atual e das ferramentas de desenvolvimento comuns: *make*, *GCC* e *glibc-devel*. Em nosso laboratório, usamos o kernel 2.6.20.

Além do suporte ao *ext4dev*, recomenda-se configurar no kernel o suporte a recursos como *ACLs* e atributos estendidos (*Extended attributes* ou *XATTR*). Em relação à opção por compilar essas opções embutidas no kernel ou como módulos, isso fica a cargo do usuário. Para incluir o suporte ao *SELinux*, será necessário acrescentar também o suporte a rótulos de segurança (*Security labels*).

O suporte à depuração de *JBD2* torna o sistema de arquivos sensivelmente mais lento; portanto, é uma boa idéia excluir esse recurso do seu kernel.

Usando o Ext4

Após compilar o novo kernel (não se esqueça da opção *-j*, caso possua uma máquina multiprocessada) e configurar adequadamente o gerenciador de inicialização, vamos começar os testes em uma partição real.

Para criar uma partição Ext4, é necessária uma versão recente do pacote *e2fsprogs*[2]. Se sua distribuição não disponibilizar uma versão suficientemente nova, é possível baixar o código-fonte do pacote em [2] e realizar a compilação com os tradicionais `./configure && make && make install`. Se algum erro ocorrer na etapa do *make*, provavelmente isso significa que é necessário instalar o pacote *texinfo* no sistema antes de tentar novamente essa compilação.

A criação de uma nova partição Ext4 é feita com `mke2fs -j <partição>`, obviamente substituindo *<partição>* pelo arquivo de dispositivo pertinente. Também é possível usar uma interface gráfica para criar uma nova partição Ext3. Depois disso, basta montar a partição com `mount -t ext4dev <partição> <ponto de montagem>`. O kernel deve carregar o módulo *ext4dev* automaticamente.

Se o objetivo for utilizar o recurso de extents do sistema de ar-

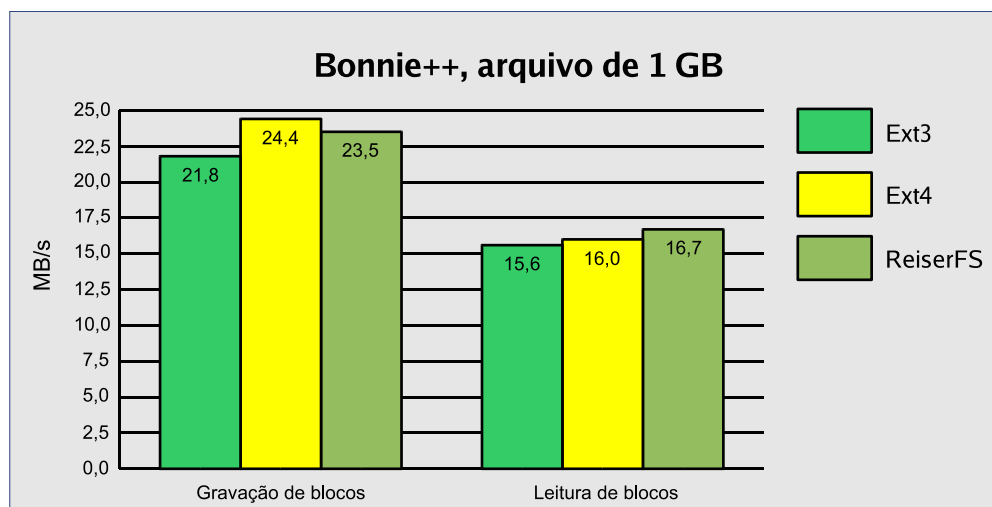


Figura 3 Sem extents, o Ext4 fica muito mais lento nas gravações, descendo ao mesmo nível que o Ext3.

quívos, é necessário passar o parâmetro `-o extents` para o comando `mount`. É importante lembrar que uma partição montada com extents não poderá ser montada como Ext3 posteriormente. Por isso, é fundamental não montar uma partição Ext3 pré-existente com `-o extents`. Caso você cometa esse erro, a única forma de não causar problemas é desmontar a partição sem realizar alterações nela.

Os desenvolvedores têm planos de migrar o suporte a extents para as ferramentas `mke2fs` e `tune2fs` no futuro, eliminando assim a necessidade da opção no momento da montagem de partições.

Além dessas opções, o Ext4 suporta parâmetros de montagem mais familiares para sistemas de arquivos com `journal`. No caso de laptops, a opção `-o commit=<segundos>` também pode ser interessante. O intervalo especificado em `<segundos>` determina a frequência com que o Ext4 gravará dados no disco. O valor padrão é a cada cinco segundos. Valores maiores aumentam o desempenho e também podem economizar energia. Entretanto, note que isso compromete a segurança de qualquer dado que ainda não tenha sido salvo. Dito isso, nossos *benchmarks* não re-

velaram diferenças significativas entre `commit=5` e `commit=60`.

Em nossos primeiros testes com a versão de desenvolvimento do Ext4, medimos seu desempenho com os benchmarks *Bonnie++* [3] e *Slow.c* [4]. A distribuição utilizada foi o *OpenSuse* 10.2, com um kernel personalizado e o `ext4dev` como módulo. Nos testes, foi utilizada a opção de montagem `-o extents`, a menos que esteja especificado o contrário. Todos os outros sistemas de arquivos utilizaram parâmetros padrão.

O Ext4 alcança velocidades de gravação muito maiores que seus antecessores, e de fato ultrapassa, pela primeira vez, seu concorrente direto *ReiserFS* (figura 1) em operações de gravação por blocos. Dito isso, o *ReiserFS* ainda é um pouco mais veloz que o Ext4 na leitura. Para criação e apagamento sequenciais de arquivos, o novo sistema de arquivos não é muito mais rápido que seu antecessor Ext3 (figura 2).

Os efeitos dos extents quanto ao desempenho são claramente demonstrados pelos resultados do teste de “Criação aleatória”. É compreensível o Ext4 perder para o Ext3 nessa rodada, pois ele necessita de tempo extra para reservar espaço de armazenamento

para os próprios extents. Esse trabalho adicional não é necessário ao se apagar arquivos, o que fica evidente quando o Ext4 ultrapassa tanto o *ReiserFS* quanto o Ext3, como mostram os *stress tests* do *Bonnie++*.

A figura 3 finalmente mostra a velocidade do Ext4 sem extents, no benchmark *Slow.c* com

um arquivo de 1 GB. Os resultados mostram que o desempenho excepcional de gravação desse sistema de arquivos é resultado principalmente dos extents.

Conclusões

O Ext4 é um sistema de arquivos veloz que ainda se encontra em estágio inicial de desenvolvimento. Apesar de a retrocompatibilidade apenas parcial poder causar certa confusão, ela não representa motivo para evitar o uso do Ext4. No entanto, o fato de ainda chamarem o sistema de `ext4dev` provavelmente significa que faz sentido permanecer um pouco mais com o Ext3. ■

Mais Informações

- [1] Proposta do Ext4:
<http://lkml.org/lkml/2006/6/28/454>
- [2] E2fsprogs:
<ftp://ftp.kernel.org/pub/linux/kernel/people/tytso/e2fsprogs-interim/>
- [3] *Bonnie++*:
<http://www.coker.com.au/bonnie++/>
- [4] *Slow.c*:
<http://www.jburgess.uklinux.net/slow.c>

Virtualização com o VirtualBox

Caixinha virtual

Se você quer fugir das ferramentas de virtualização muito complexas ou caras, experimente o VirtualBox.

por Thomas Leichtenstern



A virtualização vem ganhando popularidade como técnica para simplificar a administração de sistemas. As ferramentas de virtualização simulam uma máquina autônoma independente do sistema hospedeiro.

Infelizmente, vários programas de virtualização são caros, como

algumas versões do VMware[1], ou difíceis de usar, como o Xen. Alternativas como o Qemu geralmente não conseguem oferecer desempenho adequado em ambientes de produção.

A empresa alemã Innotek[2] recentemente deu um passo à frente no preenchimento desse nicho, lançando seu sistema de virtualização VirtualBox[3] sob a GPL (veja também o quadro 1). A empresa descreve o VirtualBox como uma ferramenta gratuita e amigável, que oferece suporte a uma grande variedade de sistemas hóspedes e hospedeiros.

Podem ser hóspedes do VirtualBox todas as distribuições Linux populares, além dos BSD's, o OS/2 e qualquer

sistema Windows® (incluindo o Vista). Os sistemas hospedeiros incluem o Windows XP e distribuições Linux com kernel 2.4 ou posterior, mas apenas em plataformas de 32 bits (aparentemente, há uma versão para 64 bits em desenvolvimento). Testamos a versão 1.3.8 do VirtualBox (a mais recente até o fechamento deste artigo), para verificar se o programa corresponde aos ambiciosos objetivos de seus desenvolvedores.

Recursos

Diferentemente do VMware Workstation, o VirtualBox não gerencia máquinas virtuais como abas dentro de uma janela; em vez disso, ele mostra os sistemas hóspedes em múltiplas janelas independentes (figura 1). Mas há semelhanças entre as duas ferramentas: assim como o VMware, o VirtualBox trata os sistemas virtuais como instâncias independentes.



Figura 1 O VirtualBox abre máquinas virtuais como instâncias independentes em janelas separadas, permitindo que o usuário rode diferentes sistemas operacionais ao mesmo tempo.

O VirtualBox emula um computador com chipset *Intel 440FX* (“Natomia”), placa de rede *AMD 79C973* (*PCnet-II*), chip de som *Intel AC97* e um adaptador VGA com memória de vídeo configurável até 32 MB. Os desenvolvedores pretendem integrar uma placa de rede Gigabit virtual da Intel.

Uma barra permite o ajuste da quantidade de memória até o limite da memória física. Como as máquinas virtuais rodam como processos normais no sistema hospedeiro, o escalonador deste fica responsável por alocar ciclos de CPU. No momento, o VirtualBox ainda não possui gerenciamento centralizado de processos para as máquinas virtuais, mas o objetivo é incluí-lo por volta do meio do ano. O suporte nativo a imagens do VMware está planejado para antes do meio do ano.

Assim como o VMware, o VirtualBox também possui um gerenciador de *snapshots* que permite que o usuário paralise e recupere o status de um sistema ativo, a qualquer momento.

Há um servidor RDP que pode ser ativado individualmente para qualquer sistema hospedeiro para suportar o acesso gráfico através de redes.

Instalação

A página de download na homepage do VirtualBox possui pacotes com os binários do *Debian* (3.1 e 4.0), *Ubuntu* (6.06 LTS até 7.04), *OpenSuse* 10.2, *Mandriva* 2007.1 e *RHEL* 4. Os usuários de outras distribuições podem usar o script genérico de instalação, que também inclui os binários.

Como o VirtualBox requer um módulo do kernel, será necessário o código-fonte do kernel e seus cabeçalhos, além do *make* e do GCC. O VirtualBox compila o módulo a partir dos fontes, a menos que o usuário

já possua um módulo adequado disponível. O software também necessita da versão 3.3.5 ou mais recente das bibliotecas *Qt*, assim como da biblioteca multimídia *SDL* 1.2.7 ou mais nova.

Os usuários das distribuições atendidas pelos pacotes nativos podem utilizar seu gerenciador de pacotes preferido para realizar a instalação do VirtualBox. Já a instalação genérica requer que o usuário root execute o script de instalação com o argumento *install*.

A rotina de instalação cria um grupo chamado *vboxusers*. Em sistemas Ubuntu e Debian é necessário acrescentar a eles, manualmente, os usuários aptos a utilizar o VirtualBox, com um *usermod -G vboxusers -a <usuário>*. Em sistemas como o Suse ou o Mandriva, o comando é *usermod -A vboxusers <usuários>*. Note que usuários logados precisam sair e entrar novamente para aplicar as novas configurações de grupos.

O script de instalação cria automaticamente uma entrada para iniciar o serviço do *vboxdrv* em */etc/init.d/*, eliminando a necessidade de iniciar o serviço ao iniciar a máquina hospedeira. Pode-se controlar o serviço com o script de inicialização */etc/init.d/vboxdrv*, passando-lhe argumentos como *start*, *stop* e *restart*.

O suporte a USB é baseado no sistema de arquivos virtual *USBFS*. Como o OpenSuse 10.2 não

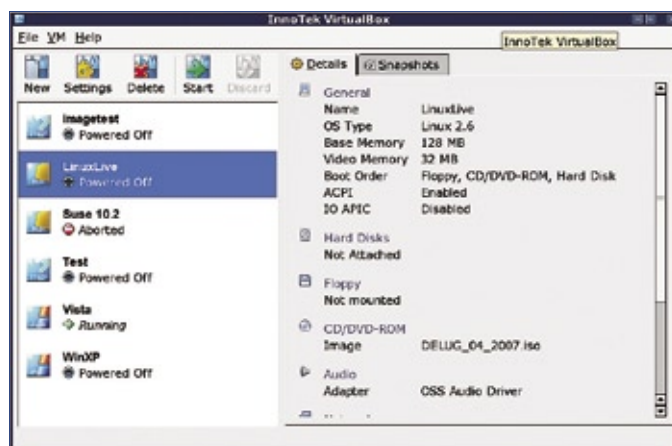


Figura 2 A interface gráfica do VirtualBox é simples e limpa.

possui suporte a esse sistema de arquivos por motivos de segurança, os usuários dessa distribuição precisam instalar um kernel diferente, ou então simplesmente não utilizar USB nos sistemas virtuais.

Os usuários de outras distribuições precisarão modificar os pontos de montagem em */etc/fstab* para ter certeza de que o software possui os direitos de acesso necessários para o *USBFS*. Para fazer isso, abra o */etc/fstab* como root e procure a entrada que monta o *USBFS*, como:

```
usbfs /proc/bus/usb usbfs noauto 0 0
```

Acrescente a seguinte linha a essa entrada:

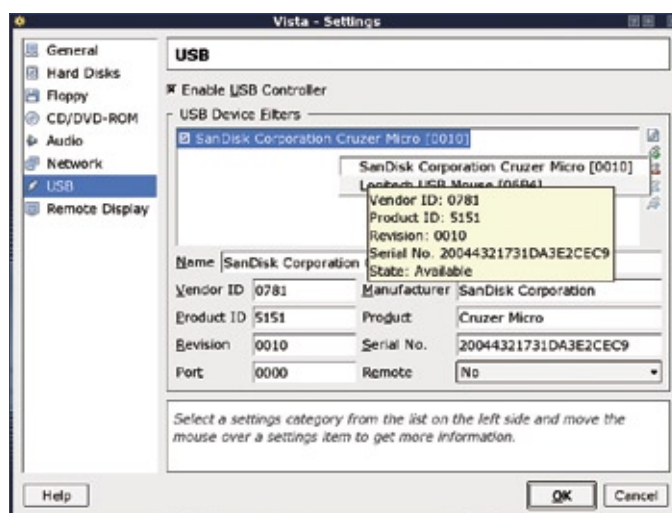


Figura 3 O VirtualBox exibe os nomes dos dispositivos USB do hospedeiro, e permite seu uso na máquina virtual.

Quadro 1: Questões de licenciamento

A Innotek oferece dois “sabores” do VirtualBox: a *Open Source Edition (OSE)*, com código-fonte sob a GPL, e a versão binária de código fechado, lançada sob a *VirtualBox Personal Use and Evaluation License*.

A empresa permite que se use essa variante com propósitos pessoais e acadêmicos, gratuitamente; todos os outros usos estão sujeitos ao pagamento de uma licença, após um “razoável” período de avaliação de “algumas semanas”. A vantagem da variante paga é que ela oferece recursos valiosos, como diretórios compartilhados e suporte a USB, RDP e iSCSI.

```
usbfs /proc/bus/usb usbfs devgid=
<GID_do_grupo_vboxusers>,de
vmode=664,noauto 0 0
```

Após um `mount usbfs`, os preparativos já estão terminados, e é possível rodar o VirtualBox. Porém, no caso do OpenSuse 10.0, que ignora as instruções para o sistema de arquivos USBFS presentes em `/etc/fstab`, é necessário remontar o USBFS com um pequeno script que pode ser executado na inicialização:

```
#!/bin/bash
/bin/umount usbfs
/bin/mount usbfs
exit 0
```

Salve o script como `usbfsstart.sh` em `/etc/init.d/`, e crie um link simbólico para o diretório de `runlevel` adequado (normalmente, `/etc/init.d/rc5.d/`).

Configurações

Para iniciar a interface gráfica do VirtualBox (**figura 2**), é possível selecionar tanto *Sistema | Innotek | VirtualBox* no menu do seu ambiente desktop, quanto digitar `VirtualBox` (`virtualbox`, no Gentoo) na linha de comando; não são necessários privilégios de root.

As configurações globais (*Global Settings*), como os diretórios padrão (*Default Folders*) de imagens e snap-

shots, ou *Hostkey* para deixar a máquina virtual (que por padrão é a tecla **[Ctrl]** direita) estão disponíveis no menu *File | Global Settings*.

Para criar uma nova máquina virtual, clique no menu *VM* e em seguida no botão *New*. Isso inicia o *Virtual Machine Wizard*, um assistente para configurar parâmetros como o nome da máquina virtual, o espaço em disco que ela poderá utilizar e a alocação de memória, além de se especificar o sistema operacional hospede.

Como o VirtualBox não verifica o espaço disponível na partição física ao criar discos dinâmicos, é necessário certificar-se de que há espaço físico suficiente antes de informar um tamanho de disco virtual para a criação de uma nova máquina.

Ao se configurar a memória, também é necessário tomar cuidado, pois o software de cada máquina virtual vai usar sua memória alocada de forma exclusiva. Se forem iniciadas múltiplas máquinas virtuais que, em conjunto, ultrapassem o espaço de memória disponível, uma das máquinas pode vir a travar ou fechar, e até mesmo os processos do hospedeiro podem vir a ser terminados.

Clicar em *Finish* informa o *Virtual Machine Wizard* para acrescentar a nova máquina virtual com os parâmetros básicos especificados para a lista de máquinas virtuais de-

finidas (**figura 2**). No lado direito da janela, há mais configurações para a máquina virtual, na aba *Details*. É possível ativar mais funções, como o suporte a áudio (as opções são *ALSA* e *OSS*), a quantidade de memória de vídeo (configurável até 32 MB), e compartilhamentos RDP.

O software possui uma abordagem muito interessante para o gerenciamento de dispositivos USB (**figura 3**). Para listar todos os dispositivos USB ligados à máquina, junto com seus descritores de fabricante e produto, apenas clique no ícone *Add from*, na barra de ferramentas do lado direito.

Para usar o dispositivo necessário na máquina virtual, basta clicar nele. O menu *Remote* permite aos usuários especificar se desejam compartilhar o dispositivo para uso remoto (via USB sobre RDP). Se essa opção for ativada, é possível plugar um dispositivo, como um pendrive, por exemplo, ao computador remoto em uma sessão RDP, e acessar o dispositivo pela máquina hospede.

Em nosso laboratório, o suporte a USB causou alguns efeitos colaterais incomuns. Em um dos casos, o mouse USB do sistema hospede parou de funcionar após iniciarmos uma máquina virtual, voltando apenas após desligarmos o sistema hospede e recarregarmos



Figura 4 A função de redimensionamento automático do desktop modifica automaticamente o tamanho da janela do sistema hospede, de acordo com o tamanho da janela.

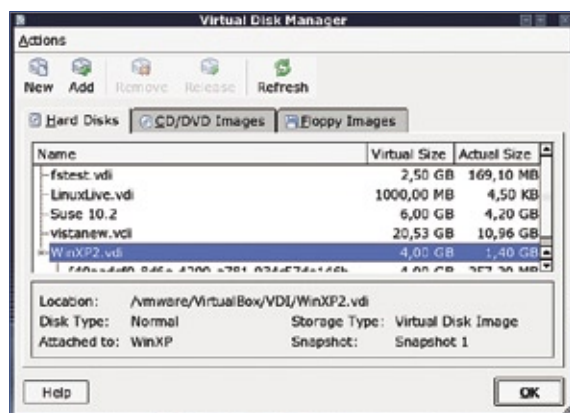


Figura 5 O *Virtual Disk Manager* é responsável pelo gerenciamento de discos e imagens de discos usados pelo *VirtualBox*.

os módulos do kernel responsáveis pelos controladores USB. Em outro, o sistema hóspede recusou-se a colaborar com pendrives que o sistema operacional normalmente detectaria sem qualquer problema.

Operações e funções

Diferente do que acontece no VMware, as máquinas virtuais no VirtualBox não têm uma BIOS separada, em vez disso, é necessário usar a interface de configuração para algumas operações, como alterar a ordem de inicialização dos discos. Na parte inferior da janela da máquina virtual, alguns ícones mostram o status dos dispositivos ativos, assim como o da rede e das unidades removíveis e fixas. Um clique direito no ícone de CD ou USB mostra um menu de contexto que permite a montagem ou desativação de unidades de disco e dispositivos, dinamicamente.

O redimensionamento automático do hóspede modifica o tamanho de sua respectiva janela, para adequar-se à resolução da tela (**figura 4**). A seta verde no ícone do desktop da barra de ferramentas informa se essa função está ativa, e um clique com o botão direito pode ativá-la ou desativá-la. Para usá-la, é necessário instalar os recursos extras para hóspedes (*guest add-ins*). Para montar

sário configurar os fontes e cabeçalhos do kernel manualmente. Os add-ins também habilitam o cursor do mouse automático ao alternar entre as máquinas virtuais e o sistema hospedeiro. O VirtualBox não suporta cópias do tipo *arrastar-e-soltar* entre o hóspede e seu hospedeiro.

A interface gráfica do VirtualBox é simplesmente uma forma conveniente de se controlar a base da ferramenta de virtualização, em modo texto. Algumas configurações como os diretórios compartilhados para todas as máquinas virtuais, só estão disponíveis através da linha de comando.

O comando `VBoxManage`, sem qualquer parâmetro, lista os comandos disponíveis. Para configurar um compartilhamento, basta digitar `VBoxManage sharedfolder add <hóspede> -name <nome do compartilhamento> -path <caminho/até/o/diretório>`. Para isso, novamente serão necessários os *guest add-ins*.

Discos virtuais

O VirtualBox gerencia discos independentemente das máquinas virtuais, através do *Virtual Disk Manager* (**figura 5**), acessível através do menu *File*, na janela principal. O programa exibe discos virtuais na aba *Hard Disks*, sem

importar em que diretórios eles estejam fisicamente.

Para usar discos em máquinas virtuais às quais eles estejam vinculados, basta clicar no botão *Release*. Com isso, o disco aparecerá no menu de seleção de discos das outras máquinas virtuais. Para criar um novo disco independente, para ficar disponível a todas as máquinas virtuais, pode-se clicar no botão *New*. A aba *CD/DVD Images* lista as imagens ISO que tenham sido montadas em alguma máquina virtual, em algum momento.

Conclusões

Apesar de alguns bugs pouco importantes, o VirtualBox cria uma impressão favorável e oferece bom desempenho. A única crítica importante é o suporte falho a USB, mas para compensar isso, essa ferramenta possui uma excelente solução de gerenciamento de discos virtuais e imagens de CD-ROM. O suporte a RDP e iSCSI, além da função de USB sobre RDP, por exemplo, ainda estão ausentes nos concorrentes.

Os desenvolvedores prometem melhorias impressionantes para a próxima versão. Além do controle de processos de uma função de importação para imagens do VMware, as mudanças incluirão uma interface gráfica para gerenciar compartilhamentos virtuais. Considerando que uma licença do VMware para uso doméstico custa US\$ 189,00, o gratuito VirtualBox é uma boa escolha em muitas situações. ■

Mais Informações

- [1] VMware:
<http://www.vmware.com>
- [2] Innotek:
<http://www.innotek.de>
- [3] VirtualBox:
<http://www.virtualbox.org>

Acesso mais seguro

Use o sistema de autenticação por Digest no Squid e evite a exposição de senhas.

por Emanuel dos Reis Rodrigues



Quando se fala no aumento de segurança em redes, já nos vêm à mente *switches*, *SSL*, *TLS* ou algum mecanismo baseado em criptografia pesada. Infelizmente, nem sempre conseguimos implementar *SSL* em tudo. Em redes grandes, onde o gerenciamento não é centralizado, isso se torna ainda mais complicado, pois há sempre alguém usando um hub velho numa sala desconhecida.

Os switches estão cada vez melhores, mais robustos e bem mais confiáveis, e os hubs estão tentando ficar mais inteligentes, mantendo seu baixo custo para continuar no mercado.

Uma técnica muito utilizada por invasores é o *sniffing*, que captura dados da rede, geralmente originários

de e destinados a outros usuários. Essa técnica é parcialmente bloqueada por vários switches; porém, os hubs, assim como os switches mais antigos, ainda permitem a captura do tráfego. Esse tráfego pode conter senhas de *FTP*, *HTTP*, *SMTP*, *POP3* e qualquer outro serviço que se utilize de senhas para garantir a autenticidade dos usuários sem o uso de uma camada segura.

Centralizando informações

Com o aumento significativo das estruturas e sistemas integrados, o serviço de diretórios é cada vez mais utilizado no ambiente corporativo, fornecendo informações e centralizando a autenticação para diversos outros serviços.

Em uma empresa onde existem vários serviços que solicitam autenticação, sendo necessária uma senha para cada um, os usuários tornariam essa estrutura extremamente complicada. Utilizando o serviço de diretório, o usuário passa a usar apenas uma senha para todos os serviços da empresa. Com isso, cada usuário assume total responsabilidade pelas atividades envolvidas com seu login na rede.

O *OpenLDAP* é um software livre que oferece um serviço de diretórios baseado no protocolo *LDAP*, e é perfeito para esse tipo de solução.

Dentre os serviços existentes em uma rede, o acesso à Internet pode ser destacado pelo uso intenso; utilizando o serviço de diretórios, é possível controlar o acesso dos usuários

Tabela 1: Alguns Mecanismos de Autenticação suportados pelo Squid

Categoria	Descrição
ntlm_auth	Normalmente utilizado para atender clientes Windows, que ao fazerem login na rede passam automaticamente suas credenciais ao <i>Squid</i> , que autoriza ou não o acesso à internet.
external_acl	Qualquer mecanismo de autenticação externa que possa receber parâmetros e retornar <i>ERR</i> ou <i>OK</i> , bastante utilizado para ACLs com grupos de usuários.
negotiate_auth	É um negociador de autenticação nativo do Windows, que também utiliza informações de usuários logados no domínio NT. Pouco utilizado.
digest_auth	Utiliza o protocolo HTTP, em um esquema de desafio e resposta baseado no algoritmo <i>HMAC</i> .
basic_auth	Utiliza o protocolo HTTP, aplicando <i>base64</i> para o tráfego das senhas.

à rede mundial de computadores, garantindo a transparência sobre o uso da Internet corporativa.

Serviço de acesso à Internet

Para servir Internet aos usuários de uma rede, o software livre mais utilizado é o *Squid*. Esse proxy web é capaz de prover acesso à Internet sem que os usuários precisem buscar diretamente o conteúdo das páginas, permitindo com isso o armazenamento das páginas num cache – com a conseqüente aceleração do acesso às mesmas – e o controle de acesso dos usuários, com filtros e mecanismos de autenticação. A **tabela 1** mostra as categorias de autenticação disponíveis para o Squid. É importante lembrar que cada uma dessas categorias possui vários módulos de autenticação.

O problema e a escolha do mecanismo

A maioria das implementações do Squid com OpenLDAP são feitas usando o método *basic* de autenticação HTTP (*basic_auth*). Apesar de manterem a conexão entre o Squid e o LDAP em SSL ou *loopback*, o tráfego de senhas entre o navegador e o proxy ocorre em *Base64*, permitindo que invasores consigam capturar e reverter as senhas para uso indevido. Somado à presença dos inseguros hubs, esse cenário pode se tornar altamente perigoso.

O método de autenticação *NTLM* possui a vantagem da facilidade de integração com máquinas Windows, porém, em redes heterogêneas, com máquinas Linux e Windows, esse modelo pode comprometer as máquinas Linux. Uma boa alternativa aos dois métodos citados é o *Digest*. O *Digest* utiliza o algoritmo *HMAC*, que faz uso de *hashes MD5* da combinação de informações dinâmicas com a senha e o login do usuário, para transportar seus dados na rede.

Em termos de segurança, a autenticação por *Digest* não substitui a criptografia por SSL/TLS, pois esses últimos são muito mais confiáveis. O *Digest* não é capaz de resolver todos os problemas de insegurança na autenticação do Squid, mas aumenta-a significativamente, com baixo custo e pouca sobrecarga.

Funcionamento do Digest com Squid

O *Digest* é um sistema de autenticação baseado em desafio e resposta (**figura 1**). No caso do Squid, que não é diferente das demais implementações de *Digest*, o usuário, utilizando um navegador, faz uma requisição ao proxy para uma página, www.linuxmagazine.com.br/faq/, por exemplo, que retorna o desafio: *Proxy Authentication Required* tipo *Digest*, o *realm*, o *nonce* e o *qop* (**tabela 2**).

Após receber o desafio, o navegador solicita ao usuário seu login e senha, e emprega o seguinte algoritmo:

```
A1 = login:realm:senha
A2 = GET:/faq/

hashA1 = md5(A1)
hashA2 = md5(A2)

reponse = md5(hashA1:nonce:nc:
               ↳cnonce:qop:hashA2)
```

Isso significa que o mecanismo *Digest* gera um hash MD5 do valor especificado em *A1* e outro daquele de *A2*. Em seguida, gera um terceiro hash, dessa vez com os valores do primeiro hash de *A1*, *nonce*, *nc*, *cnonce* *qop* e o segundo hash, de *A2*. Esse terceiro hash é a resposta (*response*) que será enviada ao Squid, que é o que realmente lhe interessa.

Integração com OpenLDAP

A senha do usuário no OpenLDAP costuma ser guardada em um campo chamado *userPassword*, em um

dos vários formatos: *crypt*, *md5*, *sha*, *blowfish*, *clear* e outros. Contudo, nenhum desses é compatível com o hash do método *Digest*. O Squid irá pesquisar o login na base LDAP, solicitando o retorno de um campo para comparação com a resposta enviada pelo *Digest*. Esse campo é simplesmente um atributo do usuário que possa armazenar uma cadeia de caracteres com o tamanho mínimo de *REALM:{hha1}* mais os 32 caracteres do hash. Esse campo é passado para o *squid_ldap_digest*, e deve conter o seguinte formato: *realm:{hha1}hash*, como por exemplo:

```
Planeta Terra:{hha1}253a0909ab7dbb
↳dba534f46b8d52d5e7
```

Ao obter uma resposta, o Squid compara os realms; se forem diferentes, ele informa que a senha é inválida, e se forem iguais, o restante é testado em seguida. O segmento *{hha1}* é necessário, mas o *squid_ldap_digest* o elimina, mantendo apenas o hash, que é *md5(login:realm:senha)*, ou a senha em texto puro, no caso do uso sem criptografia (não recomendado).

De posse do hash do valor *A1* vindo do servidor LDAP, o Squid calcula novamente o valor:

```
md5(hashA1_vindo_do_LDAP:nonce:nc:
↳cnonce:qop:hashA2)
```

e o compara com o valor de *response* calculado previamente, tendo assim o resultado da autenticação (**figura 1**).

Implementação

Vamos agora implementar esse método de autenticação para o proxy Squid. Como o *digest* do Squid 2.5 não suporta LDAP, e é o mais recente no momento da escrita deste artigo, demonstraremos como implementar essa solução usando partes do código da versão 3 do proxy web, ainda em desenvolvimento.

Tabela 2: Chaves utilizadas durante a transação Digest

Chave	Descrição
nonce	É uma chave para a sessão gerada aleatoriamente pelo Squid; possui um tempo de vida definido.
nc	<i>Request Counter</i> – um ID da requisição.
cnonce	É uma chave gerada pelo cliente durante a transação, <i>Client nonce</i> .
qop	Código de proteção, geralmente com o valor <i>auth</i> .
Uri	Quando se acessa um site, por exemplo www.linuxmagazine.com.br , seu URI é <i>GET:/</i> , pois nesse caso está sendo solicitado o acesso à raiz do site. No acesso a www.linuxmagazine.com.br/faq , o URI é <i>GET:/faq</i> .
realm	É o “reino” da uma sessão Digest.
response	Hash completo da transação, que será enviado ao Squid.
md5()	Não faz parte da transação, sendo apenas um símbolo para a demonstração. Ele gera um hash MD5 do que está dentro dos parênteses.

Após baixar o código-fonte do Squid 3 em [1], é necessário descompactá-lo e executar as etapas de configuração e compilação:

```
$ tar -zxvf squid3-XX.tar.gz
$ cd squid3-XX
$ ./configure --enable-digest-
  ↪ helpers=ldap
$ make
```

Não será necessário o `make install`, pois não iremos usar o proxy Squid 3, e sim o 2.5, que é estável e está pronto para o uso em produção.

Em seguida, pode-se instalar o Squid a partir dos binários empacotados pela sua distribuição. No caso dos usuários de *Debian* e derivados:

```
# apt-get install squid
```

O momento mais importante vem agora. Vamos utilizar no Squid 2.5 recém instalado o binário da autenticação Digest gerado com o código-fonte do Squid 3 na etapa anterior.

Para isso, precisamos apenas copiar o binário gerado para o local onde se encontram os binários que vieram no pacote da distribuição:

```
# cd squid3-XX/helpers/digest_
  ↪ auth/ldap/
```

```
cp digest_ldap_auth /usr/lib/
  ↪ squid/
```

É necessário que o Squid 2.5 que instalamos pelo gerenciador de pacotes tenha sido compilado com suporte ao *helper digest*, como é o caso no Debian.

Instalação do OpenLDAP

Se ainda não houver um servidor OpenLDAP em execução, será necessário instalar um. No Debian, o comando a seguir instalará os pacotes necessários:

```
# apt-get install slapd ldap-utils
  ↪ apache-ssl phpldapadmin
```

A instalação do pacote *slapd* exigirá o fornecimento de algumas informações. Para exemplificar, mostraremos a configuração para o domínio *linuxmagazine.com.br*:

- ◆ Domínio LDAP: *linuxmagazine.com.br*
- ◆ Organização: *linuxmagazine*
- ◆ Senha do administrador da base: *suasenha*
- ◆ Habilitar acesso à base usando o protocolo *ldapV2*: *Sim*

O *apache-ssl* também demanda algumas informações:

- ◆ Habilitar *suExec*: *Não*
- ◆ Gerar as chaves SSL.

Novamente, o pacote *phpldapadmin* também pedirá o preenchimento de alguns valores:

- ◆ Tipo de Autenticação: *Sessão*
- ◆ Daemons do servidor Web para configurar: *Todos*
- ◆ Reiniciar servidores Web: *Sim*

O OpenLDAP não possui necessidades especiais de instalação ou compilação; tanto o *slapd* do Debian quanto a configuração (*./configure*) dos fontes funcionam sem problemas.

Devido a limitações de espaço, não é possível cobrir aqui a administração de uma base LDAP. Para mais informações a esse respeito, há bastante documentação na página do OpenLDAP, em [2].

Configuração do OpenLDAP

Para ter acesso à base LDAP através do utilitário *phpldapadmin*, será necessária a configuração dos arquivos sob */usr/share/phpldapadmin/*.

Se o OpenLDAP tiver sido compilado manualmente, o diretório *phpldapadmin/* estará localizado no mesmo diretório onde foi feita a instalação.

No arquivo *config.php*, informe a localização da base LDAP, seu nome e seu domínio. Algumas informações podem ser obtidas no arquivo */etc/ldap/slapd.conf*.

```
$servers[$i]['host']='localhost'
$servers[$i]['base']='dc=linuxmagazine,dc=com,dc=br'
$servers[$i]['login_dn']='cn=admin,dc=linuxmagazine,dc=com,dc=br'
```

Em seguida, podemos acessar o *phpldapadmin* pelo navegador web, no endereço https://ip_da_máquina_local/phpldapadmin/.

Serão solicitados um login e uma senha:

```
Login DN: cn=admin,dc=linuxmagazin
```



```
e,dc=com,dc=br
Senha: suasenha
```

Se forem fornecidas as informações corretas, o sistema fará o login do usuário, mostrando no canto esquerdo da tela o nome da base LDAP - no caso, *dc=linuxmagazin* e, *dc=com,dc=br*.

Criaremos agora um novo usuário, clicando no símbolo + à esquerda do nome da base e, na lista que se abre, clicando em *Organizational Unit | OU Name | Create*.

Agora, clicando em *ou=usuários | User Account (posixAccount)*, pode-se preencher as informações a respeito do primeiro usuário. É importante lembrar que o campo *User Name* será o login do usuário criado. Não é necessário informar o tipo de criptografia, e a *shell* de login deve ser */bin/false*. É bom não alterar o valor de *Container*.

Clicando em *Continue | New User Account | Create Account*, o novo usuário será criado na base LDAP. Entretanto, a configuração feita até o momento não leva em conta a integração com outros serviços da rede.

Integrando

Para começar a realizar a integração do OpenLDAP com os outros serviços, precisamos primeiro gerar o conteúdo a ser usado no próximo passo, isso é, o primeiro hash necessário para a autenticação Digest. Para tanto, deve-se realizar essa operação num terminal:

```
$ echo -n "fulano:Planeta Terra:
senhadologin" | md5sum | cut -b
0-32
d7e7a8f04c18cc1e0ad5ac83798d452c
```

É importante guardar temporariamente esse hash, pois ele será usado em breve.

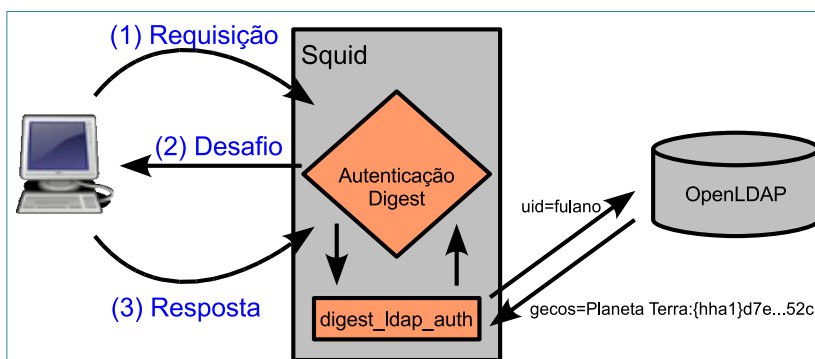


Figura 1 Esquema da autenticação por Digest no Squid com OpenLDAP.

Depois de criado o usuário e o hash Digest, precisamos de um atributo para guardá-los. Como visto anteriormente, esse atributo pode ser qualquer um, desde que caiba nele a informação do tipo *string* com o tamanho necessário.

Em nosso exemplo, vamos utilizar o atributo *gecos* do *nis.schema*, que tem outra finalidade, mas pode ser adequado de maneira genérica para guardar nossa cadeia de caracteres.

Voltando ao *phpldapadmin*, deve-se clicar em *uid=fulano* dentro de *ou=usuários* e, na parte superior, inserir um novo atributo, selecionando *gecos* e inserindo o valor:

```
Planeta Terra:{hha1}d7e7a8f04c18cc
1e0ad5ac83798d452c
```

É fundamental lembrar-se de substituir o hash acima pelo que foi copiado da etapa anterior.

Agora o usuário *fulano* está pronto para utilizar a internet.

Configuração do Squid

A configuração do Squid é realizada no arquivo */etc/squid/squid.conf*. Nele, é necessário inserir os parâmetros de autenticação:

```
auth_param digest program /usr/
lib/squid/digest_ldap_auth -b ou
=usuarios,dc=linuxmagazine,dc=co
```

```
m,dc=br -F "uid=%s" -D cn=admin,
dc=linuxmagazine,dc=com,dc=br -W
/etc/secret -h localhost -v 3 -
A gecos -e
auth_param digest children 5
auth_param digest realm Planeta
Terra
```

Ao inserir o realm *Planeta Terra*, deve-se verificar se não há um espaço em branco após o termo, pois um simples caractere a mais pode acarretar problemas na autenticação, uma vez que causará a geração de um hash distinto.

Para obrigar o uso de senha para o acesso à Internet, descomenta-se a linha:

```
acl password proxy_auth REQUIRED
```

Na seção de definição das ACLs, no mesmo arquivo, a seguinte linha deve ser inserida:

```
http_access allow all password
```

Após salvar o arquivo *squid.conf*, deve-se inserir a senha do administrador da base no arquivo */etc/secret* e reiniciar o Squid:

```
# echo "suasenha" > /etc/secret
# /etc/init.d/squid restart
```

Configurando-se o proxy do navegador para o endereço e a porta do proxy (em nosso caso, 10.0.0.1 e porta 3128), podemos tentar entrar em alguma página, e a auten-

Exemplo 1: Script para adicionar o campo digest ao LDAP

```
<?
/// Pré-requisito: PHP com suporte à LDAP

$base = "dc=linuxmagazine,dc=com,dc=br";
$dn = "uid=fulano,ou=usuarios,dc=linuxmagazine,dc=com,dc=br";
$server = "localhost";
$dn_admin = "cn=admin,dc=linuxmagazine,dc=com,dc=br";
$senha_admin = "suasenha";
$realm = "Planeta Terra";
$user = "fulano";
$senha = "senhalogin";

$ds=ldap_connect($server) or die ("Nao foi possivel estabelecer conexao com $server !");

ldap_set_option($ds,LDAP_OPT_PROTOCOL_VERSION,3);

$r=ldap_bind($ds,$dn_admin,$senha_admin) or ("Erro ao autenticar: Credenciais invalidas");

// Gerando o hash MD5
$hash = md5("$user:$realm:$senha");
$dados["gecos"]=$realm . ":" . "{hha1}" . $hash;

// Inserindo o attributo do Digest no ldap
$r=ldap_modify($ds,$dn,$dados);

if ($r) {
    echo "Inclusao do Digest executada com sucesso para o usuario $user : ";
    echo $realm . ":" . "{hha1}" . $hash;
} else {
    echo "erro ao incluir Attributo Digest!";
}
?>
```

ticação será solicitada: *Forneça a senha para o proxy: Planeta Terra em 10.0.0.1:3128*

Evidentemente, o nome e a senha do usuário devem ser aqueles que criamos nos passos anteriores.

Problemas?

O script `digest_ldap_auth` precisa receber como parâmetro o login e a realm. É possível testar seu funcionamento na linha de comando, com o comando:

```
# /usr/lib/squid/digest_ldap_auth
➤ -b "ou=usuarios,dc=linuxmagazine,dc=com,dc=br" -F "uid=%s" -D "cn=admin,dc=linuxmagazine,dc=com,dc=br" -W /etc/secret -h localhost -v 3 -A gecoss -e
```

Logo após entrar com o comando, o script irá esperar a en-

trada do login e realm incluindo as aspas. Se correr tudo bem, ele trará o hash:

```
"fulano": "Planeta Terra"
d7e7a8f04c18cc1e0ad5ac83798d452c
```

O **exemplo 1** mostra um script em *PHP* que pode ser usado para adicionar o campo `digest` ao LDAP.

Recomendações

Toda estrutura deve possuir suas políticas. Seria interessante agregar a possibilidade de implantação de um mecanismo para troca de senhas dentro de um tempo determinado, garantindo que os usuários troquem suas senhas e, se possível, que elas sejam testadas por outro mecanismo, como a *Cracklib*, por exemplo, para garantir sua segurança.

Considerações Finais

A principal intenção deste artigo é exemplificar o modelo de autenticação Digest, suportado por um grande número de serviços, e capaz de proporcionar uma maior segurança na validação de senhas em trânsito pelas redes. Em caso de problemas durante os procedimentos, o autor deste artigo ficará feliz em ajudar. ■

Mais Informações

[1] Squid: <http://www.squid-cache.org/>

[2] OpenLDAP: <http://www.openldap.org/>

O autor

Emanuel dos Reis Rodrigues é assessor de TI no Centro de Tecnologia da Informação do Governo do Estado de Roraima.

Barreiras de escrita

Organizando a fila

Um bom disco rígido e um sistema de arquivos com *journal* não eliminam totalmente a perda de dados. É preciso ir além.

por Martin Steigerwald



Stephanie - www.pixelio.de

Sistemas de arquivos com *journal* oferecem alguns importantes benefícios aos usuários, mas também põem alguns problemas sutis, como a necessidade do sistema de arquivos manter um registro que reflita o estado das operações de escrita no dispositivo

de armazenamento, enquanto o dispositivo pode fazer alterações na ordem das requisições de escrita de forma a otimizar o desempenho. Se o sistema falhar em um ponto em que o *journal* não esteja em compasso com a sequência real das operações de gravação, os da-

dos podem não estar tão seguros quanto se imagina.

Os desenvolvedores de sistemas de arquivos e os fabricantes de discos rígidos estão cientes desse problema, e várias soluções e ajustes já foram empregados. Uma solução no estilo “força bruta” consiste

simplesmente em esvaziar o *cache* de escrita antes e depois de cada operação de gravação, o que efetivamente elimina o *cache* sem desativá-lo na camada de hardware.

Uma solução melhor e mais veloz, e que vem recebendo bastante atenção dos desenvolvedores, é garantir que as requisições de grava-

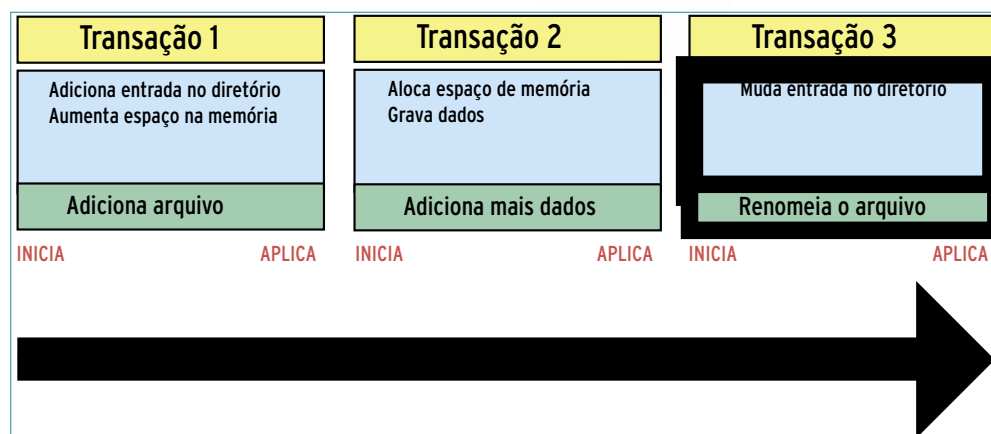


Figura 1 O sistema de arquivos grava transações individuais, como a criação de um arquivo, de forma sucessiva no *journal*. As transações podem ter o estado de completadas ou não iniciadas. As completadas são marcadas por uma operação de gravação contígua.

ção sejam efetivadas no disco em uma ordem previsível, usando requisições do tipo *write barrier* (barreira de escrita).

Apesar de o suporte a barreiras de escrita estar se tornando muito mais comum, a questão a respeito de se usar ou não essas barreiras – e se o sistema de arquivos utilizado já está empregando-as – depende do sistema de arquivos, versão do kernel e dispositivo de armazenamento.

Já passei por três problemas graves com sistemas de arquivos em uma semana, em meu IBM ThinkPad T23 com XFS e kernel 2.6.16 com *buffer* de gravação ativado[1]. Os problemas pararam quando desativei o cache de gravação, muito embora versões anteriores do kernel fossem estáveis com ele. Com um kernel 2.6.17, ao final, a estabilidade com barreiras de escrita voltou ao nível anterior.

O rápido desenvolvimento e a integração das barreiras de escrita às versões do kernel, drivers de sistema de arquivos e dispositivos de armazenamento significam que, se você pretende fazer *troubleshooting* de um sistema de arquivos, é melhor começar com ao menos um conhecimento básico desse recurso.

Como funciona o journal

Um sistema de arquivos com journal oferece um seguro de vida aos dados, pois registra cada alteração realizada neles. Sistemas de arquivos com journal dos dados (ou journal completo – *full journalling*) garante a consistência do conteúdo de arquivos (veja o **quadro 1**). Essa abordagem é bastante segura, porém, geralmente tem como custo de queda da desempenho.

Uma técnica mais rápida, conhecida como *journal de meta-*

Quadro 1: Journal de dados

Sistemas de arquivos com *journal* que escrevem apenas metadados nesse journal possuem uma desvantagem. Se as operações de gravação forem interrompidas, os arquivos podem ficar ilegíveis devido a operações incompletas. O sistema de arquivos talvez tenha alocado outros blocos de dados para o arquivo antes de completar as operações de escrita nesses blocos, ou então uma operação de gravação destinada a sobrescrever dados em um arquivo pode não ter sido completada.

Um sistema de arquivos com journal de dados soluciona isso gravando os dados primeiro no journal. Se ocorrer uma queda, o sistema de arquivos utiliza o journal para recuperar o estado em que os metadados estavam de acordo com os dados nos arquivos, e então, ou as operações de gravação individuais são completadas, ou não ocorrem.

Os sistemas Ext3, ReiserFS 3 e Reiser 4 suportam o journal de dados, diferentemente do XFS e do JFS, que, na escrita deste artigo, ainda não o faziam.

As operações de escrita são muito mais lentas se o journal de dados estiver ativo, o que é compreensível, já que todas as operações de gravação terão que ocorrer duas vezes: uma no journal e outra no disco propriamente dito. O Reiser 4 é o único sistema de arquivos que grava os dados em sua localização final e sobrepõe um *wandering journal* nos dados.

Os sistemas Ext3 e ReiserFS 3 oferecem uma solução temporária para evitar o uso do journal de dados: o sistema grava os blocos de dados de uma transação de metadados antes de registrar a transação no journal. Essa solução garante que novos blocos de dados alocados em um arquivo tenham sempre dados válidos. Entretanto, operações parcialmente terminadas que sobrescrevam dados em um arquivo sempre levarão a um estado inconsistente.

O journal de dados não garante a integridade dos dados de sua aplicação caso um processo de escrita termine de forma anormal. É por isso que muitos bancos de dados e programas servidores, como de email, por exemplo, possuem seus próprios mecanismos de assegurar a integridade dos dados em caso de interrupções inesperadas. Esse tipo de journal específico por aplicativo geralmente se baseia na gravação de dados em uma ordem específica, e costuma depender de operações de escrita atômicas. Outros programas, como as aplicações PIM do KDE (*KAddressBook*, *Korganizer* e *Akkregator*), criam backups dos arquivos críticos.

dados, garante a consistência da estrutura do sistema de arquivos simplesmente monitorando as informações dos metadados, como nomes de arquivos e diretórios, tamanhos de arquivos, permissões e localizações de armazenamento. O sistema de arquivos guarda essa informação em blocos especiais para informações administrativas, os *inodes*.

Caso o sistema de arquivos seja interrompido enquanto modifica os metadados, estes podem tornar-se inconsistentes, pois a maioria das alterações envolve múltiplas etapas, das quais talvez apenas a metade tenha sido realizada. Por exemplo, quando o sistema de arquivos cria um novo arquivo, ele precisa criar

uma entrada no diretório onde esse arquivo será armazenado, alocar espaço em disco, gravar os dados e lembrar-se de onde o arquivo foi gravado. Se ocorrer uma interrupção, o espaço de armazenamento do arquivo pode ser ocupado, embora o sistema de arquivos talvez não tenha criado uma entrada até o momento da interrupção.

Um sistema de arquivos sem journal sabe apenas que não foi corretamente desligado, e mostra isso na próxima inicialização. Um programa especial, como o *fsck*, deve verificar se os metadados estão intactos, e se houver um sistema de arquivos muito populoso, esse processo pode ser bem demorado.

Em contraste, sistemas de arquivos com journal gravam no journal as alterações necessárias para uma operação completa, como a criação de um arquivo, na forma de transações (**figura 1**). As transações são atômicas, isso é, operações contíguas com um ou dois estados possíveis: ou a transação ocorre por completo, ou simplesmente não ocorre. Supondo que a transação tenha sido completada, o sistema de arquivos atribui a ela um rótulo numa operação de gravação invisível.

Sistemas de arquivos com journal possuem um de dois formatos de armazenamento: journal físico ou lógico. Um journal físico, como o usado pelo *Ext3*, preenche blocos completos com metadados. O *Ext3* utiliza para isso o *Journal Block Device* [2] (*JBD*). O *XFS* possui um journal lógico, assim como o *ReiserFS 3* e o *JFS*. Esse journal guarda os metadados de uma forma independente dos arquivos, e mais compacta.

Ao montar novamente um sistema com journal após uma interrupção inesperada, ele tentará avaliar as informações do journal para recuperar um estado consistente. Se alguma transação ainda estiver marcada como incompleta no journal, o sistema a descartará.

O sistema de arquivos processará as transações completadas passo a passo, verificando quais mudanças foram gravadas no disco e gravando aque-

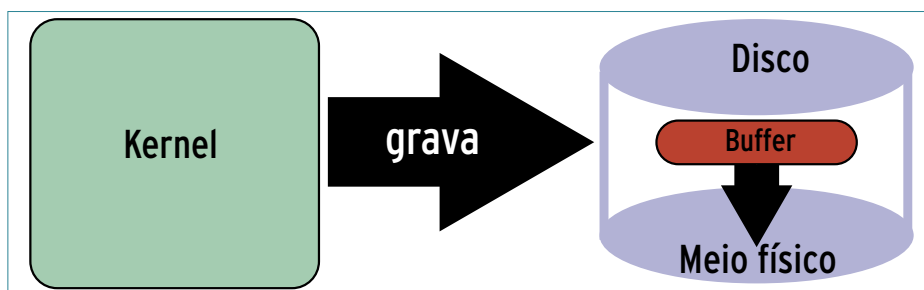


Figura 2 Não existe controle sobre a ordem de gravação se existir um *buffer* de escrita.

las que ainda não tenham ocorrido. Ele não rotula uma transação como completa até que todas as mudanças estejam gravadas no disco, e então o espaço do journal é liberado.

Como o sistema com journal apenas precisa verificar as entradas armazenadas no journal, não há necessidade de checar toda a estrutura de metadados, o que significa que o processo de recuperação não levará mais de alguns segundos sob circunstâncias normais. Se o sistema for novamente interrompido durante o processo de recuperação, ele simplesmente continuará a partir da última transação incompleta quando tudo voltar ao normal.

Essa técnica não garante que todas as alterações realizadas nos arquivos vão sobreviver a um desligamento repentino; no entanto, assegura que a estrutura do sistema de arquivos permanecerá consistente caso todas as operações de escrita ocorram na ordem correta.

O sistema de arquivos começa gravando a transação no journal, e

então aplica as mudanças nos metadados, marcando-as como completadas. Se essas mudanças chegarem ao disco antes da entrada do journal e o processo for interrompido, o sistema de arquivos será incapaz de localizar no journal as entradas referentes a essas alterações, durante o processo de recuperação. Nesse caso, o sistema obviamente adquire um estado inconsistente.

As transações marcadas como completadas antes das mudanças de metadados terem sido gravadas no disco podem causar problemas semelhantes. Portanto, o sistema de arquivos precisa assegurar que as alterações sempre sejam gravadas em uma ordem específica. Não há garantia de que isso ocorra em discos rígidos dotados de cache.

Esse tipo de disco primeiro faz um cache dos dados que precisa gravar, em um buffer de memória temporário que se localiza entre a veloz memória RAM e os morosos mecanismos de gravação física do disco. O *firmware* então decide em que ordem irá realizar

Tabela 1: Opções de montagem

Funcionalidade	Ext3	ReiserFS	Reiser 4	XFS	JFS
Barreira de escrita	<code>barrier=1</code>	<code>barrier=flush</code>	Padrão	Padrão desde o kernel 2.6.17	
Sem barreira	<code>barrier=0</code>	<code>barrier=none</code>	-	<code>nobarrier</code>	-
Journal de dados	<code>ordered=journal</code>	<code>ordered=journal</code>	Padrão (<i>wanting logs</i>)	-	-
Dados antes dos metadados	<code>ordered=data</code>	<code>ordered=data</code>	-	-	-
Modo <i>Writeback</i>	<code>ordered=writeback</code>	<code>ordered=writeback</code>	-	Padrão	Padrão

a gravação do conteúdo do buffer de escrita (**figura 2**).

Uma técnica para garantir que seja obedecida uma ordem de gravação específica envolve o sistema de arquivos informar ao driver para esvaziar o cache antes e depois de uma transação de escrita. A segunda técnica consiste em fazer o sistema de arquivos utilizar a funcionalidade de barreiras de escrita do kernel para ordenar as operações de escrita em uma ordem específica [3].

Uma requisição de barreira faz a camada de blocos do Linux manter a seguinte ordem nas operações de gravação: todas as requisições de escrita anteriores à requisição de barreira são processadas normalmente; em seguida, vem a requisição de barreira; depois disso, todas as requisições de gravação voltam a ser processadas normalmente.

Essa abordagem possui duas vantagens. Em primeiro lugar, não há necessidade de um esvaziamento imediato do cache de gravação, pois ele pode ocorrer logo antes da requisição de barreira. Além disso, o driver pode deixar a ordem de requisições parcial ou inteiramente nas mãos dos inteligentes dispositivos de armazenamento.

A camada de blocos do kernel faz distinção entre dispositivos, com base em dois critérios: a ordem de requisição e o tipo de buffer de escrita (**quadro 2**). Por exemplo, unidades do tipo *Forced Unit Access* não necessitam de um esvaziamento do cache após a requisição de barreira.

Ativar as barreiras de escrita em sistemas com journal pode aumentar tanto a estabilidade quanto o desempenho – contanto que sua versão do kernel, seu disco e seu sistema de arquivos ofereçam o suporte a esse recurso.

Aplicações práticas

Para usar barreiras de escrita, primeiro é necessário um kernel que as suporte. Os diferentes sistemas de arquivos incluíram esse recurso em versões distintas do kernel.

Para o XFS, é necessária a versão 2.6.17.7 do kernel, ou posterior. Já no ReiserFS 3, as barreiras estão presentes desde o kernel 2.6.9, com muitas mudanças tendo sido efetuadas no 2.6.16. Independente dos números, o que decide se as barreiras podem ser usadas com a sua combinação de componentes são os testes práticos.

O RAID por software também funciona com barreiras de escri-

ta, contanto que o controlador e todos os dispositivos suportem o esvaziamento de cache (*cache flushing*). No entanto, nem todos os tipos de RAID são compatíveis com o recurso.

O suporte a barreiras de escrita está evoluindo muito rapidamente. Em caso de dúvida quanto à compatibilidade de um sistema com as barreiras, deve-se usar uma das opções de montagem mostradas na **tabela 1** até ser possível determinar o comportamento padrão. Conferindo os registros do sistema, é possível identificar sucessos e fracassos no suporte ao recurso. O XFS, por exemplo, exibe nos

Quadro 2: Classes de dispositivos

A funcionalidade de *write barriers* na camada de blocos garante uma ordem específica no processamento de requisições de I/O. Requisições de barreira, portanto, necessitam de duas propriedades:

Ordem de requisição

São possíveis as seguintes variantes:

- ◆ Dispositivos com suporte a múltiplas requisições enfileiradas e a requisições sequenciais (dispositivos *TCQ* – *Tagged Command Queueing*) – tais como controladoras e dispositivos *SCSI* modernos. A camada de dados passa a requisição de barreira para o dispositivo como uma requisição sequencial. Os drivers de baixo nível, controladoras e dispositivos são responsáveis por manter a sequência correta. Essa opção ainda não está ativada no Linux, pois a função de *dispatch* do subsistema *SCSI* dos kernels até 2.6.17 não passa requisições atômicas para a controladora *SCSI*, o que significa que a ordem de requisições pode mudar.
- ◆ Dispositivos com suporte a múltiplas requisições enfileiradas, mas não às sequenciais – típico de controladoras e discos *SCSI* mais antigos, assim como de unidades *SATA*: a camada de blocos assegura a ordem correta.
- ◆ Dispositivos que lidam sequencialmente com requisições – dispositivos *SCSI* muito antigos e discos *IDE*: novamente, a camada de blocos garante a ordem correta.

Cache de escrita

Há quatro modalidades de cache de escrita:

- ◆ Sem cache: é suficiente para organizar as requisições na ordem correta.
- ◆ Cache *writeback* sem esvaziamento: é impossível garantir a ordem correta de escrita, e não há suporte às barreiras de escrita. É necessário desativar o cache de gravação, nos discos desse tipo, para oferecer suporte estável a interrupções súbitas em sistemas de arquivos com journal.
- ◆ Cache de escrita com esvaziamento, sem *Forced Unit Access (FUA)*: o subsistema de blocos aciona um esvaziamento de cache antes e após a requisição.
- ◆ Cache de escrita com esvaziamento e *FUA*: a camada de blocos aciona o esvaziamento antes da requisição de barreira, a qual passa o esvaziamento como requisição *FUA*. Essa requisição informa o disco para gravá-la imediatamente e não usar o cache de escrita para isso.

logs três possíveis mensagens quando ocorre algum erro [4]. Já o JBD, usado pelo Ext3, dá uma mensagem clara e direta.

O comando `hdparm -I /dev/hda` pode mostrar se o cache de gravação está ativado. `hdparm -W0 /dev/hda` desativa esse cache, e `hdparm -W1 /dev/hda` ativa-o.

Suporte do sistema

Em alguns sistemas, é possível testar se as barreiras de escrita são suportadas montando-se o sistema de arquivos como um dispositivo de *loop*. Como esses dispositivos não suportam as barreiras, a presença de uma mensagem de erro ao se tentar montar um sistema com barreiras como *loop* indicam que as barreiras estão sendo usadas por padrão.

Sem a funcionalidade das barreiras, os sistemas de arquivos com

journal só são capazes de conservar sua integridade, após interrupções inesperadas, caso o cache de escrita esteja desligado, ou se o sistema de arquivos gravar transações de forma síncrona.

Dispositivos com buffers de gravação que não suportem o esvaziamento do cache são, por projeto, incapazes de suportar uma ordem específica para as requisições de escrita. Nesse caso, a única forma de os usuários obterem segurança para seus dados é desativando o buffer de gravação.

Controladores e dispositivos com buffers de gravação persistentes (NVRAM) não costumam suportar barreiras, pois conseguem gravar dados no disco até mesmo após uma falta de energia. Na realidade, o suporte ao buffer de escrita às vezes pode interferir sobre o dispositivo NVRAM.

Conclusão

Ativar as barreiras de escrita resolveu os problemas de instabilidade no meu caso. A desativação do cache de gravação também foi útil, mas, ao menos em teoria, as barreiras oferecem melhor desempenho – principalmente em operações de gravação complexas. ■

Mais Informações

[1] Kernel bug #6380:
http://bugzilla.kernel.org/show_bug.cgi?id=6380

[2] Journalling Block Device:
<http://kerneltrap.org/node/6741>

[3] Documentação interna sobre barreiras no kernel 2.6.17.1: `block/barriers.txt`

[4] FAQ do XFS: Como resolver o problema do cache de gravação?:
http://oss.sgi.com/projects/xfs/faq.html#wcache_fix

pyconbrasil [3]

encontro brasileiro da comunidade python

30, 31 de agosto e 1º de setembro de 2007
em Joinville - SC, na SOCIESC.

Temas desta edição:

- Plone / Zope
- Zope3 / Grok
- Django / Turbo Gears
- Maemo
- Eagle / GTK / QT
- Sugar(OLPC)
- Ensino de Python
- ... e muito mais

Chamada de eventos, inscrições e patrocínio, acesse:

<http://pyconbrasil.com.br/>

organização:

 **pythonbrasil**
Associação Python Brasil

 **SOCIESC**
Educação e Tecnologia

apoio:

 **LINUX NEW MEDIA**
The Power of Linux

© Linux New Media do Brasil Editora Ltda.

Plugando no Nagios

Veja como utilizar a versátil linguagem Perl para criar plugins personalizados para o daemon de monitoramento de redes Nagios.
por Michael Schilli



Levi Szekeres - www.scx.hu

Muitos administradores de redes já experimentaram aquela situação em que o colega não técnico na sala ao lado de repente grita: “Minha Internet caiu!”. Evidentemente, uma possível solução para isso seria verificar se o roteador realmente está se comunicando com o provedor de acesso, e se os servidores DNS estão respondendo. Porém, usar o Nagios para monitorar esses fatores (figura 1) é muito mais racional e eficiente.

Na maioria dos casos, a instalação de um agente do Nagios no servidor a ser monitorado requer acesso a sua *shell*. Entretanto, se desejarmos monitorar a atividade de um servidor web contratado que não permite acesso por SSH, ainda há uma saída.

Estatísticas de I/O

O exemplo 1 mostra o script agente *iostat.cgi*, que pode ser inserido no diretório CGI do servidor web.

Ao ser ativado por uma requisição HTTP, o script chama o comando *iostat* do Linux, enviando parte da saída gerada de volta para o cliente, que no caso é o plugin do Nagios. O plugin examina essa saída e utiliza o código de saída para informar ao Nagios se há ou não um problema.

O script CGI *iostat.cgi* utiliza a função *tap* para chamar o comando *iostat* com os valores 1 e 2 (linha 8). Devido aos valores de intervalo (1) e

Exemplo 1: *iostat.cgi*

```
01 #!/usr/bin/perl -w
02 use strict;
03 use Sysadm::Install qw(:all);
04 use CGI qw(:all);
05 use Regexp::Common;
06
07 my ($saida, $erro, $rc) =
08     tap "iostat", 1, 2;
09
10 $saida =~
11     /avg-cpu.*?avg-cpu/g;
12
13 print header();
14
15 for my $chave (
16     qw(user nice sys
17         iowait idle)
18     ) {
19     if ($saida =~
20         /\G.*?($RE{num}{real})/gs) {
21         printf "%s %s ", $saida, $1;
22     }
23 }
```

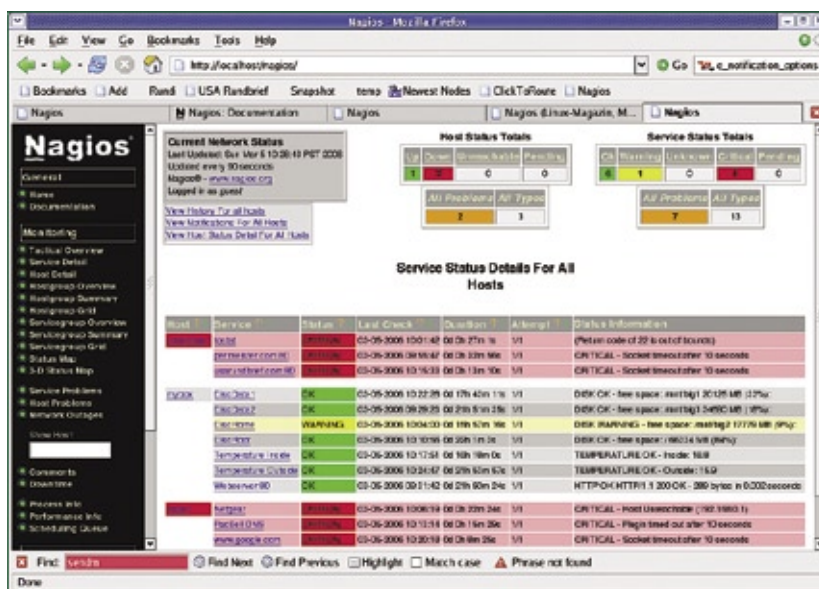


Figura 1 A página de visualização geral do Nagios mostra que os testes locais foram completados com sucesso, mas o roteador e tudo além dele encontram-se incommunicáveis.

```

root@mschilli: ~
monitorado # iostat 1 2
Linux 2.6.19-smp (mschilli)      03/05/2007

avg-cpu:  %user   %nice    %sys %iowait  %idle
           4.81    0.05    1.59    5.63   87.91

Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
hda                  3.56         29.16         48.67    56494409    94289782
hdb                  17.87        304.85        118.35   590620608   229294184
hdd                   4.16         32.40         28.16    62772880    54560680

avg-cpu:  %user   %nice    %sys %iowait  %idle
           2.99    0.00    0.50    0.00   96.52

Device:            tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
hda                  0.00         0.00         0.00         0         0
hdb                  0.00         0.00         0.00         0         0
hdd                  0.00         0.00         0.00         0         0
monitorado #

```

Figura 2 O *iostat* mostra quanto tempo a CPU esteve ociosa, e com que frequência foi necessário esperar o disco rígido.

do contador (2), ele mede o desempenho da CPU e de I/O do disco rígido duas vezes a cada segundo, criando a saída mostrada na **figura 3**.

O primeiro teste retorna o valor médio desde a última reinicialização da máquina, enquanto o segundo é mais interessante para o Nagios, pois coleta dados de desempenho por um segundo, enquanto o comando está em execução. A coluna *%ocioso* mostra por quanto tempo a CPU permaneceu disponível, e *%esperaIO* mede quanto tempo a CPU precisou esperar pelo disco rígido. Do ponto de vista do usuário, altos valores em *%ocioso* e baixos valores em *%esperaIO* são o melhor cenário possível.

O script do **exemplo 1** lê a saída do comando *iostat* e descarta o primeiro conjunto de valores. Para isso, ele usa a expressão regular `$RE{num}{real}` do repositório *Regexp::Common* para examinar os valores numéricos. Após o cabeçalho HTTP obrigatório, ele retorna uma cadeia como `user 2.99 nice 0.00 sys 0.00 iowait 0.00 idle 96.52`. O chamado termo de largura zero, `\G (linha 20)`, evita que o mecanismo de regex volte ao início do texto a cada vez, e ordena que ele continue a busca após a última coincidência.

Carga máxima

No lado do Nagios, o plugin do **exemplo 2** usa o *LWP::Simple* para chamar o script CGI do servidor mencionado acima, captura a linha de saída e executa um *split* para separá-la em campos, que então são guardados na *hash* `valores`. Se a disponibilidade da CPU estiver abaixo de 50, o plugin retorna um estado crítico, enquanto valores até 80% retornam apenas um alerta. O mesmo princípio pode ser aplicado ao valor de *iowait*, mas os valores limite são 10 e 20 por cento.

O módulo do CPAN *Nagios::Clientstatus* elimina parte da carga sobre o plugin, verificando se ele recebeu todos os parâmetros necessários. O método *exitvalue()* também entende cadeias de caracteres, como *warning*, e não apenas os valores numéricos que o Nagios exige. Se o plugin for executado na linha de comando, com *check_iostat -url=http://servidor/cgi/iostat.cgi*, ele retorna as seguintes linhas:

```

IOSTAT OK - user 2.99 nice 0.00
➔ sys 0.00
iowait 0.00 idle 96.52

```

O Nagios chama o plugin dessa mesma forma, interpreta o valor de saída e depois exibe a saída de texto

Exemplo 2: check_iostat

```

01 #!/usr/bin/perl
02 use strict;
03 use LWP::Simple;
04 use Log::Log4perl qw(:easy);
05 use Nagios::Clientstatus;
06
07 my $versao = "0.01";
08 my $cliente =
09   Nagios::Clientstatus->new(
10     help_subref => sub {
11       print "Uso: $0 ",
12         "url\n";
13     },
14     version => $versao,
15     mandatory_args =>
16       ["url"],
17   );
18
19 my $url =
20   $cliente->get_given_arg(
21     "url");
22
23 my $dados = get $url;
24
25 if (! $dados) {
26   print
27     "Falha ao obter $url\n";
28   exit $cliente->exitvalue(
29     "unknown");
30 }
31
32 my %valores = split ' ',
33   $dados;
34
35 my $status =
36   $valores{idle} < 50
37   ? "critical"
38   : $valores{idle} < 70
39   ? "warning"
40   : $valores{iowait} > 20
41   ? "critical"
42   : $valores{iowait} > 10
43   ? "warning"
44   : "ok";
45
46 print "IOSTAT ", uc($status),
47   " - $dados\n";
48
49 exit $cliente->exitvalue(
50   $status);

```

na saída padrão. Note que o *Nagios::Clientstatus* exige a versão 2.35 ou mais recente do *Getopt::Long*.

Integração do plugin

Para adicionar o novo plugin a uma instalação pré-existente do Nagios, o usuário administrador precisa copiar o script *check_iostat* para o diretório `/usr/local/`

Exemplo 3: verifica_temperatura

```

01 #!/usr/bin/perl -w
02 use strict;
03 use RRDTOol::00;
04 use Getopt::Std;
05 use Pod::Usage;
06 use Nagios::Clientstatus;
07
08 my $N = "TEMPERATURA";
09
10 my $cliente =
11 Nagios::Clientstatus->new(
12     help_subref =>
13     sub { pod2usage() },
14     mandatory_args => [
15         qw( crit warn dsname)
16     ],
17 );
18
19 my $rrd =
20 RRDTOol::00->new(file =>
21     "/tmp/temperature.rrd");
22
23 my $dsnames =
24 $rrd->meta_data("dsnames");
25
26 $rrd->fetch_start(
27     start => time() - 6 * 60,
28     end => time()
29 );
30
31 my $temp;
32
33 if (my ($hora, @valores) =
34     $rrd->fetch_next())
35 {
36     for (
37         my $i = 0 ;
38         $i < @dsnames ;
39         $i++
40     )
41     {
42         if (
43             $dsnames->[$i] eq
44             $cliente->get_given_arg(
45                 "dsname")
46         )
47         {
48             $temp = $valores[$i];
49             last;
50         }
51     }
52 }
53
54 my $status = "ok";
55
56 if (!defined $temp) {
57     $status = "unknown";
58 } elsif ($temp >=
59     $cliente->get_given_arg("crit"))
60 {
61     $status = "critical";
62 } elsif ($temp >=
63     $cliente->get_given_arg("warn"))
64 {
65     $status = "warning";
66 }
67
68 printf "$N %s - %s: %s\n",
69     uc($status),
70     $cliente->get_given_arg(
71         "dsname"),
72     defined $temp
73     ? sprintf("%.1f", $temp)
74     : "NODATA";
75
76 exit $nc->exitvalue($status);

```

`nagios/libexec` e tornar o script executável. A **figura 3** acrescenta um modelo intitulado `ez-service` à configuração do Nagios; ele facilita a adição futura de outros serviços. Nas configurações do Nagios, é comum definir modelos, facilmente identificáveis por suas entradas `register 0`. As definições de serviços podem ser usadas depois para acrescentar entradas especiais aos modelos.

A configuração `define service` na **figura 3** define o novo serviço `iostat`. Ela é feita sobre o modelo do `ez-service` que definimos antes e aceita vários parâmetros para rodadas de teste, notificação por email e outros. Essas configurações de modelos depois são herdadas pela definição do serviço e podem ser sobrescritas caso necessário.

Servidor solitário

Se o servidor Nagios for separado do resto do mundo devido a uma falha de rede, não será possível ele enviar alertas por email. Nesse caso, o administrador recebe ao menos um email de aviso quando o problema for resolvido. O sistema pode solucionar alguns problemas sem intervenção humana.

Com o Nagios 2.0, um serviço sempre é mapeado para uma máquina cuja disponibilidade é testada independentemente. A especificação da máquina requer entradas no arquivo de configuração. A linha `host_name = maquina` na configuração de exemplo define o nome da máquina a ser exibido na página do Nagios.

O parâmetro `check_command` da definição de serviços especifica como chamar o novo plugin `check_iostat`. Entretanto, a chamada não é feita diretamente na definição do serviço; em vez disso, é usado um comando configurado antes em `define command` para especificar a linha de comando a ser executada. A linha `check_command` pode usar argumentos opcionais, passados em seguida para a definição do comando. Separada por um ponto de exclamação, a URL da linha `check_command` é passada para a definição de comando do `iostat` e substitui o termo `$ARG1$`.

O valor `24x7` para `check_period` e `notification_period` requer configurações para definir o email e a disponibi-

```
mschilli@mybox:~/DEV/articles/nagios/eg
# Service Template
define service{
    name                ez-service
    active_checks_enabled 1
    passive_checks_enabled 1
    parallelize_check     1
    obsess_over_service    1
    check_freshness        0
    notifications_enabled  1
    event_handler_enabled  1
    flap_detection_enabled 1
    failure_prediction_enabled 1
    process_perf_data       1
    retain_status_information 1
    retain_nonstatus_information 1
    register               0
    is_volatile             0
    max_check_attempts      1
    check_period            24x7
    normal_check_interval    60
    retry_check_interval     1
    contact_groups          admins
    notification_options     w,u,c,r
    notification_interval    0
    notification_period      24x7
}

# Iostat Plugin
define command{
    command_name    iostat
    command_line    $USER1$/check_iostat --url $ARG1$
}

# Iostat Service
define service{
    use                ez-service
    host_name           dreamhost
    service_description iostat
    check_command        iostat!http://perlineister.com/cgi/iostat.cgi
}
```

Figura 3 Configuração do Nagios para o novo plugin *iostat*.

lidade do administrador. Pode-se usar um arquivo de exemplo com nome de *eznagios.cfg* em [1] e acrescentar ao arquivo de configuração *nagios.cfg* a linha *cfg_file=/usr/local/nagios/etc/eznagios.cfg*. Ao mesmo tempo, o *ez-nagios.cfg* define os testes do Nagios que informarão quanto espaço em disco está ocupado, e se seu roteador e DNS do provedor estão funcionando.

Quente?

O plugin *verifica_temperatura* é mais um bom exemplo de contribuição caseira para o Nagios. O script (exemplo 3) contacta o banco de dados *round-robin* para verificar a temperatura, alertando o servidor caso as temperaturas internas e externas mais recentes excederem valores específicos. No estilo típico dos plugins de Nagios, ele aceita parâmetros de linha de comando para valores de limites. Chamar *verifica_temperatura -warn=30 -crit=35 -dsname=Interior* aciona um alerta se a temperatura interior ultrapassar 30 graus Cel-

```
root@mschilli:/
monitorado # ./verifica_temperatura
Mandatory arguments not given: crit, warn, dsname
monitorado $ echo $?
2
monitorado $ ./verifica_temperatura -crit=30 -warn=20 -dsname=Exterior
TEMPERATURE WARNING - Exterior: 23.1
monitorado $ echo $?
1
monitorado $ ./verifica_temperatura -crit=30 -warn=20 -dsname=Interior
TEMPERATURE OK - Interior: 19.1
monitorado $ echo $?
0
monitorado #
```

Figura 4 Saída e valores de retorno do plugin de temperatura com vários parâmetros de linha de comando.

sus. O limite crítico é 35 graus. A figura 4 mostra os vários valores de saída e a própria saída do plugin para diferentes configurações de parâmetros.

De forma semelhante ao plugin *iostat* que fizemos antes, a linha de serviço *check_command verifica_temperatura!25!30!Interior* passa os parâmetros 25, 30 e Interior para o script. A entrada de *command* correspondente fica assim:

```
define command {
    command_name verifica_
    temperatura command_line $USER1$/
    verifica_temperatura -warn=$ARG1$
    -crit=$ARG2$ -dsname=$ARG3$
}
```

A parte central da colorida tabela da figura 1 mostra que os dois valores de temperatura estão bem normais: 18,8 graus (internos) e 15,9 graus (externos). Pelo menos meu apartamento não está em chamas!

E boa noite

Depois de todas essas alterações aos arquivos de configuração, pode ser uma boa idéia verificar novamente se não há erros de configuração, antes de tentar reiniciar o *daemon*. Para isso, execute:

```
#cd /usr/local/nagios
#bin/nagios -v etc/nagios.cfg
```

Uma estratégia de monitoramento bem planejada e realizada

de forma confiável pelo Nagios garante uma boa noite de sono, a menos que seja disparado um alerta, evidentemente. No entanto, ser acordado pelo Nagios apitando em seu celular ou pager definitivamente é melhor do que ser arancado da cama por um usuário irado no meio da noite. ■

Mais Informações

[1] Exemplos de arquivo de configuração: <http://www.linuxmagazine.com.br/arquivos/LM31/ezconfig.cfg>

Soluções
Completas em
Open Source



Suporte • Desenvolvimento • Treinamento

Av. Presidente Vargas, 962 - Grupo 1001
Centro - Rio de Janeiro/RJ • 20071-003

Tel.: (21) 2526-7262
Fax: (21) 2203-1748

www.linuxsolutions.com.br

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 2161-5400 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 Cantão – 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			✓	✓	✓	✓
Rio de Janeiro										
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4º andar Centro – CEP: 20030-012	21 2220-7055	www.nsi.com.br				✓		✓
Open IT	Rio de Janeiro	Rua do Mercado, 34, Sl, 402 – Centro – CEP: 20010-120	21 2508-9103	www.openit.com.br				✓		✓
Unipi Tecnologias	Campos dos Goytacazes	Av. Alberto Torres, 303, 1º andar - Centro – CEP 28035-581	22 2725-1041	www.unipi.com.br			✓	✓	✓	✓
Rio Grande do Sul										
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. Jurua, 159, Térreo – Alphaville – CEP: 06455-010	11 4195-2557	www.digivoice.com.br		✓	✓	✓	✓	✓
Dextra Sistemas	Campinas	Rua Antônio Paioli, 320 – Pq. das Universidades – CEP: 13086-045	19 3256-6722	www.dextra.com.br				✓	✓	✓
Insigne Free Software do Brasil	Campinas	Av. Andrades Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignesoftware.com				✓	✓	✓
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	www.microcamp.com.br				✓		✓
PC2 Consultoria em Software Livre	Carapicuíba	Rua Edeia, 500 - 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		✓	✓	✓		✓
Epopeia Informática	Marília	Rua Goiás, 392 – Bairro Cascata – CEP 17509-140	14 3413-1137	www.epopeia.com.br						✓
Redentor	Osasco	Rua Constante Piovani, 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	Av. Tiradentes, 615, Ed. Santiago, 2º andar Bom Retiro – CEP: 01101-010	11 3228-3709	www.wpc.com.br				✓	✓	✓
Big Host	São Paulo	Rua Dr. Miguel Couto, 58 – Centro – CEP: 01008-010	11 3033-4000	www.bighost.com.br	✓				✓	✓
Blanes	São Paulo	Rua André Ampère, 153 – 9º andar – Conj. 91 CEP: 04562-907 (próx. Av. L. C. Berrini)	11 5506-9677	www.blanes.com.br	✓	✓	✓		✓	✓
Commlogik do Brasil Ltda.	São Paulo	Av. das Nações Unidas, 13.797, Bloco II, 6º andar – Morumbi – CEP: 04794-000	11 5503-1011	www.commlogik.com.br	✓	✓	✓		✓	✓
Computer Consulting Projeto e Consultoria Ltda.	São Paulo	Rua 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 Carubeiras, 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	✓	✓	✓		✓	✓
Linux Komputer Informática	São Paulo	Av. Dr. Lino de Moraes Leme, 185 – CEP: 04360-001	11 5034-4191	www.komputer.com.br	✓		✓		✓	✓
Linux Mall	São Paulo	Rua Machado Bittencourt, 190, Cj. 2087 – CEP: 04044-001	11 5087-9441	www.linuxmall.com.br	✓			✓	✓	
Livraria Tempo Real	São Paulo	Al. Santos, 1202 – Cerqueira César – CEP: 01418-100	11 3266-2988	www.temporeal.com.br				✓	✓	✓
Locasite Internet Service	São Paulo	Av. Brigadeiro Luiz Antonio, 2482, 3º andar – Centro – CEP: 01402-000	11 2121-4555	www.locasite.com.br	✓				✓	✓
Microsiga	São Paulo	Av. Braz Leme, 1631 – CEP: 02511-000	11 3981-7200	www.microsiga.com.br			✓		✓	✓
Novatec Editora Ltda.	São Paulo	Rua Luis Antonio dos Santos, 110 – Santana – 02460-000	11 6979-0071	www.novateceditora.com.br			✓			
Novell América Latina	São Paulo	Rua Funchal, 418 – Vila Olímpia	11 3345-3900	www.novell.com/brasil			✓		✓	✓
Oracle do Brasil Sistemas Ltda.	São Paulo	Av. Alfredo Egídio de Souza Aranha, 100 – Bloco B – 5º andar – CEP: 04726-170	11 5189-3000	www.oracle.com.br					✓	✓
Proelbra Tecnologia Eletrônica Ltda.	São Paulo	Av. Rouxinol, 1.041, Cj. 204, 2º andar Moema – CEP: 04516-001	11 5052- 8044	www.proelbra.com.br	✓		✓			✓
Provider	São Paulo	Av. Cardoso de Melo, 1450, 6º andar – Vila Olímpia – CEP: 04548-005	11 2165-6500	www.e-provider.com.br			✓		✓	✓
Red Hat Brasil	São Paulo	Av. Angélica, 2503, 8º andar Consolação – CEP: 01227-200	11 3124-6000	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
Open Source Business Conference	22 e 23 de maio	San Francisco, EUA	osbc.com
IV Encontro de Software Livre do Amazonas	25 e 26 de maio	Manaus, AM	www.eslam.comunidadesol.org
Linux Tag 2007	30 de maio a 2 de junho	Berlim, Alemanha	www.linuxtag.org
3ª Semana do Software Livre da Universidade Federal do Ceará	6 a 9 de junho	Fortaleza, CE	www.sesol.ufc.br
OSS 2007	11 a 14 de junho	Limerick, Irlanda	oss2007.dti.unimi.it
Linux Day	23 de junho	São Paulo, SP	www.fiti.com.br
Latinoware 2007	13 e 14 de novembro	Foz do Iguaçu, PR	www.latinoware.org

Hospedagem de sites - VPS
IP Dedicado - Soluções de Voz
Servidores Dedicados - Colocation



FRACTO

www.fracto.com.br
(11) 3523-1580

Agente
Autorizado
Intelig

Índice de anunciantes

Empresa	Pág.
Celepar	15
Dextra	39
Easy Linux	43
Fracto	02
Intel	84
Itautec	07
Linux New Media	11
Linux Park	83
Linux Solutions	77
Linux World	81
LPI	55
Microsoft	09
Plugin	13
Xandros	29

OPEN Source.
OPEN Solutions.

OPEN. For Business.

LinuxWorld Conference & Expo – Worldwide Series

Tokyo	May 30 – June 1, 2007	www.idg.co.jp/expo/lw/
Seoul	June 20 – 23, 2007	www.linuxworldkorea.com
San Francisco	August 6 – 9, 2007	www.linuxworldexpo.com
Beijing	September 3 – 7, 2007	www.linuxworldchina.com
Stockholm	September 5, 2007	www.linuxworldsummit.se
London	October, 24 – 25, 2007	www.linuxworldexpo.co.uk
Utrecht	October 30 – November 1, 2007	www.linuxworldexpo.nl



World's leading Trade Event for Linux and Open Source in business

© Linux New Media do Brasil Editora Ltda.



INTERNATIONAL MEDIA SPONSOR

Na Linux Magazine #32...

DESTAQUE

Groupware

Um groupware é um sistema baseado em computador que auxilia grupos de pessoas envolvidas em tarefas ou objetivos comuns, e que provê interface para um ambiente compartilhado. O principal mote para a adoção do groupware nas empresas é a sua capacidade de tornar o trabalho em grupo mais eficiente, diminuir o tempo gasto nas atividades conjuntas e diminuir o custo de realização das atividades que devam ter mais de um executante. O Linux e o Código Aberto marcam pontos nesse mercado competitivo, mostrando que os sistemas livres sabem entrar no ritmo da sua empresa quando a palavra-chave é colaborar, inclusive interagindo com soluções proprietárias ou transferindo informações, de maneira segura, via Internet. ■



ANÁLISE

Amigo do pingüim

Software profissional dedicado a análises avançadas, tanto lineares quanto não-lineares, de processos e projetos de Engenharia, o Abaqus é famoso em todo mundo como sinônimo de ferramenta técnica de alta produtividade. O que pouca gente sabe, todavia, é que o Abaqus é compatível com sistemas Linux de longa data... e poderíamos até dizer que eles são amigos e trabalham juntos, colaborando em projetos como o desenvolvimento de modelos de carros de luxo para a Audi alemã! ■

TUTORIAL

Wireshark

O Wireshark (antigo Ethereal) é o capturador gráfico de pacotes mais usado em sistemas Linux. Porém, o roubo de informações não é sua única aplicação. Mostramos múltiplas utilidades do Wireshark em situações comuns em ambientes de rede corporativos. ■

Na EasyLinux #09...

DESTAQUE

Games no Linux

Nem só de trabalho duro vive o Linux. O sistema do Pingüim também surpreende quando o tema é games e faz rodar alguns dos jogos mais emocionantes da atualidade, feitos nos moldes dos sistemas proprietários. Como isso é possível? Através do Ceedega – software pago – ou do virtuoso Wine. Com algumas configurações e entradas básicas na linha de comando, você vai aprender a instalar jogos como o famoso *City of Heroes*, dentre outros. Não perca a série de artigos completa, com passo-a-passo, screenshots e soluções, especialmente preparada para a sua diversão! ■



LABORATÓRIO

Tudo sob controle

Você quer saber qual o uso que seu computador faz da CPU, memória e outros recursos, além de verificar o recebimento de emails? Delegue essa tarefa ao GKrellM, um programa enxuto, que oferece plugins adicionais, especialista em monitorar o sistema na forma de eficientes gráficos. ■



2º Seminário 2007:
**A importância do Software Livre
para o mercado brasileiro de TI**

28/06/2007 - Hotel Mercure - Belo Horizonte - MG

PATROCÍNIO



**Microsoft
Novell.**

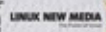
APÓIO



PROMOÇÃO



REALIZAÇÃO



ORGANIZAÇÃO





PENSE PARALELO

Novos Compiladores Intel® C++ e Fortran 10.0 Professional Editions

Agora oferecem a melhor alternativa para criar aplicações multi-thread nos ambientes Windows*, Linux* ou Mac OS* X. Somente os compiladores Professional Edition da Intel oferecem recursos de otimização avançado de código e potencialidades multi-threading que incluem vetorização, auto-paralelização, OpenMP*, prefetching de dados, desmembramento de loops e bibliotecas altamente otimizadas de rotinas multi-threading prontas, processamento matemático e de multimídia.

O Compilador Intel 10.0 Professional Edition possui bibliotecas de software que permitem a você programar no ambiente paralelo como um especialista desde o primeiro dia. Estas bibliotecas são constantemente atualizadas para uso automáticos de funcionalidades dos novos processadores.

O compilador e bibliotecas são pré-validados para trabalharem juntos:

- **Compiladores Intel® C++ e Fortran automaticamente paralelizam e otimizam seu código para melhor desempenho, para tirar máximo proveito dos processadores multi-core, com o mínimo esforço.**
- **Bibliotecas Matemáticas Intel® MKL 9.1 oferecem funções matemáticas para o ambiente multi-thread com o melhor desempenho nas plataformas multi-core.**
- **Intel® Integrated Performance Primitives 5.2 (somente para C++) são funções paralelas altamente otimizadas que aceleram o desenvolvimento de aplicações multimídia, de criptografia e de processamento de sinais.**
- **Intel® Threading Building Blocks 1.1 (somente para C++) consiste de rotinas otimizadas e testadas para simplificar o desenvolvimento de aplicações escaláveis e robustas com a utilização de recursos multi-thread.**



"Dentro de uma década, um programador que não pensar 'paralelo', não será um programador."

James Reinders

Evangelista Chefe de Software
da Intel Software Products

TAKE THE NEXT STEP—

Tech Digital
(11) 5181-1852
www.techdigital.com.br/intel

Katalogo
0800 7729897
www.katalogo.com.br/intel

Strattus
(11) 3531-6550

Itautec
0800 121444

MStech
(11) 5080-3838



Copyright © 2007 Intel Corporation. Intel, the Intel logo, Intel. Leap ahead. and the Intel. Leap ahead. logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. All rights reserved.