Snow666

LINUX NEW MEDIA
The Pulse of Open Source

LINUX PARK 2008 P.28
Em Brasília, é hora do SL/CA

CEZAR TAURION P.26
SaaS e o Código Aberto estão transformando a indústria

COLUNA DO MADDOG P.27
Em busca do próximo Einstein

48 Novembro 2008

LINUX MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

AUTENTICAÇÃO

QUANTO MAIS USUÁRIOS NA REDE, MAIOR É O TRABALHO DO ADMINISTRADOR. A MENOS QUE EXISTA UMA BOA SOLUÇÃO DE AUTENTICAÇÃO E GERENCIAMENTO DE IDENTIDADE p.33

Edição de ANIVERSÁRIO

exemplar de Assinante
venda proibida

© Linux New Media do Brasil Editora Ltda.

Snow666

NovaForge™

Nós conectamos nossos Clientes a nossos Centros de Competências de Software Livre

NovaForge, no centro da abordagem Industrial para Desenvolvimento de Sistemas da Bull.

O NovaForge é um poderoso conjunto de ferramentas e serviços amplamente testados e projetados para reduzir o esforço, otimizar custos de gestão e cronogramas, garantindo a qualidade dos produtos finais em Projetos de Desenvolvimento de Sistemas. O NovaForge foi concebido para ser utilizado em Projetos de Desenvolvimento e Atualização de Aplicações em ambientes J2EE, PHP e .net , na manutenção de aplicações desenvolvidas por terceiros e para o teste profissional e integrado dos sistemas.

BULL

Architect of an Open World™

www.bull.com

© Linux New Media do Brasil Editora Ltda.

Expediente editorial

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

Editor
Pablo Hess
phess@linuxmagazine.com.br

Revisora
Aileen Otomi Nakamura
anakamura@linuxmagazine.com.br

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

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

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

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

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

Amy Phalen (Estados Unidos)
aphalen@linuxmagazine.com

Hubert Wiest (Outros países)
hwiest@linuxnewmedia.de

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

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

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 conseqüências que advenham de seu uso. A utilização de qualquer material da revista ocorre por conta e risco do leitor.

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

Linux é uma marca registrada de Linus Torvalds.

Linux Magazine é publicada mensalmente por:

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

Direitos Autorais e Marcas Registradas © 2004 - 2008:
Linux New Media do Brasil Editora Ltda.

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

Atendimento Assinante

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

ISSN 1806-9428 **Impresso no Brasil**

INSTITUTO VERIFICADOR DE CIRCULAÇÃO

Aquisições e a crise

Prezados leitores,

Ao fim de mais um frutífero e agradável ano de convívio, é muito interessante recapitular alguns dos eventos mais marcantes dos últimos doze meses no universo do Software Livre e de Código Aberto (SL/CA) – destacado de toda a história anterior desse mercado pelo volume jamais visto de fusões e aquisições entre seus principais *players*.

Há doze meses, a BEA recusava a oferta da Oracle para sua aquisição – posição essa que seria revertida poucos meses depois, concretizando-se a compra. Pouco depois, Novell e Microsoft comemoravam o primeiro ano de seu acordo de cooperação, anunciando grande sucesso na parceria, para ambos os lados.

O lançamento do KDE 4 em janeiro sugeria a iminente ocorrência de uma revolução no visual do desktop de código aberto, mas até o momento a adesão à nova série desse popular ambiente ainda não conseguiu recuperar os usuários perdidos para seu maior concorrente. A iniciativa Creative Commons completou cinco anos, com muitas festas e uma retrospectiva de Lawrence Lessig, idealizador do movimento.

A Red Hat se despediu de seu CEO Matthew Szulik e contratou o então COO da Delta Airlines Jim Whitehurst, com grande alarde e resultados financeiros positivos logo em seguida.

A criação da LiMo Foundation, voltada à criação e promoção de telefones celulares com Linux embarcado, foi um dos pontos altos do SL/CA e do mercado móvel no início de 2008. Porém, teria chamado mais atenção não fosse pela aquisição da MySQL AB e da Innotek (fabricante do VirtualBox) pela Sun, enquanto a Trolltech era incorporada pela Nokia e o Yahoo se debatia ao máximo para evitar sua própria aquisição pela Microsoft – chegando até mesmo a "se oferecer" para o concorrente Google.

Nos meses seguintes começavam os esforços da Microsoft para obter a aprovação de seu formato de documento OOXML pela ISO como padrão internacional – que seriam coroados pouco depois com a aprovação. O resultado foi contestado – pela primeira vez na história do órgão internacional – por diversos órgãos nacionais e enfraqueceu a imagem da ISO como representante imparcial da indústria e dos consumidores de tecnologia.

No mercado editorial, a aquisição da Linux Magazine americana pela alemã Linux New Media AG (da qual a **Linux Magazine** brasileira é uma subsidiária) em junho mostrou o crescimento também do ecossistema do SL/CA, acompanhando essa indústria em pleno desenvolvimento.

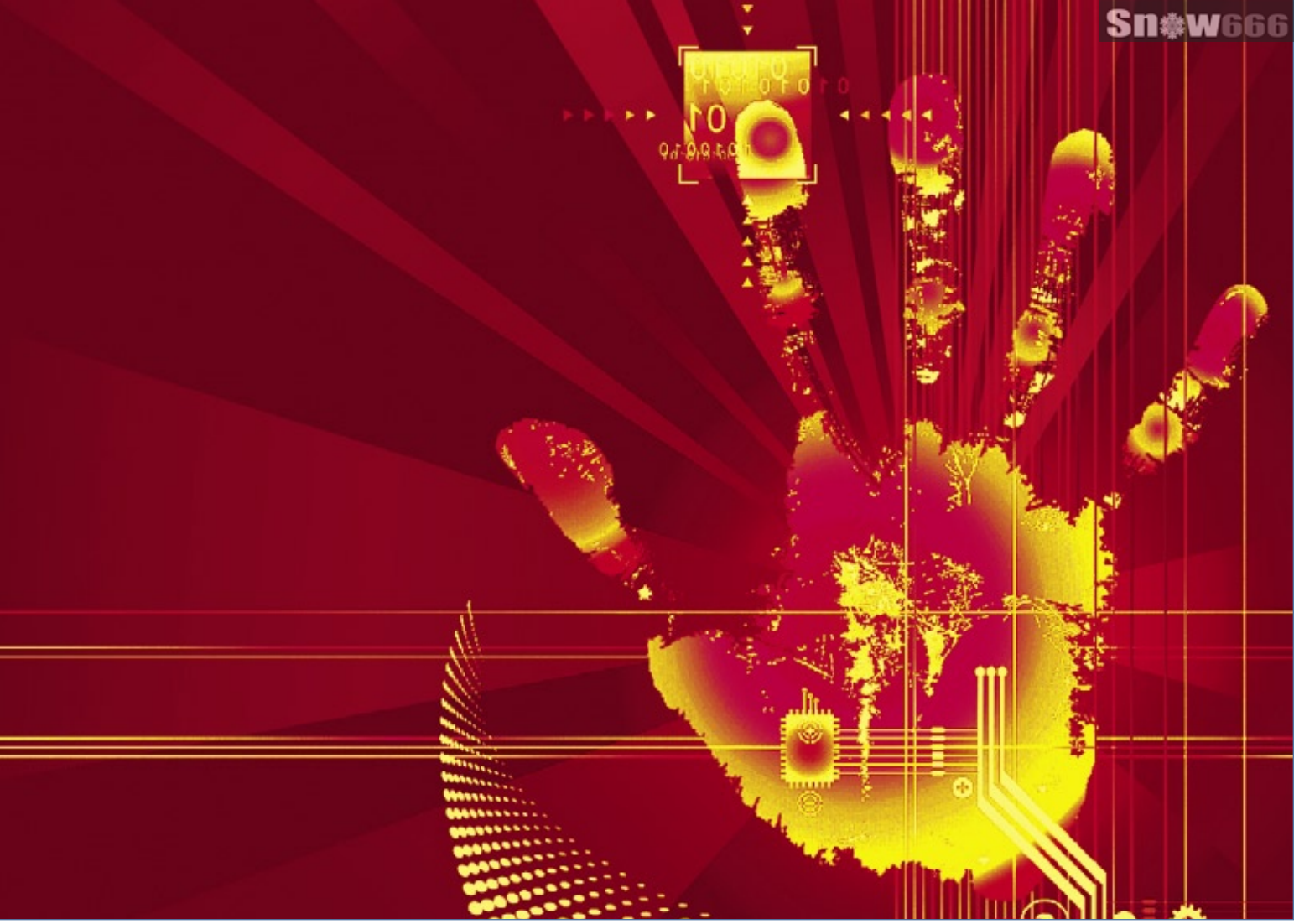
Mais recentemente, as aquisições da Jabber e da Qumranet por Cisco e Red Hat, respectivamente, finalizaram, até o momento, o frenesi de compras – que agora deve ser reduzido, com a deflagração de uma nova crise financeira mundial.

Por ora, a instabilidade financeira internacional deve se refletir num mercado mais estável no SL/CA – e potencialmente até com crescimento dos mais capazes de tirar proveito do cenário de falta de crédito.

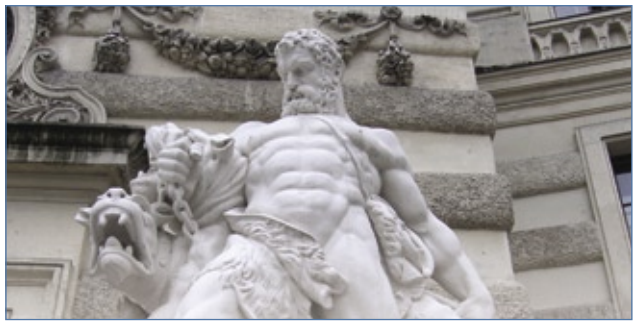
Pablo Hess
Editor

© Linux New Media do Brasil Editora Ltda.

Snow666



CAPA



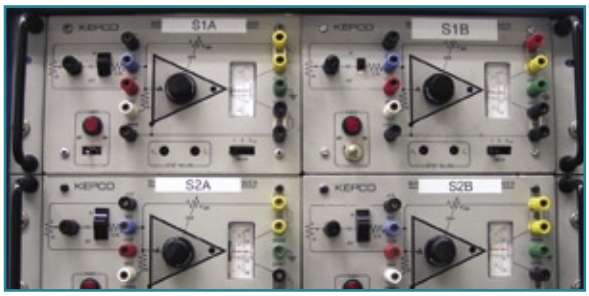
© Linux New Media do Brasil Editora Ltda.

COLUNAS

NOTÍCIAS

CORPORATE

REDES



SEGURANÇA

PROGRAMAÇÃO

SERVIÇOS

© Linux New Media do Brasil Editora Ltda.

Snow666

Emails para o editor

Permissão de Escrita

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

Quarto aniversário

Gostaria de parabenizar pela contínua qualidade com que a Linux Magazine vem trazendo mensalmente às bancas o mundo do GNU/Linux. Sou um assinante inveterado há três anos e muito pude observar durante essa caminhada que em breve completará quatro anos divulgando e informando o sistema operacional Linux e sistemas de código aberto.

Recentemente, ao passar no LPIC1, recebi um exemplar da Linux Magazine Internacional e pude notar que a versão Tupiniquim não fica nada a desejar em relação à estrangeira, a qualidade das reportagens e o conteúdo editorial e gráfico são excelentes. Contudo, gostaria de ver no futuro as 100 páginas que havia antes e que compõe a revista importada, salientando ainda que esta última possui as páginas no tamanho A4, maior que a nossa.

Como sugestão, gostaria de relatar um fato que freqüentemente vem me assolando. Recentemente, necessitei rever uma certa reportagem, mas não sabia em que revista procurar, já que tenho 38 edições. Assim, seria interessante que a revista disponibilizasse, em seu site ou num encarte especial, um índice ou sumário de todas as reportagens e colunas organizados por assunto, título e softwares envolvidos, para uma posterior consulta. Isso facilitaria e muito as pesquisas por soluções, pois às vezes uma certa reportagem que lemos pode não ter muito interesse agora, mas no futuro poderá ser bem proveitosa.

Atenciosamente,

Gunther Boeckmann, Recife/PE

Resposta

Caro Gunther, muito obrigado pelos parabéns. Com seu depoimento, sabemos que estamos no caminho certo para fornecer a informação de que nossos leitores precisam.

Em relação ao tamanho da revista, a seção Linux User, voltada aos usuários de desktops, ocupa aproximadamente dez páginas da Linux Magazine Internacional, mas, no Brasil, essa mesma seção integra a revista Easy Linux, que agora tem 68 páginas. Ou seja, nossas publicações brasileiras sobre Linux e Software Livre totalizam 152 páginas e também cobrem os usuários de desktops e os profissionais de TI. Já com relação ao tamanho físico das páginas, trata-se de uma questão operacional: o formato usado na Linux Magazine e na Easy Linux é o padrão do mercado brasileiro, portanto o parque gráfico brasileiro não contemplaria de forma satisfatória o formato A4.

No site da Linux Magazine temos também uma ferramenta de busca capaz de procurar artigos, notícias e matérias online com base nas palavras acessíveis gratuitamente. Porém, gostamos da dica de um índice detalhado de todas as matérias que já publicamos.

Parabéns por sua certificação. Desejamos muito sucesso no futuro. ■

© Linux New Media do Brasil Editora Ltda.

Snow666

caixa.gov.br

SOLUÇÕES BASEADAS EM SOFTWARE LIVRE E PADRÕES ABERTOS.

ESSA É A MANEIRA DA CAIXA SE CONECTAR AO FUTURO.

Nas lotéricas, na Universidade Corporativa, na nova rede de auto-atendimento, a CAIXA baseia suas soluções de TI em LINUX e em outros softwares livres. Isso faz da CAIXA uma das instituições bancárias líderes mundiais na utilização de padrões abertos e uma referência em inovação, criatividade e eficiência tecnológica no país.

Central de Atendimento CAIXA: 0800 726 0101,
0800 726 2492 (para pessoas com deficiência auditiva).
Ouvidoria CAIXA: 0800 725 7474

CAIXA

© Linux New Media do Brasil Editora Ltda.

Snow666

COLUNA

Pergunte ao Klaus!

Klaus Knopper

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

por Klaus Knopper

Freqüência não suportada

Eu uso dois monitores no Windows, mas o Linux diz "Unsupported Frequency" e desliga um dos monitores em seguida. Como posso resolver isso e usar os dois monitores no Linux também?

Resposta

Não é o Linux que diz "Unsupported Frequency", mas seu monitor (que se desliga em seguida). Assim como você fez quando configurou o driver do Windows para dois monitores, é preciso fazer o servidor X usar ambos os monitores, além da forma como você pretende fazer isso (isso é, um monitor como extensão do outro, ou em paralelo). O site http://gentoo-wiki.com/HOWTO_Dual_Monitors tem uma boa descrição em inglês de como fazer isso.

Normalmente, não é necessário um "driver" especial para isso, mas é preciso adicionar uma entrada no arquivo `/etc/X11/xorg.conf`

Dois monitores

Tenho dois monitores e uma placa de vídeo Nvidia Geforce 7100. O Fedora 9 que eu uso reconhece os dois monitores, e eu gostaria de ter dois desktops independentes.

Quando acesso o menu de configuração do desktop, ele me permite ativar o segundo monitor, mas quando eu reinicio o ambiente gráfico para ativar as mudanças, tudo volta às configurações originais. Você pode me ajudar?

Resposta

Se você quer duas áreas de trabalho independentes, você vai usar um monitor por placa de vídeo, e também precisará iniciar um servidor X por placa gráfica. Note que isso é diferente de uma configuração com dois monitores para criar uma área de trabalho "maior" que use ambos. Para esse segundo caso, o site http://gentoo-wiki.com/HOWTO_Dual_Monitors possui uma boa descrição de como fazê-lo.

O motivo da falha descrita por você é que reiniciar apenas um servidor X é insuficiente. Em vez disso, é preciso garantir que estejam rodando dois servidores X com dois arquivos `xorg.conf` independentes – o primeiro, por exemplo, com:

```
Xorg -config /etc/X11/xorg-0.conf :0
```

e o segundo com:

```
Xorg -config /etc/X11/xorg-1.conf :1
```

Para usar as placas de vídeo corretas (provavelmente a opção `PCI` da seção `Device`), é preciso editar tanto o `xorg-0.conf` quanto o `xorg-1.conf`. Agora, não sei se a sua placa Nvidia é reconhecida como duas placas independentes. Em caso positivo, ela deve mostrar duas entradas no comando `lspci -v`. Para descobrir os números PCI para cada `xorg.conf`, pode-se usar os endereços mostrados pelo `lspci -n`, mas talvez seja simplesmente impossível com essa placa.

Se for o caso, ou se você decidir instalar uma outra placa, é preciso garantir que o gerenciador de login (*XDM*, *GDM* ou *KDM*) inicie dois servidores X. Tente encontrar o arquivo `Xservers` correspondente ao seu gerenciador de login (`updatedb ; locate Xservers`) e adicione outra linha para iniciar o segundo servidor:

```
/etc/X11/xdm/Xservers:

:0 local /usr/bin/X :0 vt7 -config /etc/X11/xorg-
➥0.conf -nolisten tcp
:1 local /usr/bin/X :1 vt8 -config /etc/X11/xorg-
➥1.conf -nolisten tcp
```

Na próxima vez em que o XDM for executado, ele vai iniciar dois servidores X, cada um usando uma placa com um monitor ligado a ela e mostrando uma tela de login.

Um possível problema que eu imagino seria tentar determinar qual teclado e qual mouse devem ser os correspondentes a cada servidor X. Para usar essa configuração, será necessário instalar um segundo par de teclado e mouse. ■

© Linux New Media do Brasil Editora Ltda.

DPZ

© Linux New Media do Brasil Editora Ltda.

Novo Librix Desktop 3.0, agora em 3D. É só instalar e sair trabalhando.

A liberdade do novo Librix Desktop 3.0 não termina no código aberto. Oferece programas cada vez mais compatíveis e comumente usados em sistemas proprietários, além de ter total compatibilidade com os equipamentos padrão de mercado. Sua plataforma está mais moderna, amigável e o sistema totalmente configurável na instalação. Assim como todo produto Itautec, já foi testado, aprovado e tem assistência técnica em todo o país. Liberdade, interoperabilidade e facilidade de uso, isso é TI. Isso é Tecnologia Itautec.

Acesse www.itautecshop.com.br ou ligue 0800 121 444.

COMPROMISSO COM A SUSTENTABILIDADE

Itautec

Snow999

COLUNA

FireHOL

Charly Kühnast

Se você não tem tempo para ajustar regras complexas de firewall, talvez valha a pena conferir a inteligente técnica do FireHOL.

por Charly Kühnast

Não existe lugar como a nossa casa. Eu ouço um som baixo e constante vindo do armário da cozinha. Pelo menos está baixo até eu abrir a porta. Depois, ouço o barulho de um motor defeituoso de avião. Entre óleo, cera para sapato e potes aleatórios está a tecnologia que me conecta ao mundo externo. Ao lado dos modems fornecidos pela minha empresa telefônica e um Cisco asmático – culpado pela maior parte do barulho – está um idoso PC, meu firewall.

Originalmente, minhas regras manuais de *iptables* cuidavam somente do *masquerading* para conexões vindas da LAN e destinadas ao mundo externo, com algumas regras personalizadas para servidores individuais. Ao longo do tempo, as regras se tornaram mais complexas, enquanto eu procurava uma ferramenta de gerenciamento.

Finalmente, encontrei o *FireHOL*[1]. Ao contrário do *Firewall Builder*[2], o FireHOL não precisa de uma interface gráfica. Em vez disso, basta adicionar diretivas simples a um arquivo de configuração e o FireHOL as traduz para comandos do iptables.

Se você só precisa de masquerading e deseja restringi-lo ao tráfego HTTP, basta essa pequena configuração:

```
interface eth0 home
     client all accept
interface eth1 internet
     client all accept
router to-internet inface eth0 outface eth1
     masquerade
     route http accept
```

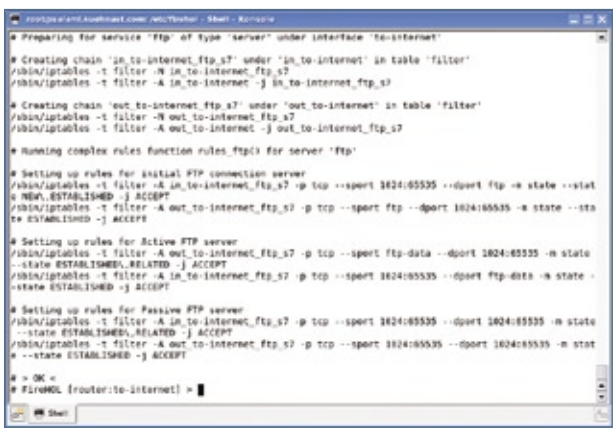


Figura 1 O FireHOL reduz o esfoço administrativo envolvido com a configuração de um firewall. Essa tela mostra um arquivo de controle para conexões FTP.

As linhas `client all accept` permitem que o firewall estabeleça conexões arbitrárias na LAN e na Internet.

Para evitar restringir o masquerading ao HTTP e abrir a porta para qualquer protocolo, basta mudar a última linha assim:

```
     route all accept
```

Com base nessa diretiva, o FireHOL gera várias dezenas de comandos iptables. O motivo disso é que ele tem uma forma especial de lidar com protocolos complexos como FTP ativo, por exemplo. A **figura 1** mostra parte das regras que tratam o FTP.

O FireHOL pode ter seu funcionamento observado e oferece uma prática função `explain` para facilitar essa tarefa. Pode-se usar o shell interativo para digitar regras na sintaxe exibida no exemplo de código, e a ferramenta responde com as regras de iptables correspondentes, que o FireHOL aplicará se você pedir para ele.

Depois de simplificar em silêncio o gerenciamento do meu firewall doméstico, agora tenho tempo para pensar em fazer alguma coisa com o barulho que vem do armário. ■

Mais informações

[1] FireHOL: http://firehol.sourceforge.net

[2] Firewall Builder: http://www.fwbuilder.org/

© Linux New Media do Brasil Editora Ltda.

Snow666

A Xandros é líder em inovação. De desktops a servidores e de groupware ao licenciamento de sistemas operacionais, a Xandros dita o ritmo da tecnologia com uma rede global e suas inovações em Netbooks, Moblin, utilização do processador e consumo de energia. A Xandros está redefinindo a forma como são feitos PCs e dispositivos móveis, e adaptando-se ao nosso mundo em constante mudança.

Entre em contato com a Xandros hoje para descobrir como a sua empresa pode fazer as nossas inovações funcionarem a seu favor.

xandros

jamesl@xandros.com | www.xandros.com.br
646-747-7640 | 0800-891-6799

© Linux New Media do Brasil Editora Ltda.

COLUNA

Crônicas do kernel

Zack Brown

Nova documentação de qualidade, um repositório de firmware e um monitor para o barramento PCI.

por Zack Brown

Desenvolvimento do kernel para empregadores

Jonathan Corbet escreveu uma bela e longa documentação sobre desenvolvimento do kernel da perspectiva dos empregadores e desenvolvedores que trabalham para eles. O documento foi escrito para ser incluído nos fontes do kernel, mas talvez também seja abrigado no site kernel.org.

A principal questão parece ser o fato de que aprender as minúcias do processo e da cultura de desenvolvimento ajudam as empresas a gerenciar suas próprias expectativas e chegar mais rápido onde desejam.

Como diz Jonathan nos parágrafos introdutórios, "o processo de desenvolvimento do kernel pode parecer estranho e intimidador para novos desenvolvedores, mas há bons motivos e uma experiência sólida por trás dele.

O desenvolvedor que não compreender como funciona a comunidade do kernel (ou, pior ainda, que tentar contorná-la) terá uma experiência frustrante. A comunidade de desenvolvedores, apesar de ajudar quem precisa aprender, não tem tempo para quem não quer escutar ou não se importa com o processo de desenvolvimento".

Isso certamente é verdade. Há vários exemplos de desenvolvedores que tentaram – durante anos, em alguns casos – forçar a entrada de seu código no kernel (um exemplo relativamente recente é o *ReiserFS*), para descobrir que os desenvolvedores perderam interesse.

O documento começa com uma introdução geral ao valor de ter seu código incluído na árvore oficial, as várias questões de licenciamento e uma explicação de números de versão e calendários de lançamento.

Segue-se uma explicação detalhada do "ciclo de vida" de patches enviados. Essa parte descreve as várias ferramentas e listas de email que podem ser úteis para novos desenvolvedores. Depois, o documento explica em detalhes tudo que um desenvolvedor precisaria fazer, desde a idéia até a implementação e a incorporação do código à árvore, incluindo uma lista de armadilhas a evitar, como problemas advindos do uso de `#ifdef`.

O documento é bastante profundo e compõe um panorama bastante impressionante e orientado ao usuário a respeito do desenvolvimento cultural da comunidade desenvolvedora do kernel.

Jonathan já contribuiu com vários ótimos textos para a comunidade Linux ao longo dos anos, e esse documento é outro excelente esforço de sua parte. Além disso, incorporando o texto aos fontes do kernel, ele se torna parte de um documento vivo que já recebeu inúmeras sugestões e alterações de pessoas como Andrew Morton e outros.

Leia-o online em: `http://ldn.linuxfoundation.org/book/1-what-this-document-is-about`.

Repositório de firmwares

Seguindo o esforço geral de eliminar firmwares binários dos fontes do kernel, David Woodhouse anunciou um novo repositório git para firmwares, que incluirá não apenas aqueles hoje distribuídos com os fontes do kernel, mas também qualquer outro cujo fabricante deseje disponibilizar para Linux.

PCItop

Rick Jones, da HP, anunciou a nova ferramenta *PCItop*. Lançada sob a GPL, ela é semelhante ao clássico utilitário *top* de monitoramento do sistema, e informa toda a atividade no barramento PCI. Atualmente, somente sistemas HP Integrity são suportados, mas Rick convidou todos a se juntarem a ele para incluir suporte a outras plataformas. ■

Sobre o autor

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

© Linux New Media do Brasil Editora Ltda.

Os melhores servidores – Os melhores preços

Novo!

Só profissionais

HOT

Olá, nós falamos português.
Visite o nosso live chat:
www.server4you.com

Por que SERVER4YOU?

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

Microsoft GOLD CERTIFIED Partner

Parallels Gold Partner

SERVER4YOU

	POWER L	PREMIUM XL
Processador	Intel Pentium IV, 2.8 GHz	AMD Opteron 146
Memória RAM	512 MB DDR2 RAM	2048 MB DDR2 RAM
Disco rígido	80 GB SATA (7200 RPM)	2x 120 GB SATA (7200 RPM)
Tráfego mensal	2000 GB inclusos no pacote	4000 GB inclusos no pacote
Infra-estrutura de software	Grátis: Fedora 8, CentOS 5, Debian 4, Ubuntu 8 e PLESK 8! Windows 2003 Server Enhanced Edt. – gastos ad. $12.00/mês	
Recursos adicionais	Grátis: PowerFeatures: PowerReboot, PowerRecovery, PowerRestore etc.	
Suporte	Grátis: 24x7 suporte técnico	
Preço por mês a partir	$49.00 $0 INSTALAÇÃO GRÁTIS	$119.00 $0 INSTALAÇÃO GRÁTIS

Preços em dólares. Impostos incluídos.

Servidores Dedicados Premium

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

Datacenter em St. Louis, EUA

WWW.SERVER4YOU.COM

© Linux New Media do Brasil Editora Ltda.

COLUNA

Ataques contra o DNS, o centro macio da Internet

Insegurança

Seus sistemas estão seguros contra ataques ao DNS? Veja como eles são importantes e como determinar se você está vulnerável.

por Kurt Seifried

Assim como na maioria dos protocolos originais nos quais a Internet se baseia, as decisões originais de projeto que levaram a sua popularidade e sucesso agora voltam para nos assombrar com problemas de segurança.

Tenha em mente que quando a Internet foi criada, ela era uma comunidade relativamente pequena e bem conectada. A segurança não estava numa posição muito alta na lista de preocupações – simplesmente fazê-la funcionar e obter algo útil dela já era suficientemente incrível.

A importância dos ataques

Como tenho certeza de que você sabe, o DNS fornece um dos serviços infra-estruturais mais fundamentais da Internet – especificamente, a tradução de nomes legíveis como *www.linuxmagazine.com.br* para endereços IP como 189.14.98.138. Esse serviço é importante porque permite o registro de um nome estático, mas os serviços subjacentes podem ser locais arbitrários e podem ser criados ou movidos com facilidade. Por exemplo, eu fiz *outsourcing* do meu email, de *seifried.org* para o Gmail.

Dependência

Portanto, nós dependemos do DNS toda vez que usamos outro protocolo ou serviço, incluindo email, a Web, clientes de mensagem instantânea, VoIP etc. Se agressores conseguirem iniciar ações hostis, como redirecionar *www.seubanco.com.br* para seus servidores, eles conseguirão executar qualquer ataque, como sites forjados, ler seus emails e assim por diante.

Por que o DNS é rápido (e inseguro)

Uma das melhores decisões foi tornar o DNS um protocolo extremamente leve e rápido. A maioria das requisições e respostas usam o protocolo UDP, que não depende de estado e é semelhante a enviar uma mensagem de texto por SMS (respostas maiores podem resultar numa sessão baseada em TCP).

Então, estamos limitados em relação à quantidade de dados que podem ser enviados, e não saberemos se a outra ponta da conexão os recebeu ou sequer respondeu; ficamos apenas esperando uma resposta.

Um pacote UDP é o mais simples possível – contém as informações básicas de endereço (IPs e portas de origem e destino) e as informações dos pacotes (tipo, comprimento, *checksum*, dados).

O UDP não possui um mecanismo de segurança significativo para garantir que o pacote tenha vindo da máquina alegada ou que seja parte de uma transação legítima, o que é bom para a velocidade.

Se você enviar uma requisição, pode apenas esperar receber uma resposta, permitindo que os servidores DNS lidem com grandes volumes de requisições. Na verdade, em 2007, os servidores raiz receberam na ordem de 4 bilhões de requisições por dia.

Pacote UDP forjado

Para forjar um pacote UDP, é preciso saber os endereços IP e portas usados, o que é trivial em requisições DNS, pois os endereços IP são conhecidos (o servidor que faz a requisição e o que responde) e, como se trata de uma requisição DNS, a porta de destino sempre é a 53. Isso deixa somente a porta de origem a ser determinada, e como vários sistemas operacionais simplesmente usam uma porta estática para conexões de saída, ou portas incrementadas uma a uma para cada requisição de saída, é relativamente fácil um agressor adivinhar esse número.

© Linux New Media do Brasil Editora Ltda.

ID da transação

Como tentativa para resolver o problema de forjar pacotes no protocolo DNS, foi adicionada uma ID de transação. Um simples número de 16 bits – com 65.536 possibilidades – que é enviado na requisição e deve ser copiado no pacote de resposta teoricamente evita que um agressor forje cegamente as respostas, pois ele passa a precisar adivinhar a ID da transação.

Infelizmente, criar valores aleatórios realmente bons é surpreendentemente difícil, e algumas implementações do *Bind* simplesmente usam IDs de transação incrementados em um a cada requisição, tornando-as completamente previsíveis. Agora estamos de volta ao estágio em que o agressor consegue facilmente forjar um pacote e inserir dados hostis num servidor DNS.

Como funciona

Então, como os agressores exploram essa falha? A primeira coisa que eles fazem é encontrar um servidor vulnerável e um domínio que queiram controlar (por exemplo, *www.seubanco.com.br*). Depois, encontram uma máquina capaz de usar o servidor DNS vulnerável para consultas DNS.

Grandes provedores são bons alvos, pois comprometê-los dá aos agressores acesso a milhares de clientes, e então comprometer uma única máquina para desferir o ataque deixa de ser um problema.

Alto volume

Alternativamente, o agressor pode usar *JavaScript* para criar uma página web que realize o ataque e depois fazer uma consulta ao DNS por *www.seubanco.com.br* e tentar forjar pacotes com dados hostis para o servidor DNS do provedor.

Outro motivo pelo qual o sucesso desse ataque é tão provável é que o DNS é um serviço de alto volume e que poucos sites registram as requisições de entrada e saída, então a detecção de um ataque é extremamente improvável. Os agressores podem simplesmente atirar qualquer dado ao servidor, fazendo milhares de requisições e forjando respostas até terem sucesso.

```
[user@vmware1 ~]# dig @fixed.example.org +short porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"68.151.45.105 is GREAT: 78 queries in 49.5 seconds from 28 ports with std dev 1
7516"
[user@vmware1 ~]# dig @broken.example.org +short porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"68.151.45.105 is POOR: 26 queries in 1.7 seconds from 1 ports with std dev 0"
[root@vmware1 ~]#
```

Figura 1 Um teste de DNS.

Você está vulnerável?

Existem testes via Web e por linha de comando que verificam essa vulnerabilidade. Eles geralmente fazem diversas consultas DNS, que são examinadas, procurando números de porta e IDs de transação em busca de aleatoriedade, e os resultados são rapidamente visualizados. Em [1] e [2] há dois testes via Web.

Além disso, o centro DNS-OARC oferece uma verificação por linha de comando (**figura 1**) que pode ser acessada com uma ferramenta como o *dig* ou o *nslookup*:

```
$ dig @ip.ou.nome +shot porttest.
➥dns-oarc.net TXT
```

Para consertar a vulnerabilidade, é preciso atualizar o servidor DNS; quase todos os fabricantes liberaram atualizações em julho. Após atualizar seu servidor DNS, presumindo que o Bind responda por esse serviço, certifique-se de que ele esteja corretamente configurado.

Para isso, verifique o arquivo `named.conf` e assegure-se de não ter nele algo como:

```
query-source port 53;
query-source-v6 port 53;
```

mas sim algo como:

```
query-source port *;
query-source-v6 port *;
```

Depois de atualizar, você deve usar um dos testes via Web ou linha de comando para garantir que esteja funcionando conforme esperado.

Conclusões

Ataques DNS ilustram tanto as limitações de alguns protocolos usados na Internet quanto a robustez inerente ao sistema, e é improvável que esse tipo de ataque venha a desaparecer.

Mesmo com a publicidade em torno do tema, uma parcela significativa – superior a 50 por cento, de acordo com alguns relatórios – dos servidores DNS ainda não foram consertados. Assim como o spam, esse tipo de ataque é algo com o qual teremos que aprender a conviver. ■

Mais informações

[1] DoxPara: http://www.doxpara.com/

[2] DNS-OARC: http://www.dns-oarc.net/

Sobre o autor

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

© Linux New Media do Brasil Editora Ltda.

Snow666

COLUNA

5 de outubro: 130 milhões de brasileiros usando Linux

Augusto Campos

A presença de Linux e software livre em todas as urnas eletrônicas é ponto para o Brasil.

por Augusto Campos

No primeiro domingo de outubro, 130 milhões de brasileiros puderam participar diretamente de um dos maiores deployments do Linux no mundo, fato que na ocasião passou despercebido por muitos. As eleições municipais de 2008 foram mais um marco para nosso país: se desde 2000, quando as urnas eletrônicas foram aplicadas pela primeira vez em 100% dos municípios brasileiros, somos o maior case deste tipo no mundo, e a partir de agora somos também o maior case de uso do software livre nesse tipo de aplicação.

> ***A interface com o usuário permanecia a mesma adotada nos anos anteriores, e assim o eleitorado brasileiro usou o Linux sem perceber.***

Espalhadas pelos 5.563 municípios brasileiros, havia uma urna eletrônica em cada uma das mais de 400.000 seções eleitorais do país, e em todas elas rodava o kernel Linux, acompanhado por um conjunto de outros softwares livres (bibliotecas básicas etc.) e dos aplicativos desenvolvidos pela própria Justiça Eleitoral.

E, como esperado, para os eleitores nada disso era especialmente visível. A interface com o usuário permanecia a mesma adotada nos anos anteriores, e assim o eleitorado brasileiro usou o Linux sem perceber, da mesma forma como fazem tantos clientes de caixas eletrônicos, operadores de caixa de supermercados e outras categorias de usuários de aplicações.

Para os técnicos dos TREs e até mesmo para os mesários, a presença do Linux era um pouco mais visível. Ainda que não haja acesso a uma shell comum e muito menos a um ambiente gráfico desktop, ao ligar a urna é possivel acompanhar o boot do kernel, apresentado da maneira tradicional, com as linhas de texto correndo em uma tela de console e o logo do Tux exibido no topo, orgulhosamente à frente da imagem de uma urna, ao lado do brasão da República e da identificação da Justiça Eleitoral.

As urnas brasileiras adotam a arquitetura do PC, com processador compatível com a linha x86 da Intel, mas com desempenho e demais capacidades adaptadas à (baixa) demanda do processo eleitoral, que ocorre offline e com pouco processamento local. Até mesmo os procedimentos criptográficos adotados (baseados em padrões abertos) estão ao alcance de CPUs com clock bem menor que a do seu computador pessoal.

Deixar de ter de dotar de caros sistemas operacionais proprietários um parque de tantas centenas de milhares de equipamentos certamente pode economizar recursos que serão melhor empregados na robustez, autonomia e até na logística associada a estes equipamentos. Mais do que pelo aspecto econômico, entretanto, a iniciativa merece ser avaliada pelo que significa em termos de transparência e segurança.

Quanto à abertura do código dos aplicativos, já houve avanços com as normas que passaram a exigir que o código-fonte fique à disposição da OAB, do Ministério Público e de todos os partidos, que depois assinam digitalmente o executável gerado publicamente a partir desses fontes. Mas a substituição do sistema operacional fechado pelo Linux é um passo muito mais visível, e ajuda até mesmo a provocar a discussão sobre a adoção do código aberto em mais aplicações governamentais. Ponto para o Brasil! ■

Sobre o autor

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

© Linux New Media do Brasil Editora Ltda.

Snow666

Complete a sua coleção

Mais informações

Site:

www.linuxmagazine.com.br

Tel: 11 4082-1300

LINUX MAGAZINE

LINUX NEW MEDIA
The Pulse of Open Source

© Linux New Media do Brasil Editora Ltda.

Snow666

DVD do assinante

Librix Desktop 3.0

O DVD distribuído aos assinantes nesta edição traz o Librix Desktop 3.0, uma distribuição nacional flexível e de alta qualidade.

por Pablo Hess

Controle sobre o hardware é algo que falta à maioria dos fabricantes de software. Muitos atribuem a famosa instabilidade do próprio Windows ao fato de seu fabricante, a Microsoft, não ter controle sobre as peças usadas nas máquinas equipadas com o sistema. No caso do Linux, essa falta de controle dos distribuidores sobre o hardware se reflete em uma maior dificuldade na integração dos aplicativos à máquina física.

Uma distribuição brasileira, no entanto, não sofre desse problema. O Librix, desenvolvido pela Itautec com base no Gentoo, roda com perfeição nos computadores da empresa.

Na edição do quarto aniversário da **Linux Magazine**, os assinantes que optaram pela modalidade com DVD recebem junto com seus exemplares um DVD de instalação do Librix Destkop 3.0, que agora podem testar e instalar em qualquer PC.

Após a série 2.x, o Librix fez grandes avanços em usabilidade e autoconfiguração, que valem a pena conferir.

A instalação do sistema, bem mais longa do que a maioria das outras distribuições, continua sendo um ponto a ser melhorado. Nesse ponto, o culpado é o sistema de pacotes herdado do Gentoo, que prima pela flexibilidade mas que, com isso, perde em velocidade. A facilidade do processo de instalação, no entanto, é justamente a que se espera de uma distribuição que contempla os usuários iniciantes.

Figura 1 Há vários conjuntos de pacotes a selecionar.

Pacotes

Por padrão, o sistema utiliza uma seleção de pacotes adequada para desktops. Porém, os usuários avançados têm a possibilidade de personalizar essa seleção a partir dos pacotes e grupos pré-escolhidos pela equipe da distribuição, ou podem optar pela seleção manual de cada um dos pacotes a serem instalados .

No processo de escolha de pacotes (**figura 1**), a seleção chamada de *Mínimo* informa que o sistema ocupará aproximadamente 1,60 GB após a instalação – um valor alto para uma seleção mínima de pacotes, mas comum para a família Gentoo –, enquanto a instalação padrão mostra o valor de 2,77 GB – também bastante alto. Se forem instalados todos os pacotes do DVD (botão *Todos*), o tamanho da instalação alcança volumosos 5,81 GB.

Desktop

A criação de usuários para o sistema é fácil, mas a exigência de uma senha de root pode ser nova para quem já usa outras distribuições voltadas ao desktop, já que Ubuntu e companhia optam pelo uso do comando `sudo` em detrimento do login com usuário root.

Como distribuição para uso em desktops, o Librix é uma agradável surpresa após a instalação. Sua área de trabalho do KDE já vem embelezada de uma forma que tomaria de

Figura 2 O aplicativo KBFX é bonito e funcional, mas pode assustar quem já se habituou ao menu padrão do KDE.

© Linux New Media do Brasil Editora Ltda.

usuários Gentoo algumas horas de downloads e ajustes.

Diferente da maioria das outras distribuições gratuitas para desktops, o Librix já traz a versão 2.0 do *Skype* instalada por padrão, assim como o gerenciador de downloads *d4x* e o sistema *Superkaramba* pré-configurado com diversos monitores.

O aplicativo de menu *KBFX* (**figura 2**) substitui o menu tradicional do KDE, mas pode desagradar os já habituados ao padrão encontrado nas outras distribuições. Porém, numa distribuição que pretende crescer em adoção, é fundamental ser capaz de se diferenciar da concorrência.

Configuração

O *Librix ConfigCenter* é o centro de controle da distribuição, mas fica um tanto escondido na última posição do menu *Sistema*. Mesmo assim, é bastante agradável contar, num sistema Gentoo, com aplicativos gráficos para realizar todas as configurações que usuários desktop podem desejar, desde alterar o layout do teclado até configurar mais de uma interface de rede na mesma máquina, ajustar data e hora do sistema, habilitar o firewall e configurar redes sem fio.

É no ConfigCenter que se percebe que o Librix também foi pensado para o desktop corporativo: há utilitários para a configuração de um proxy Microsoft ISA e também um outro para login em diretórios *Active Directory* (**figura 3**).

Figura 3 O Librix traz também um assistente de configuração para diretórios Microsoft Active Directory.

Conclusão

Seguindo os princípios do Gentoo e graças à compatibilidade com ele, o Librix dispõe de milhares de pacotes "a um `emerge` de distância", facilmente instaláveis com utilitários gráficos.

Em máquinas Itautec, o Librix já vem instalado e dispensa o longo processo de instalação. Chegando agora a qualquer PC, essa distribuição nacional altamente flexível pode ganhar muito espaço dentro das empresas e dos lares brasileiros. Vale a pena experimentá-la. ■

Complete
a sua coleção

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

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

LINUX MAGAZINE
LINUX NEW MEDIA
The Pulse of Open Source

© Linux New Media do Brasil Editora Ltda.

Snow666

Projeto GNU comemora 25 anos

O projeto GNU comemorou seu 25º aniversário no final de setembro 27. Com seu compilador GCC e a shell *Bash*, o GNU sempre esteve presente nas distribuições Linux. Para começar a comemoração, o humorista britânico Stephen Fry apareceu num vídeo em defesa do Software Livre.

A Free Software Foundation, sempre profundamente envolvida no projeto GNU, produziu um vídeo intitulado "Happy Birthday to GNU" (Feliz Aniversário ao GNU) em homenagem à comemoração. Durante seus cinco minutos, o ator, escritor e diretor Stephen Fry fala com o típico humor seco britânico sobre a história do Projeto GNU e o debate com relação a softwares livres e proprietários. Sua narração acompanha imagens como a de um computador antigo e de Richard Stallman tocando flauta.

Peter Brown, diretor executivo da FSF, sugeriu que o 25º aniversário deveria ser "mais que uma reflexão". O vídeo de Fry e acontecimentos posteriores no evento deveriam ser "um chamado para o trabalho que ainda precisa ser feito" para substituir o software proprietário nos sistemas. ■

Números de versão do kernel

Greg Kroah-Hartman, desenvolvedor Linux da Novell, sugeriu um novo sistema de nomes e números para as versões do kernel. Greg afirma que pretendia dar essa sugestão durante o Kernel Summit 2008, ocorrido no último mês de setembro. Ele sempre esteve envolvido com a numeração de versões e acha o sistema atual difícil demais de gerenciar.

Sua recomendação: versões futuras do kernel Linux deveriam seguir o padrão *quatro_dígitos_do_ano.versão_major.versão_minor*. A *versão_major* indica o estágio mais macro do desenvolvimento, enquanto a *versão_minor* mostra as correções de falhas da versão major a qual pertence.

Seguindo esse padrão, a primeira versão do próximo ano seria a 2009.0.0, a segunda 2009.1.0 e assim por diante. Se não for interessante usar versões de número zero, ele sugere o início em 2009.1.1, por exemplo.

Greg argumenta que esse novo sistema de numeração oferece uma forma melhor para determinar a idade de uma versão. O kernel 2004.9.0 revela sua idade mais claramente do que o 2.6.9, por exemplo. ■

Debian 5.0 muito atrasado

A versão 5.0 do Debian ultrapassou o prazo pretendido para setembro e o projeto estava em silêncio em relação a isso. A última estimativa nos círculos de desenvolvedores é que o "Lenny" não ficará pronto até junho de 2009.

O porta-voz do Debian Alexander Reichle-Schmehl fez um novo pedido de ajuda aos desenvolvedores e usuários em seu blog "para ajudarem a lançar o Lenny pelo menos este trimestre", dando continuidade a seu artigo "What you can do for 'Lenny'" (O que você pode fazer pelo 'Lenny') publicado na LWN.net. Logo depois, o site Heise Online interpretou o artigo como afirmação de que o Debian 5.0 seria lançado até o fim de 2008.

Essa notícia irritou o desenvolvedor Debian Bastian Venthur, que vinha criando gráficos dos bugs críticos do "Lenny" e já havia previsto no início de agosto que o Debian 5.0 não ficaria pronto em setembro e nem em 2008. Sua estimativa, baseada na comparação da taxa de bugs críticos com a da versão anterior do Debian, é de que o "Lenny" só ficará pronto em junho de 2009.

Em seu blog, Venthur foi particularmente crítico da natureza casual com que seus colegas desenvolvedores do Debian anunciaram as datas de lançamento e que esses anúncios deveriam ser mais realistas e precisos. Quanto a isso, ele acrescenta: "Algumas pessoas podem realmente acreditar nas nossas estimativas (sei que isso parece bobo)". ■

© Linux New Media do Brasil Editora Ltda.

Linux Foundation: "OS X é prisão de luxo"

Como diretor da Linux Foundation e um dos desenvolvedores SCSI do Linux, James Bottomley abriu o Linux-Kongress em Hamburgo, Alemanha, com um keynote que investigava as semelhanças e diferenças entre os vários sistemas operacionais de código aberto.

O desenvolvedor britânico não mediu palavras. Num curto panorama histórico, ele descreveu o Linux como o derivado de Unix esperado há muito por instituições de ensino superior e desenvolvedores privados fora dos EUA, pois permite-lhes evitar as longas batalhas legais dos anos 1980 e início dos 1990. Uma série dessas batalhas envolveu disputas sobre quando e como poderiam usar os derivados do BSD como código aberto.

Bottomley atirou em cheio no BSD ao citar a afirmação do diretor de engenharia Jordan Hubbard de que o FreeBSD é o desktop favorito de código aberto. Naturalmente, Hubbard, que está na Apple, quis dizer o Mac OS X. Em vez de desafiá-lo nessa questão, Bottomley preferiu comparar o OS X a uma prisão de luxo e afirmar que os usuários Microsoft estão claramente perdidos entre duas alternativas ruins na comparação. Os usuários Mac, segundo ele, nem conseguem enxergar as barras da cela. Ele frisou que a Apple pode participar do Código Aberto, mas que oferece pouco em retribuição e não divulga vários de seus componentes. ■

Android liberado e aberto

No dia 22 de outubro, a plataforma baseada em Linux para smartphones desenvolvida pelo Google, o Android, foi liberada para download, erradicando as dúvidas em torno da ocultação do código-fonte do sistema após o lançamento do primeiro aparelho a utilizá-lo, o HTC G1.

De acordo com a gigante da Web, o código-fonte consiste em milhões de linhas de código, sendo que apenas quatro horas e meia depois da liberação foram adicionadas seis novas linhas. Em um relatório, David Bort, do projeto Android, afirmou que qualquer pessoa que precise de software para dispositivos móveis ou que trabalhe com bibliotecas de reconhecimento de voz deve ficar à vontade para usar o software. Tudo está disponível: bibliotecas gráficas, codecs de mídia e algumas ferramentas de desenvolvimento muito bem feitas. ■

© Linux New Media do Brasil Editora Ltda.

Novell adquire Managed Objects

A Novell anunciou a aquisição da empresa de serviços de gestão Managed Objects com a intenção de ampliar seu portfólio de soluções para data center, acrescentando ferramentas para fornecer uma visão unificada de toda a informação e rotinas de trabalho desse tipo de ambiente operacional. Segundo a empresa, por causa da integração das soluções oferecidas pela Managed Objects ao portfólio da Novell, tanto os gerentes de negócios quanto os de TI serão capazes de usufruir de uma melhor visibilidade sobre como seus sistemas de informação entregam serviços corporativos, seja por ambientes físicos ou virtuais. Dessa forma, os executivos poderão tomar decisões melhores para assegurar a disponibilidade e a qualidade de serviço, melhorando ao mesmo tempo a agilidade e reduzindo o custo total de gerenciamento do data center.

"A aquisição da Managed Objects mostra o compromisso da Novell com a expansão estratégica de gerenciamento e os torna fortes fornecedores no setor de gerenciamento de serviços", afirmou Tim Grieser, vice-presidente de programas e software de gerenciamento de sistemas corporativos da IDC. "A Managed Objects é uma empresa reconhecida em BSM (*Business Service Management*) e tem experiência comprovada com algumas das maiores empresas no mundo. Com a compra da Managed Objects, a Novell pode ter acesso a discussões de negócios mais facilmente com os CIOs, gerentes de negócios e os principais acionistas do setor de data center. Esse novo foco em gerenciamento de serviço representa um passo na direção certa para a Novell e oferece maior credibilidade aos clientes da Managed Objects", concluiu o executivo. ■

1,5 milhões de PCs com Insigne

Quando o Brasil anunciou seu programa de inclusão digital "Computador para Todos" em novembro de 2005, a meta era oferecer à população computadores com um sistema operacional de código aberto gratuito e um conjunto de programas para acesso à Internet, enviar e receber emails, ouvir e gravar músicas, entre outras tarefas.

"Foi difícil, mas também agradável trabalhar para chegar a 1,5 milhão de famílias", comenta João Pereira da Silva Jr., presidente da Insigne, ao comemorar a marca de 1,5 milhões de computadores equipados com o sistema da empresa. "Os novos usuários de PC consideraram o sistema muito amigável e os usuários de outros sistemas expressaram admiração e o desejo de migrar para o Insigne. Estamos motivados a melhorar o Insigne de modo a aumentar nossa cota de participação no mercado", comentou o executivo.

Segundo Pereira, um dos principais motivos para a conquista desses resultados é o programa de suporte e treinamento oferecido aos fabricantes e varejistas, que compõem o primeiro ponto de contato com os novos usuários que buscam informações sobre como comprar um PC novo.

Pereira afirma que a Insigne vai atingir o objetivo de 2 milhões de unidades até o fim do ano, a partir de PCs de escritório e domésticos, portáteis e notebooks. ■

Trolltech vira Qt Software

Não foi somente a biblioteca multiplataforma *Qtopia* que ganhou um novo nome (*Qt Extended*) com o lançamento da nova versão. A Trolltech, empresa recentemente adquirida pela Nokia, também acabou de ganhar um novo nome: Qt Software.

Os desenvolvedores da empresa norueguesa anunciaram o lançamento da versão 4.4 da Qt Extended, baseada em Linux, que conta com novidades como design modular, recursos melhorados para criação de interfaces gráficas para telas sensíveis ao toque e uso do protocolo *XMPP* por meio da integração do framework *Telepathy*.

© Linux New Media do Brasil Editora Ltda.

Canonical busca comunicação

Para melhorar a comunicação com os desenvolvedores de pacotes e distribuições derivados do Ubuntu, a Canonical criou, como primeira medida, o Upstream Report, um site em tempo real com uma lista dos 1.000 projetos com o maior número de bugs abertos.

O site mostrará quantos desses bugs estão de fato ligados a um desenvolvedor (que a Canonical chama de "upstreamable") e quantos relatórios já foram absorvidos com sucesso pelos sistemas de rastreamento de bugs dos autores originais.

Isso significa que, pela primeira vez, os responsáveis pelos pacotes da Canonical terão números concretos para, por exemplo, permitir que determinem se repassaram 90% dos relatos de erros para cada projeto, ou quais projetos precisam de mais suporte por baixa qualidade. A iniciativa também vai esclarecer como funciona o encaminhamento de relatos de erros para os desenvolvedores – irritantemente chamado também de upstreaming. Há explicações abrangentes sobre como usar as informações disponíveis nos upstream reports no wiki do Ubuntu e no blog do desenvolvedor do recurso.

CANONICAL

Sun

Sun oferece gerenciamento de identidades

A Sun Microsystems começou a oferecer sua própria solução para gerenciamento de identidade, o *OpenSSO*. O software está disponível gratuitamente e com código aberto, e agora se torna um produto da Sun com suporte e serviços.

A sigla SSO significa *single sign-on* (entrada única), ou acesso a múltiplos serviços usando uma única senha. A Sun combinou seu *Java System Access Manager* ao *Java System Federation Manager* no OpenSSO. A próxima versão do software unificado deve ser lançada como *Federated Access Manager* 8.0. O produto oferece o gerenciamento de identidades e dá aos usuários uma identidade única para acesso em múltiplas aplicações e redes.

DPZ

No mercado de TI todo dia aparece uma novidade. A próxima pode ser no seu currículo.

Exames de certificações e cursos preparatórios Senac. Para quem quer ser aprovado pelo mercado.

Consulte a lista de cursos no site www.sp.senac.br/certificacoes ou ligue 0800 883 2000.

senac são paulo

CISCO Networking Academy | CENTRO TREINAMENTO AUTORIZADO FURUKAWA | Microsoft GOLD CERTIFIED Partner Learning Solutions | WORKFORCE DEVELOPMENT PROGRAM | APPROVED EDUCATION CENTER | PMI Registered Education Provider Project Management Institute | PROMETRIC Testing Center | PEARSON VUE AUTHORIZED TEST CENTER

© Linux New Media do Brasil Editora Ltda.

Snow666

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

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

© Linux New Media do Brasil Editora Ltda.

Snow666

Flexibilidade e Confiabilidade

Solução de gestão integrada ADempiere:

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

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

Kenos
Sistemas de Gestão Integrada

© Linux New Media do Brasil Editora Ltda.

Como será a indústria de software em 2020?

Cezar Taurion

Dois modelos já estão transformando a indústria do software: o Open Source e o Software-as-a-Service (SaaS), que em 2020 serão dominantes.

por Cezar Taurion

O Open Source afeta diretamente a cadeia de valor da indústria, pois atua nas importantes variáveis que entram na composição dos seus preços, como os custos de desenvolvimento (diluídos pelo trabalho colaborativo) e o marketing/comercialização (via Internet). Oferecendo alternativas "boas o suficiente", custos de propriedade mais competitivos (em alguns casos os custos de aquisição tendem a zero) e modelos de negócio mais flexíveis, o resultado gerado pelo Open Source é uma pressão maior nas margens, obrigando muitos produtos a terem seus preços sensivelmente reduzidos.

Saas é outro modelo. Sua proposta de valor é a funcionalidade oferecida e não a propriedade do produto. Você não necessita instalar um pacote de CRM ou ERP, mas precisa das suas funcionalidades. O cliente não adquire licença de uso, mas paga uma taxa mensal baseada no número de funcionários que acessam o serviço.

O mercado vem dando sinais de grande receptividade ao modelo. Algumas estimativas apontam que SaaS pode chegar a 25% ou 30% do mercado total de software já nos próximos três a quatro anos. Outra aponta que já em 2010 pelo menos 65% das empresas americanas terão pelo menos uma aplicação rodando no modelo SaaS. Como é um horizonte de aproximadamente dez anos, imaginamos que um percentual bem significativo do mercado de software será baseado em SaaS e Open Source por volta de 2020.

O resultado é que a indústria de software precisará ser reinventada. Por que comprar uma licença de uso de um software caro se existir uma solução "boa o suficiente" mais barata e que não precisa ser instalada em suas máquinas? Atrás dessas mudanças estão novos modelos de negócio que provavelmente não terão margens de lucro tão altas quanto hoje. A dificuldade maior vai aparecer para as empresas já estabelecidas, que precisam mudar seu modelo de negócios e provavelmente sua estrutura organizacional, de vendas e de custos. E também precisarão recriar o ecossistema de parceiros, ou seja, existem barreiras culturais e organizacionais a serem vencidas!

A lucratividade do SaaS depende de três variáveis básicas: custo para atrair um novo cliente, rendimento desses clientes com assinaturas (ou receita média por usuário, ou ARPU – *Average Revenue Per User*) e com que freqüência os assinantes deixam o serviço e precisam ser substituídos (taxa de rotatividade ou *churn rate*).

A transição para o modelo SaaS não é simples. Os custos de vendas e marketing ainda são muito altos. A empresa SaaS mais bem sucedida até o momento, a Salesforce.com, gasta metade de suas receitas em vendas e marketing. Além disso, no modelo tradicional a troca de um software é mais complexa e o aprisionamento do usuário é quase uma regra da indústria. Quantos usuários de ERP trocam de fornecedor? No SaaS, a barreira de saída é muito mais baixa.

A conseqüência é uma competição mais acirrada e preços menores. Resultado: margens e lucros menores. Definitivamente, em 2020, a indústria de software deverá ter uma "cara" bem diferente da atual e as empresas lucrativas de hoje provavelmente estarão ganhando dinheiro com outros modelos de negócio (mais focados em serviços de consultoria e integração) ou estarão fora do jogo. ■

Sobre o autor

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

© Linux New Media do Brasil Editora Ltda.

Em busca do próximo Einstein

Jon 'maddog' Hall

A abertura do Software Livre incentiva a inovação através de gerações e fusos horários.

por Jon 'maddog' Hall

É provavel que eu sempre tenha percebido as habilidades de alguns programadores de Software Livre, então eu não deveria continuar surpreso com o que eles conseguem fazer. Porém, preciso admitir que eles continuam me impressionando.

Conheço um rapaz, Nick, que começou a programar aos nove anos de idade e aos 15 escreveu drivers de dispositivo para Linux. Ele ajudou o FBI a capturar alguns crackers criando um honeypot aos 21 e depois foi fazer pesquisa – sem jamais ter sequer completado o ensino médio.

Outro começou sua própria distribuição Linux aos 14 e espalhou 20.000 cópias de seu sistema antes mesmo que seus pais descobrissem o que ele estava fazendo.

Fonte

Esses hackers e muitos outros creditam o acesso visual ao código como um fator importante para o avanço de suas habilidades. Com o Software Livre, poucas pessoas perguntam sua idade, sexo, religião ou qualquer coisa além de "cadê o código?". Novos programadores conseguem trabalhar tanto e tão rápido quanto quiserem lendo o código de outros e aprendendo com ele.

No meio dos anos 70, um professor universitário acreditava que a melhor forma de ensinar programadores a escreverem bom código era mostrando-lhes o código de programadores muito bons. John Lions conseguiu comentar e anotar a listagem completa do *Sixt Edition of Unix* antes de a AT&T alterar a licença no *Sevent Edition of Unix*, que proibiu o uso do código-fonte com fim educacional. Felizmente, para a Ciência da Computação, algumas cópias "escaparam" e esse conjunto de dois volumes se tornou um dos livros de Ciência da Computação mais fotocopiado de todos os tempos.

Programadores Unix mediam seu tempo no campo da computação pela posse ou não de uma fotocópia de quinta geração do livro de Lion ou uma fotocópia de décima geração.

Olhar o código de um bom programador ainda é uma ótima forma de aprender a profissão. Eu realmente não entendo como um instrutor de Ciência da Computação pode propor o uso de softwares proprietários de código fechado para ensinar aos alunos, quando há softwares livres comparáveis. No software proprietário, você vê o que o programa faz, mas não como ele faz.

E o Software Livre não apenas mostra o código – é possível conhecer o programador. Como alguém que já trabalhou tanto com software proprietário quanto aberto, eu aprecio o fato de que, se eu quiser conhecer a pessoa que escreveu um programa específico e entender como essa pessoa se encaixa num ambiente de desenvolvimento, normalmente eu posso simplesmente olhar a lista de emails do projeto. Essa estratégia me permite localizar vários dos ótimos programadores que estão surgindo.

Recentemente, eu soube de um estudante universitário que está participando do que eu considero trabalho de graduado. Ele é articulado, parece ter vários interesses e mora na Romênia. A abertura do Software Livre me permitiu encontrá-lo, e espero trabalhar com ele no futuro como tenho feito com os prodigiosos programadores que mencionei antes.

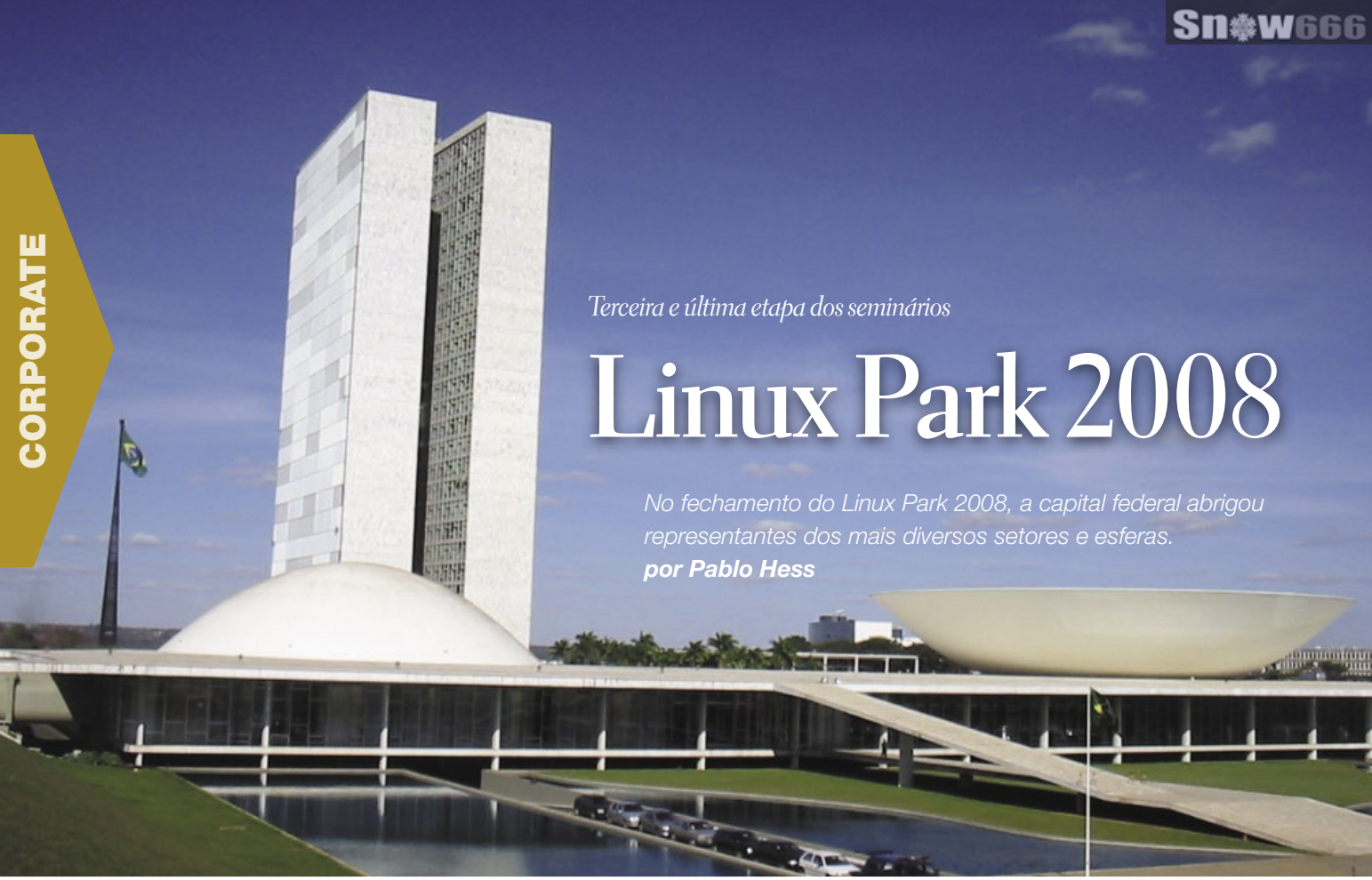
Eu continuo procurando o próximo "Albert Einstein da Ciência da Computação", e não sou egoísta a ponto de achar que esse gênio precisaria vir dos EUA, ou sequer ter sido educado aqui. Com problemas demais e gente de menos para resolvê-los, o próximo "Albert" ou "Alberta" pode vir do Brasil, da China, da Romênia ou até mesmo de Helsinki, Finlândia.

O que eu sei é que a abertura do Software Livre nos ajudará a encontrar a próxima geração de experts. ■

Sobre o autor

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

© Linux New Media do Brasil Editora Ltda.



Terceira e última etapa dos seminários

Linux Park 2008

No fechamento do Linux Park 2008, a capital federal abrigou representantes dos mais diversos setores e esferas.

por Pablo Hess

Numa época em que todos precisam se preocupar com o meio ambiente, a cidade de Brasília, DF, abrigou mais um evento sobre o ecossistema. No entanto, esse evento visava a abordar questões de um outro ecossistema: o dos negócios com Software Livre e de Código Aberto (SL/CA) no Brasil.

Figura 1 Rafael Peregrino abriu o evento com um keynote sobre o ecossistema brasileiro de negócios em SL/CA.

No dia 23 de setembro, a capital federal novamente foi palco do Linux Park, o principal evento sobre SL/CA em ambiente corporativo no Brasil. Realizado pela Linux New Media do Brasil e promovido pela Linux Magazine, o terceiro evento da série de seminários Linux Park 2008 (após edições em Porto Alegre, RS e Rio de Janeiro, RJ) teve como mote "O ecossistema de negócios em Software Livre no Brasil". Reunidos no Hotel Naoum Plaza, executivos dos setores privado e público, nas mais variadas esferas e de diferentes áreas de atuação, trocaram informações, sugestões e contatos sobre como usam SL/CA e de que forma podem tornar esse uso mais produtivo para seus negócios.

Abertura

Abrindo a terceira série de seminários Linux Park 2008, o diretor da Linux New Media do Brasil, Rafael Peregrino (**figura 1**), dissertou em seu *keynote* sobre o estado atual do ecossistema brasileiro de negócios em SL/CA. Ele apresentou resultados dos estudos mais recentes sobre o valor do SL/CA, que demonstraram que a redução de custos de licenciamento é o quarto colocado entre os principais motivos para a adoção do SL/CA nas empresas em todo o planeta, atrás da confiabilidade, da segurança e do desempenho desses sistemas livres.

Rafael ressaltou os diferentes componentes do ecossistema de SL/CA, como hardware, software, serviços e mídia, destacando os fornecedores em cada uma dessas esferas.

Caixa Econômica Federal

A primeira palestra do evento foi de Clarice Coppetti (**figura 2**), vice-presidente de TI da Caixa Econômica Federal. Na apresentação intitulada "Superando desafios com Software

© Linux New Media do Brasil Editora Ltda.

Livre", Clarice narrou a experiência da CEF na ampla adoção de Linux e SL/CA, num dos maiores casos de sucesso dessa tecnologia no mundo.

A executiva afirmou que a estratégia de adoção de SL/CA na instituição "não tem volta", pois "já estava arraigada nos profissionais antes de se tornar institucionalizada". Embora tenha reconhecido uma certa resistência por parte da equipe anterior de gestão do banco, Clarice disse que o SL/CA já era objeto de estudo em virtude das vantagens demonstradas.

Os slides mostrados por Clarice revelaram que a infra-estrutura de TI do banco – baseada em SL/CA

Figura 2 Clarice Coppetti narrou a experiência da Caixa Econômica Federal em um dos maiores cases de SL/CA do mundo.

– processa um dos maiores volumes de transações no segmento no país: 2,4 bilhões de transções financeiras por ano, além de 2,2 bilhões em jogos das diversas loterias, 500 milhões de acessos ao website, 129,3 milhões de transações via Internet banking e 86 milhões de atendimentos de telemarketing de produtos, atendimentos e URA.

Paulo Maia da Costa (**figura 3**), gerente de projetos de TI da Caixa, também foi chamado por Clarice para falar sobre a adoção do ODF e esclarecer questões técnicias.

Com sua experiência, a Caixa está se tornado fornecedora de sua própria tecnologia, além de fornecer também para outras instituições. A instituição criou uma distribuição Linux personalizada e patrocina eventos comunitários, como o FISL e o Latinoware, como mais uma forma de promover o desenvolvimento da tecnologia aberta.

Pesquisa com CIOs

Após o coffee-break, Álvaro Leal (**figura 4**), analista de mercado e consultor do ITData, apresentou a pesquisa realizada pela consultoria ITData em parceria com o Instituto Sem Fronteiras sobre o mercado brasileiro do SL/CA. Os resultados mais marcantes do estudo são a maior presença dessa tecnologia nas maiores empresas em relação às pequenas empresas. Esse resultado contraria o que se acreditava até então, que as menores empresas seriam mais sensíveis ao custo do software e, portanto, utilizariam SL/CA com mais intensidade.

Segundo Álvaro, uma forma de interpretar essa discrepância entre os dois tipos de empresas seria o fato de que as grandes empresas têm setores de TI específicos, com políticas mais estritas de qualidade, desempenho e segurança da infra-estrutura, o que propicia o uso de SL/CA, enquanto as pequenas, apesar de sensíveis ao custo dos softwares, são mais permeáveis às cópias ilegais de software.

Álvaro esclareceu que o estudo contou com a participação de mais de mil CIOs de empresas de todos os tamanhos e de diversas verticais, compreendendo, portanto, uma amostragem bastante confiável do panorama das empresas brasileiras. O resultado geral do estudo – 59% das empresas do país utilizam SL/CA – também marcou o público.

Figura 4 A pesquisa realizada pelo Instituto Sem Fronteiras e pela ITData foi apresentada por Álvaro Leal e revelou dados surpreendentes sobre o mercado brasileiro do SL/CA.

Na separação por regiões, o Centro-Oeste brasileiro se destacou pela maior porcentagem de uso do SL/CA em servidores: 78%. A grande difusão da tecnologia aberta cabe, segundo Álvaro, à forte adoção por parte do Governo Federal.

A presença do SL/CA nos desktops das empresas foi mais um aspecto surpreendente da pesquisa, pois era

Figura 3 Paulo Maia da Costa participou da palestra de Clarice Coppeti e esclareceu aspectos relacionados ao padrão ODF.

© Linux New Media do Brasil Editora Ltda.

Snow666

difundida a crença de que "Software Livre só é bom para servidores", segundo o analista.

Após analisar minuciosamente os detalhes mais relevantes do estudo, Álvaro concluiu sua apresentação ressaltando a ordem de importância dos fatores declarados pelos CIOs para o uso do SL/CA, na qual o custo não era o principal, novamente contrariando a crença mais difundida.

Chaves públicas

Depois do almoço, Ruy Cesar Ramos Filho (**figura 5**), assessor da diretoria de infra-estrutura de chaves públicas do Instituto Nacional de Tecnologia da Informação (ITI), palestrou sobre o programa João de Barro. O programa consiste em um sistema de gerenciamento de certificados digitais, assunto de grande importância na política federal.

Figura 5 Ruy Cesar Ramos Filho descreveu a ICP Brasil e suas atribuições no contexto da certificação digital.

Segundo esse programa, o ITI seria responsável por gerenciar toda a infra-estrutura de chaves públicas brasileiras, o que inclui a fiscalização das autoridades certificadoras, com o objetivo de garantir as características fundamentais desses dispositivos, como autenticidade, integridade, confidencialidade e validade jurídica.

Ruy finalizou sua apresentação descrevendo a estrutura institucional envolvida com o programa João de Barro, que inclui universidades, órgãos federais e bancos.

SL/CA na educação

O uso do SL/CA na educação foi o tema do seminário de Regiane Soares de Carvalho (**figura 6**), especialista em Linux e softwares educacionais do Ministério da Educação. Regiane descreveu seu trabalho no MEC como a prospecção de tecnologias que auxiliam no processo educacional, a serem aplicados no programa Proinfo de uso da tecnologia para esse fim.

Figura 6 Regiane Soares de Carvalho apresentou a distribuição Linux Educacional e abordou a utilização do SL/CA nas escolas públicas servidas pelo programa Proinfo.

O programa Proinfo começou em 2002 com pouco mais de 4 mil laboratórios de informática em escolas públicas, e hoje já ultrapassou os 54 mil, ajudando os alunos da rede pública a se familiarizarem com a tecnologia da informação por meio do SL/CA.

Regiane apresentou também a distribuição Linux desenvolvida pelo MEC, o Linux Educacional, com um ambiente completamente voltado às necessidades dos alunos da rede pública de ensino com acesso ao programa Proinfo.

Software Público

Corinto Meffe (**figura 7**), gerente de inovações tecnológicas da Secretaria de Logística e TI (SLTI) do Ministério do Planejamento, abordou em seu seminário o tema da economia dos bens intangíveis. Trata-se de um conceito, segundo Corinto, diferente da economia a qual estamos acostumados, pois carrega importantes diferenças quanto a fatores como escassez e restrição, geralmente marcantes na economia tradicional dos bens tangíveis.

Corinto afirmou que o mercado de software, por exemplo, é artificialmente incluído na economia

Figura 7 Corinto Meffe discursou sobre a economia de bens intangíveis e afirmou que é preciso todos reverem seus conceitos sobre o assunto.

© Linux New Media do Brasil Editora Ltda.

de bens tangíveis, justamente pelas licenças de software. Um programa seria intangível, mas a existência da licença que concede o direito de uso do software a uma pessoa ou uma máquina cria uma "indivisibilidade artificial", nas palavras de Corinto.

O gerente de inovações tecnológicas demonstrou que a proposta de Richard Stallman, criador da licença GPL, do projeto GNU e do Software Livre, é equivalente à remoção do pedágio de uma estrada. Segundo ele, a economia dos bens intangíveis contraria algumas das teorias econômicas mais fundamentais, como o Princípio da Escassez de Adam Smith, a Teoria do Valor de Karl Marx e a Organização Burocrática de Max Weber.

Como exemplo de empresa que já está abordando a economia dos bens intangíveis, Corinto citou a IBM, cuja receita proveniente do SL/CA já ultrapassa aquela advinda de suas patentes, apesar de a empresa ser a maior detentora mundial de patentes.

O seminário abordou ainda o fenômeno da Web 2.0 e sua característica participativa, chegando ao conceito de mercado público virtual, relacionado ao próprio Portal do Software Público mantido pela SLTI.

Em sua conclusão, Corinto Meffe afirmou que a economia do SL/CA requer uma revisão de conceitos por parte de todos os envolvidos, pois suas bases são bastante diferentes daquelas da economia tradicional e nem sequer estão formalizadas pelos teóricos.

Figura 9 Sob o olhar de Rafael Peregrino, Rodrigo Assumpção e Ricardo Masstalerz assinaram o acordo que incluiu a solução WebIntegrator no Portal do Software Público.

Figura 8 Como de costume, o Linux Park foi freqüentado por profissionais do mais alto nível e de diversas áreas.

WebIntegrator

Após a palestra de Corinto Meffe, a SLTI assinou, em parceria com a empresa ITX Tecnologia da Informação e sob os olhos do público qualificadíssimo (**figura 8**), o acordo para disponibilizar a solução WebIntegrator sob o Portal do Software Público. O acordo foi assinado por Rodrigo Assumpção, secretário-adjunto de logística e TI, e Ricardo Masstalerz, sócio-diretor da ITX (**figura 9**), assistidos por Rafael Peregrino, diretor da Linux New Media.

A solução WebIntegrator consiste em um ambiente para produção facilitada de aplicações web em plataforma Java e já está disponível no Portal do Software Público.

SL/CA na SLTI

A terceira e última etapa dos seminários Linux Park 2008 foi finalizada com a apresentação de Rodrigo Assumpção a respeito do SL/CA na SLTI. Ele discursou sobre o WebIntegrator e o valor de sua inclusão no Portal de Software Público, mencionando ainda a importância do próprio Portal na nova economia apresentada por Corinto Meffe. ■

© Linux New Media do Brasil Editora Ltda.

AMQP

Ricardo Bimbo

Código aberto e padrões abertos ajudam o JPMorgan a alcançar maior interoperabilidade e desempenho.

por Ricardo Bimbo

Pouca gente já ouviu falar sobre o AMQP [1], sigla de *Advanced Message Queuing Protocol*. Em tradução literal, Protocolo Avançado de Filas de Mensagem. Trata-se de um projeto de padrão aberto para mensagens de *middleware* e vem ocupar um espaço restrito a alguns protocolos (MQ's) fechados. O projeto atende não apenas à demanda de grandes usuários de tecnologia, gente que tem ou precisa de muito processamento e grande integração com *web services* e servidores de aplicação, mas também para muitas especificações voltadas à implementação da SOA e, não menos importante, oferece ferramentas para uma série de necessidades.

O AMQP está disponível para as linguagens *C*, *C++*, *Java*, *JMS*, *.NET*, *C#*, *Ruby*, *Python* e é interoperável, por ser multilinguagem, multifabricante, multiplataforma. O AMQP é um protocolo *wire-level* integrado ao IP que permite o transporte das mensagens de forma integrada e onipresente, possibilitando que uma mensagem (transmitindo, armazenando, compilando, direcionando, autorizando) esteja em mais de um lugar ao mesmo tempo.

Já existem quatro produtos no mercado baseados nesse protocolo: *OpenAMQ*[2], *Qpid*[3], *RabbitMQ*[4] e o *Red Hat Enterprise MRG*[5], todos com vasta documentação de casos de uso e de sucesso.

O projeto foi fundado em 2006 e, com pouco mais de dois anos, o sucesso de sua especificação se comprova por meio do alto nível de detalhamento técnico e na inovação, que permitiu que em tão pouco tempo quatro produtos fossem desenvolvidos e estabelecidos de maneira madura, consistente, documentada e suportada.

Quem acompanha o debate em torno de padrões, e, principalmente, dos projetos de especificações de alguns padrões abertos, está acostumado a se deparar com a participação, o envolvimento e, por que não, o investimento de universidades e grandes fabricantes de TI no grupo de trabalho e na coordenação de projetos. O AMQP não é diferente: o projeto conta com a participação da Red Hat, da Cisco e da Imatix. Quase passaria despercebida a participação do JPMorgan Chase Bank & Corp. O que um banco faz no grupo de trabalho? Bem, esse banco não só faz parte do grupo de trabalho como também é o fundador e coordenador do projeto.

O AMQP surgiu da necessidade do próprio banco por um protocolo aberto e livre para mensagens. Diante do desafio de integrar em tempo real aplicações de auto-atendimento (ATM's) com uma aplicação de segurança, o JPMorgan esbarrou nos protocolos e nas especificações fechadas de mensageria, que impediam o tratamento e o tuning das aplicações, obrigando as mensagens a seguirem um modelo de fila convencional, isso é, primeiro passar por uma aplicação para ser autorizada por outra e assim sucessivamente.

O JPMorgan entendeu a lição como poucos: em vez de apenas "se aproveitar" de forma parasitária de softwares abertos, exerceu e estimulou o papel de fomentador tecnológico que um grande cliente tem. Não preciso explicar aqui o valor que a TI tem para as instituições financeiras, mas o JPMorgan poderá criar um outro padrão além do AMQP, o padrão de usuários que vão liderar projetos de código aberto e padrões abertos. ■

Mais informações

[1] AMQP www.amqp.org

[2] OpenAMQ: http://www.openamq.org/

[3] Qpid: http://cwiki.apache.org/confluence/display/qpid/Index

[4] RabbitMQ: http://www.rabbitmq.com/

[5] Red Hat Enterprise MRG: http://www.redhat.com/mrg/

© Linux New Media do Brasil Editora Ltda.

Snow666

Técnicas para autenticação no Linux

Acesso inteligente

Talvez a segurança por senhas não seja perfeita, mas a maioria das redes depende dela. Conheça algumas formas mais inteligentes e versáteis de autenticação.

por Joe Casad e Pablo Hess

Apesar dos vários anos de constante inovação tecnológica, a senha continua sendo um recurso fundamental na maioria dos sistemas. Várias ferramentas permitem que se consolide, criptografe, saneie e sincronize as senhas, mas a menos que sua empresa invista pesadamente em smart cards ou outras tecnologias recentes, certamente você precisará fazer login em algum local. Este mês veremos algumas técnicas para simplificar e tornar mais segura a autenticação no Linux.

Nosso primeiro artigo examina algumas ferramentas para autenticar usuários com senhas digitadas uma única vez (*one-time passwords*, como são chamadas mais freqüentemente). Mostraremos por que várias organizações preferem senhas que mudem a cada login. Depois, abordaremos as ferramentas OPIE e OTPW – duas soluções de código aberto para a autenticação com one-time passwords.

Muitos usuários Linux prefeririam nem pensar na Microsoft, mas parte de nossa missão sempre foi trazer aos nossos leitores informações sobre ferramentas livres e de código aberto para integração fácil com tecnologias proprietárias. Nosso próximo artigo descreve como o serviço *Winbind* do *Samba* permite que clientes Linux participem de ambientes Microsoft *Active Directory*.

O último artigo introduz as técnicas de autenticação por biometria disponíveis em código aberto e apresenta também as principais questões envolvidas nessa área. Leia mais para algumas ótimas técnicas de autenticação e gerenciamento de identidades no Linux. ■

Índice das matérias de capa

© Linux New Media do Brasil Editora Ltda.

Snow666

Autenticação segura com one-time passwords

Chaves nunca repetidas

Uma senha do tipo one-time não compromete a segurança caso caia em mãos erradas. O OPIE e o OTPW trazem a segurança dessa técnica para o Linux.

por Udo Seidel

Apesar da explosão no uso da biometria, as senhas ainda são a forma mais popular de autenticação. Em ambientes hostis, usuários maliciosos capturam ou registram a digitação de senhas. É possível combater essas tentativas usando uma técnica conhecida como *one-time password* ("senha para uma única vez"). Uma one-time password fica obsoleta imediatamente após seu uso. Mesmo que o agressor consiga capturar a senha no meio do caminho para o servidor de autenticação, essa senha seria inútil. Para uma one-time password funcionar, o cliente precisa de alguma forma de determinar qual senha usar, e o servidor deve saber qual senha esperar.

Figura 1 Exemplo de token que utiliza a técnica desafio-resposta. O usuário digita o desafio pelo teclado do token e lê a resposta na tela.

Técnicas

Especialistas em segurança já desenvolveram várias técnicas para geração de one-time passwords. Alguns métodos criam novas senhas com base na manipulação matemática da hora atual. Outra técnica conhecida como desafio-resposta começa com o servidor enviando um número aleatório para o cliente. O cliente então calcula uma resposta com uso de um processo conhecido por ambos os computadores.

Obviamente, se um agressor capturar alguns desses desafios e respostas, ele conseguiria, em teoria, descobrir o método usado. Essa técnica de cripto-análise, freqüentemente chamada de *known plaintext* (texto puro conhecido), foi descrita em várias publicações científicas. Porém, se ambos os parceiros aplicarem uma função de *hash* após calcularem a resposta, um "farejador" teria muito mais dificuldade para desvendar o valor original. O resultado é muito semelhante a um número aleatório.

Esses tipos de cálculo são difíceis de realizar de cabeça, então os usuários costumam empregar um dispositivo eletrônico chamado *token*, semelhante a um chaveiro ou a uma calculadora de bolso. As **figuras 1 e 2** mostram exemplos de alguns tokens Outra opção é instalar num telefone celular ou PDA o software necessário para atuar como token baseado em hardware.

Soluções em software

Os tokens são relativamente caros; além disso, a tecnologia costuma ser patenteada, ou então os mecanismos

Figura 2 Exemplo de token que codifica a hora atual e a chave interna. A tela exibe um número (PIN) diferente a cada minuto.

© Linux New Media do Brasil Editora Ltda.

Exemplo 1: Inicialização do OPIE

```
01 # opiepasswd
02 Adding root:
03 You need the response from an OTP generator.
04 New secret pass phrase:
05    otp-md5 499 te3049
06    Response:
07 ^C
08 # opiepasswd -c
09 Adding root:
10 Only use this method from the console; NEVER from remote. If you
➥are using telnet, xterm, or a dial-in, type ^C now or exit with no
➥password. Then run opiepasswd without the -c parameter.
11 Sorry, but you don't seem to be onthe console or a secure
➥terminal.
12 # opiepasswd -cf
13 Adding root:
14 Only use this method from theconsole; NEVER from remote. If you
➥are using telnet, xterm, or a dial-in, type ^C now or exit with no
➥password. Then run opiepasswd without the -c parameter.
15 Using MD5 to compute responses.
16 Enter new secret pass phrase:
17 Again new secret pass phrase:
18
19 ID root OTP key is 499 te5843
20 DANG TOOK HUNT GYM HICK PAW
21 # cat /etc/opiekeys
22 root 0499 te5843  6f1dba738c197a64  October 16,2008 05:42
```

internos não são completamente revelados por medida de segurança. Se for preferível evitar o esforço e os custos de um token baseado em hardware, também é possível usar uma solução com base somente em software.

Sistemas de one-time passwords baseados em software existem há vários anos e estão presentes até em vários RFCs na Internet. O sistema S/Key, desenvolvido em 1995 pela Bellcore, é definido no RFC 1760. Originalmente, ele empregava criptografia MD4. Seu sucessor, o OTP, é especificado no RFC 2289 e também pode usar hashes MD5 e SHA.

OPIE universal

Dois projetos de código aberto conhecidos como *OPIE*[1] e *OTPW*[2] oferecem ferramentas para one-time passwords no Linux. A implementação do OTP em software mais popular no Linux é uma cortesia do projeto OPIE (*One-Time Passwords in Everything*).

É fácil instalar o OPIE a partir dos pacotes disponíveis para várias distribuições, assim como sua compilação a partir dos fontes. A instalação cria programas compatíveis com OTP para substituir os tradicionais `login`, `su` e `ftpd`, e também fornece a biblioteca `pam_opie.so`, além de várias ferramentas e do arquivo de configuração `/etc/opiekeys`.

A primeira etapa é inicializar o sistema OTP (**exemplo 1**). Os usuários precisam fazer isso eles próprios, fazendo login no sistema e executando o comando `opiepasswd` (**linha 1**). Os resultados podem causar confusão a princípio (**linha 3**); por padrão, a ferramenta presume que o usuário não esteja logado nem localmente conectado ao console.

Como o tráfego de rede costuma ser sujeito ao "farejamento" e portanto inseguro, o `opiepasswd` espera uma OTP. Para evitar um problema do tipo "ovo e galinha", os usuários precisam declarar (com a opção `-c`) que estão usando um console seguro (**exemplo 1, linha 8**).

Se o comando descobrir que o usuário está mentindo, ele se recusará a cooperar. Usuários que levam segurança a sério devem evitar a opção `-f` (**linha 12**), que ignora o pedido subseqüente.

O processo é específico para cada usuário; em outras palavras, cada usuário que desejar usar one-time passwords precisará executar o comando individualmente.

Após completar a inicialização, é acrescentada ao arquivo `/etc/opiekeys` uma entrada referente ao usuário. Esse arquivo também con-

Exemplo 2: pam_opie.so

```
01 ...
02 auth sufficient pam_opie.so
03 # Pode excluir esta linha se você
➥ já tiver testado o OPIE:
04 auth sufficient pam_unix.so
➥ nullok try_first_pass
05 ...
```

Exemplo 3: Login por SSH com OPIE

```
01 $ ssh root@servidor.com.br
02 otp-md5 498 te5843 ext
03 Response:
04 # cat /etc/opiekeys
05 root 0498 te5843 2b84befd37cacb9f
➥ Feb 16,2008 05:58
06 #
```


© Linux New Media do Brasil Editora Ltda.

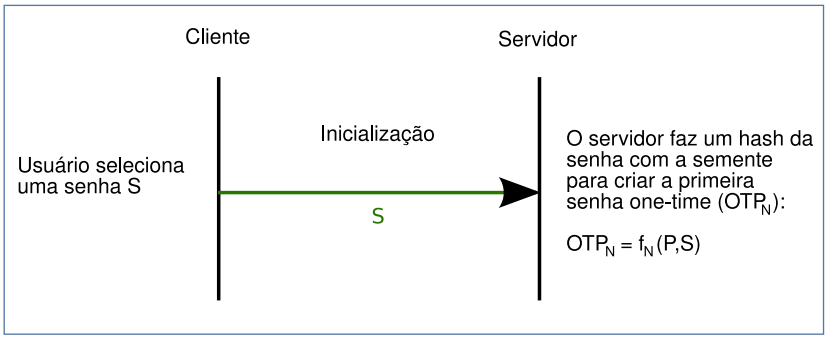


Figura 3 Para inicializar, o gerador envia uma senha ao servidor. O servidor faz um hash da senha com uma semente e calcula a primeira senha *one-time*.

Exemplo 4: Criação de três OTPs com o opiekey

```
01 # opieinfo
02 497 te5843
03 # opiekey -5 -n 3 `opieinfo`
04 Using the MD5 algorithm to compute response.
05 Reminder: Don't use opiekey from telnet or dial-in
06 sessions. Sorry, but you don't seem to be on the
07 console or a secure terminal.
08 Warning: Continuing could disclose your secret pass
09 phrase to an attacker!
10 Enter secret pass phrase:
11 495: MUSH ACT GRIM SEE MAID LIES
12 496: HAD FED WORD ROY STAB ACID
13 497: IO INK RIG DAME RULE TUM
14 #
```

tém a semente (`te5843`, nesse caso), o hash (`6f1dba738c197a64`), uma nova senha do tipo one-time e o número de seqüência (`499`, nesse exemplo – **linhas 31 e 32**).

Para gerar one-time passwords válidas depois, os usuários precisam de suas senhas pessoais, da semente e do número de seqüência. Felizmente, a única dessas que é necessário memorizar é a senha do usuário; as outras duas credenciais são fornecidas e exibidas pelo servidor.

Rede de segurança

A próxima etapa é integrar o mecanismo de autenticação à pilha do PAM (**exemplo 2**). Os módulos *pam_unix* ou *pam_unix2* fazem a maior parte desse trabalho. Esses módulos têm uma marca de controle que diz `sufficient` (suficiente), mas, como precisamos substituí-los pela biblioteca `pam_opie.so`, é necessário alterar a configuração de forma correspondente.

Note que também é possível configurar o sistema para que, caso o OPIE falhe por algum motivo, os usuários ainda consigam usar suas senhas legadas para a autenticação.

Após modificar a configuração do PAM, o sistema já estará pronto para o OTP. Alguns serviços como o *daemon* SSH ainda precisam de certa atenção manual antes de começarem a usar one-time passwords. No caso do SSH, somente a seguinte linha é necessária no arquivo de configuração `/etc/sshd/sshd_config` do servidor:

```
ChallengeResponseAuthentication
➥yes
```

O **exemplo 3** mostra um login por SSH usando o OPIE. Após fazer a autenticação com sucesso, o OPIE atualiza o arquivo `/etc/opiekeys`, acrescentando o novo número de seqüência e o hash da última senha usada.

Semear e colher

Os usuários precisam da `opiekey` para gerar suas senhas one-time. O gerador do **exemplo 4** espera a senha do usuário, a semente e um número de seqüência. Os usuários podem executar `opieinfo` para visualizar essas informações. O OPIE também tem um mecanismo para gerar uma lista de OTPs caso o usuário não possua um gerador.

Há outros geradores além do `opiekey`. O programa em *Java OTP*[3] pode ser executado em qualquer telefone celular com Java ou num site normal, embora o site precise ser absolutamente confiável. Usuários de Palm podem usar o *Palmkey*[4] ou o *Pilotp*[5], e usuários desktop têm o *Otpcalc*[6] à disposição.

O comando `opiepasswd -d` desativa uma entrada de usuário no arquivo `/etc/opiekeys` e, portanto, elimina o usuário do sistema OPIE (veja o

Exemplo 5: Destativar o OPIE para um usuário

```
01 user1@servidor$ opiepasswd -d
02 Updating user1:
03 Disable user1's OTP access?
➥ (yes or no) yes
04 ID user1 is disabled.
05 user1@servidor$ su -
06 Password:
07 # grep user1 /etc/opiekeys
08 user1 0359 te2880
➥ ********** Feb 16,2008
➥ 08:37
09 #
```


© Linux New Media do Brasil Editora Ltda.

Exemplo 6: Configuração do OTPW

```
01 # otpw-gen -h 5
02 Generating random seed ...
03
04 If your paper password list is stolen, the thief should not gain
05 access to your account with this information alone.
➥ Therefore, you
06 need to memorize and enter below a prefix password.
➥ You will have to
07 enter that each time directly before entering the
➥ one-time password
08 (on the same line).
09
10 When you log in, a 3-digit password number will be displayed. It
11 identifies the one-time password on your list that you
➥ have to append
12 to the prefix password. If another login to your account
➥ is in progress
13 at the same time, several password numbers may be shown and all
14 corresponding passwords have to be appended after the prefix
15 password. Best generate a new password list when you have
➥ used up half
16 of the old one.
17
18 Enter new prefix password:
19 Reenter prefix password:
20
21 Creating '~/.otpw'.
22 Generating new one-time passwords ...
23
24 OTPW list generated 2008-03-16 10:23 on testvm3.seidelnet.de
25
26 000 a7Sj rWoC 001 %URK VvmD 002 EoQa sgon 003 IQhJ kVMG
➥ 004 QsS% H=aU
27
28 !!! REMEMBER: Enter the PREFIX PASSWORD first !!!
28 #
```

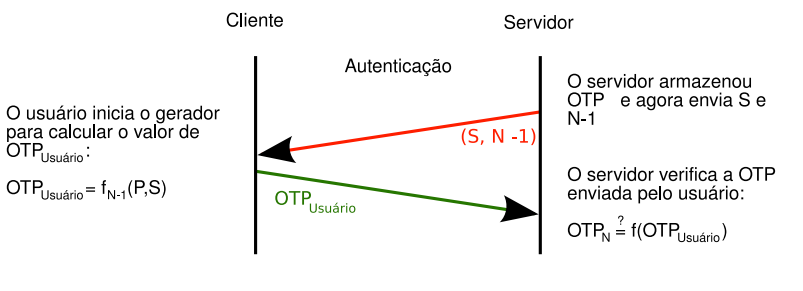


Figura 4 Durante a autenticação, o servidor apresenta a semente e um contador. O usuário executa um gerador para calcular a senha *one-time* e pede ao servidor sua validação.

exemplo 5). O sistema sobrescreve o hash da senha com uma série de asteriscos, mas o número de seqüência e a semente permanecem visíveis.

Alternativa: OTPW

A solução alternativa baseada em software OTPW não emprega o método especificado no RFC 2289, baseando-se numa versão de 160 bits do hash RIPEMD. O OTPW inclui uma versão modificada do programa de login (`demologin`) e um módulo alternativo para integração à pilha do PAM. Os usuários recebem senhas na forma de uma lista, semelhante às antigas linhas TAN usadas por bancos.

Para se autenticar, o usuário digita uma cadeia de caracteres com a entrada da lista e sua senha pessoal. O servidor OTPW guarda os hashes RIPEMD de todas as senhas one-time (junto com um número) no arquivo `.otpw` no *home* do usuário. O programa sobrescreve com traços as senhas usadas, impedindo assim sua reutilização.

O pacote OTPW é bem menor que o OPIE; o código-fonte possui apenas 18 arquivos. Um simples `make` cria os programas `demologin` e `otpw-gen`, assim como a biblioteca `pam_otpw.so`.

Em sistemas Linux com PAM, o OTPW requer apenas o gerador `otpw-gen` e o módulo `pam_otpw`. O usuário inicializa o sistema OTPW por meio do comando `otpw-gen` (**exemplo 6**). Depois de digitar uma senha, o `otpw-gen` cria uma lista de OTPs e exibe o resultado.

O parâmetro `-p1` faz com que o `otpw-gen` mostre as OTPs em uma lista de palavras de quatro letras, como por exemplo:

```
hare lane fyfe self lucy
```

Apagar o arquivo `.otpw` desativa o uso de senhas one-time nessa conta.

© Linux New Media do Brasil Editora Ltda.

Snow666

É importante imprimir a lista gerada. Os usuários são os responsáveis por acompanharem o número de senhas one-time ainda válidas.

Para economizar papel, também se pode verificar o conteúdo do arquivo `.otpw` ao fazer login. As OTPs são marcadas com um `-`. A integração do OTPW ao sistema PAM usa as mesmas etapas que o OPIE.

De acordo com a documentação, acrescentar essa entrada:

```
session optional pam_otpw.so
```

faz com que o OTPW informe quantas OTPs ainda estão disponíveis logo no login.

Esse comando não funcionou em nossos testes no laboratório. Os passos manuais para o daemon SSH são semalhentes àqueles do OPIE.

O usuário cria senhas one-time por meio da concatenação de sua senha pessoal com as cadeias de caracteres da lista gerada pelo `otpw-gen`.

Quando um usuário tenta fazer login, o OTPW cria um link simbólico para `.otpw.lock` no seu diretório `home`. Se o usuário cancelar a tentativa de login pressionando [**Ctrl**]+[C], o link simbólico é mantido. O usuário fica trancado do lado de fora enquanto o link estiver lá, pois ele impede o uso do OTPW.

Além disso, o OTPW normalmente não suporta logins simultâneos, por motivos de segurança. Segundo a documentação do programa, nesse caso o usuário deve digitar uma senha one-time estendida. A OTP estendida engloba a senha do usuário e mais três cadeias de caracteres contidas na lista. Não conseguimos testar esse comportamento no laboratório.

Senhas one-time são úteis em ambientes inseguros sob risco de farejamento de senhas. As implementações OPIE e OTPW são fáceis de integrar às distribuições Linux, graças ao PAM. ■

Mais informações

[1] OPIE: http://www.inner.net/opie

[2] OTPW: http://www.cl.cam.ac.uk/~mgk25/otpw.html

[3] JOTP: http://www.cs.umd.edu/~harry/jotp/

[4] Palmkey: http://palmkey.sf.net

[5] Gerador OTP Pilot: http://www.valdes.us/palm/pilOTP/

[6] Calculadora OTP e S/Key para X-Window: http://killa.net/infosec/otpCalc/

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 professional 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/américalatina

© Linux New Media do Brasil Editora Ltda.

Snow666
Gabarito

JÁ PENSOU EM TER SEUS SERVIDORES HOSPEDADOS NO UOL?

→ HOSTING DEDICADO

→ COLOCATION

→ GERENCIAMENTO DE SERVIDORES

→ PROJETOS ESPECIAIS

UOL HOST é a unidade de negócios UOL, especializada em soluções avançadas de Data Center. Oferecemos infra-estrutura e serviços para diversos tipos de aplicação, com alta confiabilidade, excelente desempenho, total monitoramento dos serviços, além de suporte técnico especializado 24x7x365.

Porque usar as soluções de Data Center do UOL HOST:

→ Seus aplicativos estarão hospedados na mesma estrutura do Portal UOL

→ Melhor performance e disponibilidade

→ Atendimento por equipe própria e especializada UOL HOST

→ Melhor relação custo x benefício do mercado

Fale agora com um de nossos gerentes de negócios:

São Paulo
(11) 3038-8720

Porto Alegre
(51) 3123-1788

UOL HOST
DATA CENTER

www.uol.com.br/idc

© Linux New Media do Brasil Editora Ltda.

Autenticação no Linux com Active Directory e Kerberos 5

Domando os cães do inferno

O sistema Active Directory da Microsoft oferece gerenciamento de usuários centralizado e um login único. Com poucos ajustes manuais, o Linux é capaz de aproveitar todo esse potencial.

por Walter Neu

Sistemas Linux vivem em paz com máquinas Windows em muitas empresas hoje em dia. Com freqüência, redes heterogêneas são compostas por softwares de escritório dominados pelo Windows e servidores Unix ou derivados. O serviço *Active Directory* (ou simplesmente AD, como é chamado), introduzido pela Microsoft no Windows 2000 Server, costuma ser usado para o gerenciamento centralizado de informações de usuários.

O Linux geralmente usa o sistema legado do `/etc/passwd` ou alguma solução distribuída como NIS ou LDAP. Porém, é fácil integrar o pingüim à infra-estrutura do AD por meio de algumas ferramentas gratuitas e abertas.

Este artigo parte do princípio de que existe um servidor Active Directory gerenciando uma estrutura completa de domínio no Windows. Com isso, vamos mostrar como configurar clientes Linux para fazerem login (autenticação), acessarem (autorização) e utilizarem a infra-estrutura do domínio. A cobertura do bolo é o recurso de login único (ou *single sign-on*), e a cereja é a capacidade de criar automaticamente diretórios de usuários nos clientes.

O exemplo deste artigo se baseia no serviço *Winbind* do projeto *Samba* e no *Kerberos* 5 para autenticação. Obviamente, o Kerberos não foi criado pelos engenheiros da Microsoft em Redmond; ela adaptou esse método de autenticação do mundo Unix. O Kerberos foi desenvolvido originalmente no MIT (EUA) na década de 1980. Tanto o projeto livre *Heimdal*[1] quanto a aplicação de referência do MIT [2] oferecem suporte completo ao Kerberos 5. O *Shishi*[3] é mais uma implementação livre.

Segredos bem escondidos

O Kerberos é um serviço de autenticação em rede baseado em tíquetes que depende de senhas compartilhadas. O sistema mantém uma área separada logicamente conhecida como *realm*, que pode incluir diversos clientes e serviços.

Neste exemplo, os clientes e vários serviços, como o servidor de arquivos, rodam em Linux. O Windows é responsável pelos serviços de diretório e autenticação pelo Centro de Distribuição de Chaves (*Key Distribution Center*, KDC). O KDC é um componente central do Kerberos (**figura 1**) que inclui o Servidor de Autenticação (AS) e o Servidor de Fornecimento de Tíquetes (TGS).

No início de uma sessão, cada membro (ou *principal*) do realm demonstra sua autenticidade ape-

© Linux New Media do Brasil Editora Ltda.

nas uma vez. Para isso, o principal pede um *Ticket Granting Ticket* (TGT) para o AS. Ele aplica esse tíquete no TGS para pedir outros tíquetes posteriores.

O que o Kerberos chama de tíquete é uma credencial eletrônica. Quando um principal recebe um tíquete, ele ganha acesso às aplicações "kerberizadas" que requerem provas de sua identidade, sem necessidade de digitar uma senha. Os usuários precisam apenas digitar uma senha para receber o TGT.

Tíquetes, por favor!

O programa de login pede um TGT em nome do cliente (vide a **figura 2**). Uma forma alternativa é o `kinit` fazer uma requisição após o login do usuário. O AS procura no Active Directory o membro que está pedindo o tíquete. Quando o encontra, o Active Directory fornece um TGT.

Então, o AS criptografa o TGT com a chave do membro e retorna o hash para a entidade que está pedindo o tíquete. Se ela for um cliente, o KDC extrai a chave da senha do usuário, criptografa-a e armazena seu hash no banco de dados do seu membro. O programa `login` ou o `kinit` calcula a chave secreta a partir da senha digitada pelo usuário no cliente e decifra o TGT. A senha jamais é transmitida sem proteção.

Quando um usuário precisa acessar um serviço kerberizado na rede, o usuário apresenta o TGT para o TGS e pede um tíquete de serviço para esse serviço. O TGS emite o tíquete em segundo plano. Agora que o cliente já possui o tíquete de serviço, ele consegue fazer login automático do usuário no serviço pedido sem pedir uma senha.

Os tíquetes do Kerberos possuem um tempo de vida limitado. O problema do tempo torna essencial a sincronia da hora do sistema em todos os computadores do realm. O servidor Kerberos se recusa a emitir um tíquete inicial para máquinas que estejam fora de sincronia por mais de cinco minutos.

Apesar de ser possível alterar esse limite de tempo por meio do cliente Kerberos ou do servidor Active Directory, faz mais sentido criar um servidor de hora centrali-

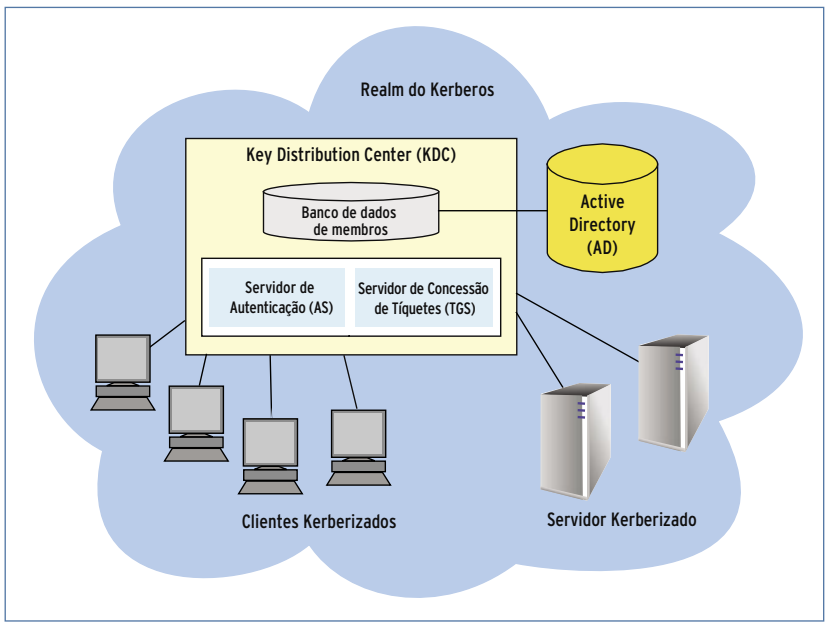


Figura 1 O Kerberos é um serviço de autenticação em rede baseado em tíquetes que depende de segredos compartilhados. Em sua arquitetura, todos os componentes pertencem ao realm do Kerberos. O núcleo do realm é o *Key Distribution Center* com seus componentes principais AS e TGS e o banco de dados de membros.

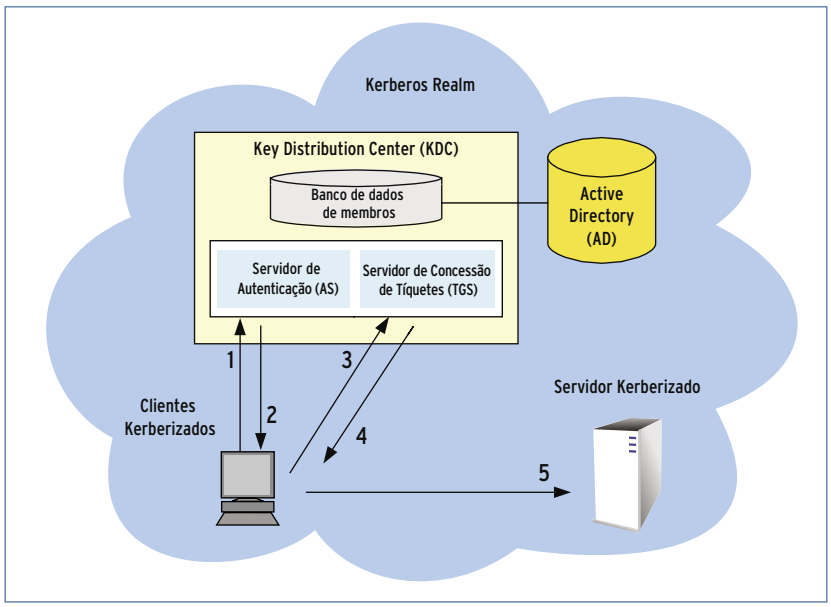


Figura 2 A autenticação com o Kerberos é sofisticada, mas flexível: o cliente envia uma requisição de TGT ao KDC (1) e recebe um tíquete de validade restrita (2). O tíquete autoriza o cliente a pedir (3) outros tíquetes (4) para serviços de rede kerberizados (5) sem necessidade de novas autenticações por senha.

© Linux New Media do Brasil Editora Ltda.

zado para permitir que os clientes sincronizem.

Os clientes também precisam ser capazes de resolver o nome DNS do servidor Kerberos. Se necessário, é possível adicionar um registro ao servidor central de nomes ou simplesmente manter o arquivo `/etc/hosts` estático em todos os sistemas envolvidos na troca.

Exemplo 1: /etc/kr5b.conf

```
01 [libdefaults]
02    default_realm = KDC.
➥EXEMPLO.ORG
03    dns_lookup_realm = false
04    dns_lookup_kdc = false
05 [realms]
06    KDC.EXEMPLO.ORG = {
07       kdc = w2k.kdc.exemplo.
➥org
08       default_domain = KDC.
➥EXEMPLO.ORG
09    }
10 [domain_realm]
11    .exemplo.org = KDC.
➥EXEMPLO.ORG
```

Exemplo 2: klist exibe os tíquetes

```
01 $ klist
02 Ticket cache: FILE:/tmp/
➥krb5cc_1000
03 Default principal: user@KDC.
➥EXEMPLO.ORG
04
05 Valid starting   Expires
➥Service principal
06 03/17/08   11:10:27 03/17/08
➥21:10   krbtgt/KDC.EXEMPLO.
➥ORG@KDC.EXEMPLO.ORG
07      renew until 03/18/08
➥11:10
08
09 Kerberos 4 ticket cache:
/➥tmp/tkt1000
10 klist: You have no tickets
➥cached
```

Instalação do Kerberos

Depois de respeitar os requisitos de tempo e resolução de nomes, deve-se instalar o Kerberos nos clientes Linux a partir dos pacotes da distribuição usada. Para a variante do MIT são necessários os pacotes *krb5-user* e *krb5-config* do repositório *Universe* no Ubuntu, ou *krb5-workstation* e *krb5-authdialog* no Fedora. Como alternativa, pode ser preferível compilar o código-fonte do MIT.

Para configurar o Kerberos, modifique o arquivo `/etc/kr5b.conf`. O **exemplo 1** mostra uma configuração mínima, porém funcional, do pacote do MIT; os clientes precisam disso para criarem uma conexão com o servidor Kerberos. As outras implementações do Kerberos usam mais ou menos a mesma sintaxe.

Criando realms

A linha `default_realm` na seção `[libdefaults]` cria um realm chamado *KDC.EXEMPLO.ORG* como padrão para aplicações Kerberos. Quando houver múltiplos realms, é possível acrescentar mais uma expressão à seção `[realms]`. A seção `[domain_realm]` define a relação entre nome de domínio e realm na biblioteca do Kerberos. Se for desejável que a biblioteca do Kerberos estabeleça uma conexão com uma máquina remota, a biblioteca precisa conhecer o realm onde reside a máquina. Entradas que começam com um ponto atribuem ao realm do Kerberos todas as máquinas com o sufixo determinado. Para garantir comunicações sem problemas com o servidor Kerberos, é importante usar caracteres em caixa alta no nome do realm.

Usando essa configuração, é possível testar a comunicação com o servidor Kerberos. O comando `kinit` solicita um TGT. Se não for especificado algum outro parâmetro, o programa tenta assegurar um TGT para o membro com nome igual àquele do usuário logado. Para permitir que isso aconteça, o usuário precisa digitar uma senha uma única vez.

O programa `kinit` então envia uma requisição de TGT sem criptografia para o servidor de autenticação; a requisição inclui o nome do membro (entre outros dados). A resposta enviada ao cliente inclui o TGT criptografado, que o `kinit` decifra e armazena localmente.

A saída do comando `klist` no **exemplo 2** inclui os dados de validade do TGT recém-emitido. Se a saída do comando mostrar o tíquete, pode-se presumir que a configuração do cliente Linux está completa. Para destruir o TGT de teste, use o comando `kdestroy`.

Membros

A próxima etapa consiste em adicionar o cliente Linux como membro do domínio no Active Directory. Para permitir isso, é preciso instalar a versão 3.0.14a ou posterior do *Samba*, junto com o pacote do Winbind para gerenciamento centralizado de usuários em Windows e Linux. O Winbind usa uma implementação para Unix

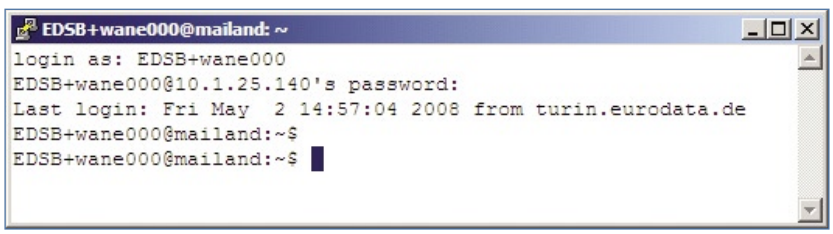


Figura 3 Como o servidor SSH identifica mais de um realm, o usuário wane000 precisa de um prefixo de domínio EDSB. O caractere + separa os dois nomes.

© Linux New Media do Brasil Editora Ltda.

Exemplo 3: smb.conf

```
01 [global]
02 ; Samba como controlador
➥de domínio
03     workgroup = kdc
04     password server = srv.
➥kdc.exemplo.org
05     security = ads
06     realm = KDC.EXEMPLO.ORG
07     encrypt passwords = yes
08
09 ; não é o navegador mestre
➥da rede Windows
10     local master = no
11     os level = 20
12     domain master = no
13     preferred master = no
14
15 ; Configuração do Winbind
16     winbind separator = +
17     idmap gid = 10000-20000
18     idmap uid = 10000-20000
19     template shell = /bin/
➥bash
20     template homedir = /
➥home/%D/%U
21 winbind enum users = yes
22 winbind enum groups = yes
```

das chamadas RPC da Microsoft, o PAM (*Pluggable Authentication Modules*) e o NSS (*Name Service Switch*) para permitir que os clientes Linux façam login no domínio Windows e trabalhem como usuários locais.

O Samba é configurado no arquivo `smb.conf`, geralmente encontrado sob `/etc/samba/`. O **exemplo 3** mostra um arquivo de configuração de exemplo que implementa um servidor membro de um domínio Active Directory com a configuração necessária do Winbind.

O parâmetro `security = ads` na **linha 5** faz o Winbind não procurar a senha no banco de dados local de usuários, repassando-a para o controlador do domínio do Active Directory. O controlador do domínio então decide se a senha é legítima.

Caso o controlador do domínio seja um sistema Windows 2003, é preciso definir `clientschannel = no` na seção `[global]`. Antes de o cliente se tornar um membro do domínio, o administrador o informa (na **linha 6**) a qual realm Kerberos pertence o membro.

Gerenciamento centralizado

Pertencer a um domínio elimina somente a necessidade de gerenciamento de senhas no sistema local; não elimina a necessidade de gerenciar as entradas de usuários. Os usuários do domínio ainda são uma propriedade desconhecida do sistema. Sistemas operacionais derivados do Unix precisam do *daemon winbindd* para garantir sua visibilidade. O componente do pacote Samba usa o NSS para resolver as identidades de usuários do domínio e servi-las ao Linux como se fossem credenciais locais.

Enquanto o Winbind está em execução, ele transfere temporariamente todos os usuários e grupos do Active Directory para o sistema Linux. Isso reduz substancialmente o trabalho administrativo do gerenciamento de usuários. O Winbind é configurado de forma centralizada na seção `[global]` do arquivo `smb.conf` (**linhas 15 a 20**).

A instrução `workgroup = kdc` na **linha 3** é importante: o Samba usa a instrução `workgroup` para definir tanto um grupo de trabalho quanto um domínio. O programa Samba decide mais tarde o que deve configurar. O domínio AD é armazenado na sintaxe do NT4 nesse ponto; em outras palavras, se houver um domínio Windows 2003 em `kdc.exemplo.org`, o Samba esperará `kdc`.

O parâmetro do Samba na **linha 6** configura o realm; normalmente, esse é o nome DNS do controlador do domínio, mas em caixa alta – ou seja, `KDC.EXEMPLO.ORG`.

Separação

O caractere que separa o domínio e o nome do usuário no Windows é a contrabarra (`\`). Entretanto, esse caractere tem significado especial no shell. Para evitar conflitos, o administrador deve definir o `winbind separator` para não usar o metacaractere do shell, usando um sinal de mais (`+`) em seu lugar, como mostra a **linha 16 do exemplo 3**.

Se houver apenas um domínio, não é necessário separar o domínio dos nomes de usuários. O Winbind fornece a configuração `winbind use default domain = yes` na seção global do arquivo de configuração. Esse parâmetro faz o Linux usar os nomes de usuários do Active Directory sem o elemento do domínio. Se isso não for definido, será necessário acrescentar um prefixo de nome de domínio aos usuários servidos pelo Winbind para usarem-no no Linux (veja a **figura 3**).

Com seus próprios dispositivos, o sistema Linux é incapaz de converter nomes de usuários e grupos do domínio para seus equivalentes nu-

Exemplo 4: Mudança de dono

```
01 # ls -l foo.txt
02 -rw-r--r-- 1 root root May 02 15:53 foo.txt
03 # chown KDC+wnew foo.txt
04 # chgrp KDC+asp foo.txt
05 # ls -l foo.txt
06 -rw-r--r-- 1 KDC+wneu KDC+asp May 02 15:53 foo.txt
```


© Linux New Media do Brasil Editora Ltda.

Snow666

méricos (UID e GID). Porém, isso é necessário porque o Linux não usa nomes internamente, baseando-se nessas IDs em vez disso. Por exemplo, o comando `ls` examina o inode de um arquivo para descobrir o UID de seu dono e traduz esse valor para um nome antes de exibir essa informação na tela.

O Linux usa uma API universal, o NSS, para mapear nomes. O NSS pode buscar no arquivo `/etc/passwd` ou, se o módulo necessário estiver carregado, consultar um servidor Active Directory. Essa capacidade permite a listagem dos usuários e grupos de um realm ADS como se fossem contas locais. Para permitir que isso ocorra, é necessário adicionar o nome de serviço `winbind` aos bancos de dados `passwd` e `group` no arquivo de configuração `/etc/nsswitch.conf`:

```
passwd: files winbind
group:  files winbind
```

Essas linhas fazem com que o serviço de nomes comece buscando arquivos locais como `/etc/passwd` antes de contactar o winbindd. Se o NIS também estiver em uso, pode-se digitar `compat` em vez de `files`.

O que ainda está impedindo o sucesso na cooperação entre o Linux e o AD baseado em Windows é que o computador Linux precisa se tornar um membro do domínio para receber informações de usuário e grupo para o domínio.

O parâmetro `security = ads` na **linha 5** adiciona o Samba como um membro do domínio AD. O comando `net ads`, que faz parte da distribuição do Samba (veja a **figura 4**), completa a transação. O usuário do domínio, *Administrator*, nesse caso, precisa ter autorização para adicionar o computador com Linux ao domínio. O comando `net` pede a senha para o usuário autorizado e, se ela estiver correta, cria a conta do computador no controlador do domínio. Se tudo isso funcionar, o cliente Linux será um membro completo do ambiente Active Directory.

Exemplo 5: Configurações do PAM

```
01 # /etc/pam.d/common-auth
02 auth sufficient pam_krb5.so forwardable
03 auth required pam_unix.so nullok_secure use_first_pass
04 auth required pam_deny.so
05
06 # /etc/pam.d/common-account
07 account sufficient pam_krb5.so forwardable
08 account required pam_unix.so
09
10 # /etc/pam.d/common-session
11 session sufficient pam_krb5.so
12 session required pam_unix.so
13
14 # /etc/pam.d/common-password
15 password sufficient pam_krb5.so nullok obscure md5
16 password required pam_unix.so nullok obscure md5
```

Para testar se a conexão com o controlador de domínio está funcionando adequadamente, use a ferramenta de diagnóstico `wbinfo`. Ela faz parte do pacote *Winbind*. O parâmetro `-u` faz o comando listar todos os usuários do domínio disponíveis no domínio:

```
KDC+wneu
KDC+mkreis [...]
```

O domínio em uso, nesse caso, é chamado de `KDC`. O nome do domínio é seguido pelo separador configurado como `winbind separator`, ou seja, `+`, nesse caso, e também pelo nome do usuário. Os nomes obtidos do AD agora já são

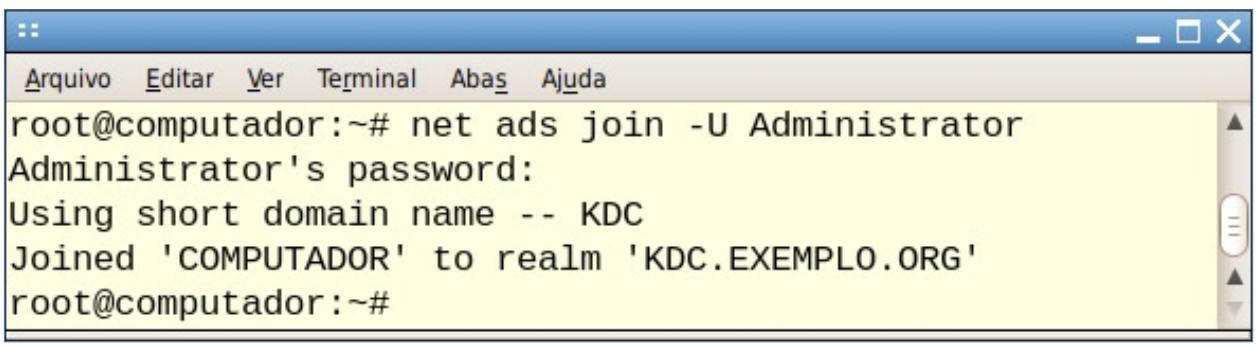


Figura 4 Para adicionar a máquina local como membro do domínio padrão, o usuário do controlador do domínio (DC) precisa de privilégios administrativos. Depois de digitar a senha, o DC adiciona o novo cliente ao domínio.

© Linux New Media do Brasil Editora Ltda.

familiares para o Linux e podem ser usados para o login. Os grupos definidos no AD podem ser listados com `wbinfo -g`:

```
KDC+accounts
KDC+asp [...]
```

Para exibir um panorama de todos os usuários e grupos dos bancos de dados do domínio ou local, use `getent passwd` ou `getent group`. A saída é semelhante aos arquivos `/etc/passwd` e `/etc/group`.

Agora teste se o Linux consegue identificar os nomes de usuário e grupo no AD: se o administrador do sistema Linux puder atribuir um dono e um grupo a um arquivo armazenado numa máquina Linux a um usuário e um grupo pertencentes ao domínio AD, isso é uma vitória. Dependendo do parâmetro `winbind use default domain` na configuração do Samba, o root pode especificar o dono como `Domínio+Usuário` e o grupo como `Domínio+Grupo` (**exemplo 4**).

Kerberos + PAM

O próximo truque é integrar o Kerberos, os usuários do domínio do AD e o mecanismo de login do Linux. Antes, cada um desses serviços esperava que o usuário se autenticasse e depois aplicava seus próprios mecanismos de autenticação e autorização para conceder aos usuários acesso aos serviços fornecidos. O PAM fornece uma interface unificada para essa autenticação integrada[4].

Alterar o método de autenticação no PAM significa mudar e servir módulos correspondentes que todos os programas possam acessar. Em outras palavras, o PAM adiciona uma camada de abstração entre a autenticação e os serviços propriamente ditos, mas sem necessidade de alterar os aplicativos. Programas como servidores FTP e Telnet se conectam a um serviço de autenticação chamando as funções da biblioteca PAM disponíveis como bibliotecas compartilhadas.

Existe uma biblioteca especial de módulo para alterar o método de autenticação do login para o Kerberos por meio do PAM. Os pacotes dessa biblioteca estão disponíveis na maioria das distribuições populares. O módulo em si é chamado `pam_krb5.so` e geralmente reside em `/lib/security/`[5].

Configuração individual

O módulo não lida apenas com o login por Kerberos, mas pede transparentemente um TGT ao servidor de autenticação em nome do usuário. Fazer isso funcionar envolve alterar diversas configurações no diretório `/etc/pam.d/`.

Cada aplicativo que requer autenticação e usa o PAM precisa de um arquivo individual em `/etc/pam.d/`. As distribuições tendem a organizar a configuração de formas um pouco diferentes, e algumas delas importam arquivos compartilhados. Cada linha desses arquivos inclui o tipo, uma marca de controle, um caminho do módulo em questão e argumentos opcionais, todos separados por espaços (**exemplo 5**). O Fedora usa a ferramenta `authconfig`, o OpenSUSE se baseia no *YaST* para manipular a configuração do PAM, e os usuários do Debian precisam editar manualmente os arquivos.

Seção por seção

Os arquivos de configuração são divididos em seções para os quatro tipos de módulos do PAM: `auth`, `account`, `password` e `session`. A seção `auth` define dois métodos alternativos de autenticação para determinar se os usuários são quem alegam ser (**linhas 2 e 3**). O PAM pede ao usuário uma senha apenas uma vez, e o Kerberos verifica as credenciais (**linha 2**). Se essa etapa for concluída com sucesso, a `pam_krb5.so` requisita um TGT com um bit *forward-capable* ativado para usar o tíquete num sistema remoto.

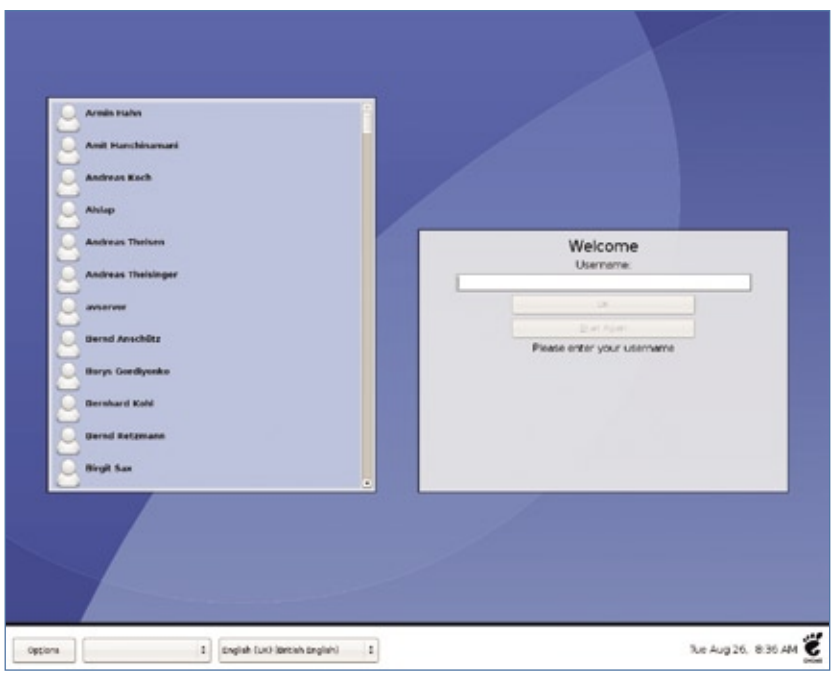


Figura 5 O GDM mostra tanto os usuários locais quanto os do AD como candidatos ao login.

© Linux New Media do Brasil Editora Ltda.

Snow666

Em caso de sucesso, o processo de autenticação marca o `pam_krb5.so` como `sufficient` e termina sem processar outros módulos.

Segunda chance

Caso a autenticação falhe, o PAM chama o segundo módulo, `pam_unix.so`, para garantir que a conta do usuário exista localmente (**linha 3**). Se o PAM for incapaz de alcançar o servidor de autenticação, o root ainda conseguirá fazer o login. O argumento `use_first_pass` do módulo significa que o segundo método de autenticação deve reutilizar a senha digitada pelo usuário em vez de pedi-la novamente. Graças ao `nullok_secure`, não há necessidade de definir uma senha no arquivo local de senhas. Apesar de ser possível fazer login com uma senha em branco, isso só é permitido nos terminais listados em `/etc/securetty`.

Depois que o PAM terminar de processar os módulos do tipo `auth`, ele prossegue à execução do próximo `include@`. O arquivo `common-account` novamente contém dois módulos, `pam_krb5.so` e `pam_unix`, e é responsável por lidar com o acesso ao sistema.

O serviço `account` do PAM verifica a senha do usuário para ver se ela ainda é válida ou se o acesso do usuário ao sistema é restrito em relação ao tempo, uso de recursos ou localização.

Se o usuário existir e tiver permissão de fazer login, o PAM segue para a próxima pilha de módulos, que é descrita pelo arquivo `common-password`. Esses módulos dão aos usuários a possibilidade de alterarem suas senhas. Diferente do procedimento normal no Linux, que só permite a troca da senha do próprio usuário, o módulo do Kerberos oferece a qualquer usuário a possibilidade de alterar a senha de qualquer outro. Porém, para fazer isso, o usuário precisa saber a senha atual da conta a ser alterada.

Gerenciamento de sessão

Por último, o PAM chama os módulos configurados em `common-session`. O tipo `session` é responsável por toda a parte extra de autenticação. As etapas que ainda faltam incluem definir variáveis ou montar diretórios. No escopo desse serviço PAM, o `pam_krb5` realiza uma tarefa muito importante: apaga os tíquetes do usuário quando este faz logout.

Depois de completar a configuração, qualquer programa compatível com PAM pode usá-lo para acessar o AD. Por exemplo, o GDM oferece tanto contas locais quanto de usuário de domínio como candidatas para o login e inicia a sessão pedida após a autenticação com o servidor Kerberos (**figura 5**).

Como última etapa, os usuários do AD precisarão de um diretório `home`. Se o NSS não contiver detalhes desse diretório, ou se o diretório informado não existir, o Linux enviará o usuário para o diretório raiz ou não permitirá que ele acesse o sistema – apesar da autenticação com sucesso –, porque um ambiente de desktop como o KDE precisa ser e escrever certos arquivos que não existirão.

/home, sweet /home

Os diretórios `home` são configurados na **linha 20** do arquivo `smb.conf` mostrado no **exemplo 3**: `template homedir = /home/%D/%U`. O Samba substitui o `%D` pelo nome de domínio curto, e o `%U` pelo usuário do domínio. O administrador pode criar os diretórios individualmente para cada usuário ou automatizar o processo chamando o módulo `pam_mkhomedir`, que integra a distribuição do PAM e é configurado na seção `session`:

```
# /etc/pam.d/common-session
session required pam_mkhomedir.so
➥silent skel=/etc/skel/ umask=0022
session sufficient pam_krb5.so
session required   pam_unix.so
```

Essa configuração faz com que o módulo crie dinamicamente os diretórios `home` que faltarem. O argumento `silent` suprime mensagens oriundas da cópia do diretório de esqueleto (`/etc/skel/`, no caso). O último argumento diz ao PAM para definir o `umask` padrão para arquivos e diretórios como `0022`. A configuração permite que os programas que estejam rodando na sessão criem diretórios com permissões `rwxr-xr-x` e arquivos com `rw-r--r--`.

Como alternativa a diretórios locais em clientes kerberizados, é possível usar diretórios `home` num servidor de arquivos central. O módulo do PAM `pam_mount.so` ajuda nessa tarefa. Qualquer comando genérico que se deseje executar após o procedimento de login é adicionado aos scripts de inicialização em `/etc/profile`.

Totalmente integrado

São necessários vários passos para suportar o login automatizado no Active Directory e diretórios `home` num cliente Linux, mas com Kerberos, NSS, PAM e Samba, esse projeto de integração pode ajudar a manter amizades com seus vizinhos de Redmond. ■

Mais informações

[1] Kerberos Heimdal: http://www.h5l.org

[2] Kerberos MIT: http://web.mit.edu/kerberos

[3] Kerberos Shishi: http://josefsson.org/shishi/

[4] PAM: http://ftp.kernel.org/pub/linux/libs/pam/

[5] Pam-krb5: http://www.eyrie.org/~eagle/software/pam-krb5/

© Linux New Media do Brasil Editora Ltda.

Snow666

TUDO SOBRE COMUNICAÇÃO IP

www.ipcomm2008.com.br

Agende!

IP COMMUNICATIONS BRASIL 2008

2 a 4 de dezembro de 2008 - Centro de Convenções Rebouças - São Paulo - SP - Brasil

IPComm 2008

- VoIP
- IP Avançado
- Soluções VoIP Open Source
- Tutoriais

Eventos Paralelos

Terrebit Peering Forum Brasil 2008 - Terremark

IP Expo

- Os melhores produtos e serviços para a Comunicação sobre IP

PATROCÍNIO

digium | Asterisk · CommLogik Corporation · Dialogic · DIATORA · KHOMP · terremark · isolve solve is our business · TEMPO REAL

MÍDIA: LINUX MAGAZINE · Convergência DIGITAL · IP news

APOIO: Asterisk Brasil.org

REALIZAÇÃO: IP COMMUNICATIONS BRASIL

ORGANIZAÇÃO: SCALE Comunicação e Marketing

© Linux New Media do Brasil Editora Ltda.

Biometria em Linux

É você mesmo?

A autenticação biométrica já é usada em todo o mundo. Conheça as iniciativas de código aberto para uso dessa técnica.

por Alessandro de Oliveira Faria (Cabelo)

Segundo o dicionário, biometria é o ramo da ciência que estuda os seres vivos baseando-se nas medidas e estrutura dos órgãos. "Bios"="vida" e "metron"="medida"; sendo assim, define-se biometria como "medida da vida". A biometria deixou de ser ficção científica há algum tempo e hoje faz parte do nosso dia-a-dia. Ao contrário do que muitos pensam, a biometria era utilizada muito antes da era da informática.

No século II a.C., governantes da China utilizavam impressões digitais para lacrar documentos. Além disso, em todo o mundo a impressão digital e fotos são utilizadas para registrar um ser humano, e com esses registros é possível a identificação sem grandes esforços.

O ineditismo na década de 90 foi apenas a utilização da biometria em sistemas de informática. A biometria ganhou atenção científica somente no final do século XIX, quando as características físicas das pessoas passaram a ser armazenadas para fins judiciais. Já no início do século XX, a biometria ganhou espaço nos documentos de identidade (RG, no Brasil).

Atualmente, no início do século XXI, esse assunto encontra-se em evidência para garantir a autenticação e gerenciamento de identidade. Para tal tarefa, a biometria é totalmente pertinente à situação. O principal motivo é a estabilidade das características corporais e comportamentais, assim agregando confiabilidade à tecnologia.

A biometria com código aberto evolui a cada dia, cada projeto na sua velocidade de amadurecimento. Essa evolução não acontece na velocidade dos projetos de software convencionais. Os principais motivos, na minha opinião, são a necessidade de profundos conhecimentos matemáticos e testes populacionais. Ou seja, qualquer projeto biométrico precisa de uma amostragem numerosa para obter uma evolução significativa em termos de algoritmo matemático.

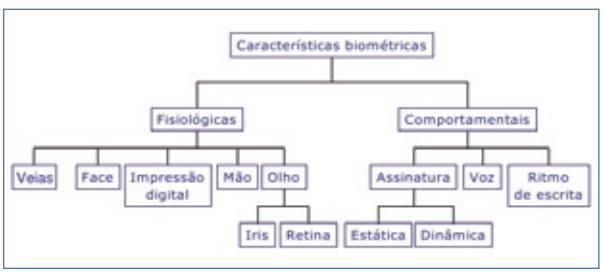


Figura 1 Classificação das técnicas biométricas.

Para quem deseja fundamentar conceitos de desenvolvimento nesse segmento, são aconselháveis estudos de algoritmos de visão computacional como *OpenCV* e *Mimas* para se familiarizar com processamento de imagens, reconhecimento de padrões e treinamento da rede de algoritmos.

No Brasil, a NETi Tecnologia desenvolve e pesquisa o assunto na plataforma Linux desde 1998. Atualmente, a empresa trabalha comercialmente com foco na tecnologia proprietária de reconhecimento facial da Cognitec System. Entretanto, a divisão de pesquisa sempre tem atenção às soluções de código aberto.

Conceito

O homem sempre teve a necessidade de restringir o acesso de outras pessoas a determinados locais ou bens considerados privilegiados ou particulares. Normalmente utilizamos cartões ou senhas para obter acesso a sistemas ou locais restritos. Entretanto, senhas e cartões podem ser roubados, perdidos, esquecidos ou revelados. Nesse momento começam as preocupações relacionadas a fraude e acesso por usuários não autorizados. Já a biometria converte uma característica ou comportamento em códigos de barras humanos que não apresentam esses pontos negativos.

© Linux New Media do Brasil Editora Ltda.

Para efetuar a autenticação biométrica em sistemas computacionais de código aberto ou proprietários, devemos num primeiro momento entender o conceito e a funcionalidade dessa tecnologia, independente do tipo (impressão digital, face, voz, íris e outros).

Em primeiro lugar, a biometria pode resolver duas necessidades distintas, ou seja, podemos utilizá-la para verificar a identidade de um usuário ou para identificá-lo. Em ambos os casos, a biometria é a única maneira de garantir a presença do proprietário durante a operação.

A identificação é apenas uma varredura no banco de características em memória ou em disco. Esse processo decide qual registro de amostragem possui o coeficiente de similaridade mais próximo ao do usuário submetido à identificação. Essa tarefa requer maior poder computacional, sendo que toda a base de dados será analisada no menor tempo possível e aceitável para uma operação. Essa técnica é chamada de *1:N* (um para muitos), porque os dados da pessoa são comparados a todos os registros da base de dados.

A verificação de identidade é o processo mais utilizado em sistemas de autenticação de usuários, pois nessa operação o usuário necessita informar a sua identidade ou PIN (número de identificação pessoal). Ao informar o PIN (por meio de um login, código, email ou outros), o usuário estará previamente recuperando na base de dados o seu registro biométrico para uma comparação. Essa técnica é conhecida por *1:1* (um para um), pois os dados do usuário são comparados apenas a um registro do banco de dados.

BioAPI

Com o mercado em constante evolução, diversas APIs e tecnologias biométricas, assim como o grande número de padrões, causam confusões e retrabalhos aos desenvolvedores de aplicativos. Então, algumas empresas sentiram a necessidade da criação de uma API única para garantir o manuseio e evolução das tecnologias biométricas. Vale a pena ressaltar que alguns projetos de código aberto, como o *Libface*, estão prevendo a compatibilidade com o consórcio da BioAPI.

Foi assim que surgiu a BioAPI Consortium, com os seguintes objetivos:

- propiciar uma API com diversos níveis;
- disponibilizar uma plataforma suportada por múltiplas tecnologias biométricas;
- oferecer uma arquitetura de segurança robusta;
- garantir o desenvolvimento independente do distribuidor.

Sendo assim, a BioAPI proporciona aos programadores o mais alto nível da API, garantindo, dentro do possível, a produtividade, a portabilidade e a preservação do investimento. A criação desse padrão único foi possível tomando como ponto de partida um exame das APIs existentes no mercado e baseando-se nos pontos positivos das chamadas de cada API.

Tipos de biometria

A biometria pode ser utilizada com o comportamento do usuário ou características físicas (veja a **figura 1**). Obviamente, cada uma das opções possui seu grau de complexidade matemática. A impressão digital, veias da mão, face, íris, retina e geometria da mão são classificadas como características fisiológicas. Já o reconhecimento de escrita, voz e assinatura encontram-se no grupo de características comportamentais. A aplicabilidade de cada tecnologia deve ser confrontada com a necessidade do cliente para obter a melhor tecnologia empregada.

O **reconhecimento facial** é o método mais usual para reconhecimento entre seres humanos. Além de identificarmos pessoas, podemos perceber seu estado emocional apenas observando sua expressão facial. Aplicações estáticas e assistidas (nas quais a imagem, a iluminação ambiente e a verificação são controladas) favorecem a precisão do sistema. Quando a aplicação é desassistida ou a iluminação ambiente e a imagem não são controladas, devemos aumentar o coeficiente de similaridade, tornando o sistema exigente e obtendo, assim, resultados precisos.

Embora o reconhecimento facial seja uma tarefa simples para o ser humano, é extremamente complexo

Figura 2 Projeto Malic em ação marcando os pontos importantes para a identificação facial.

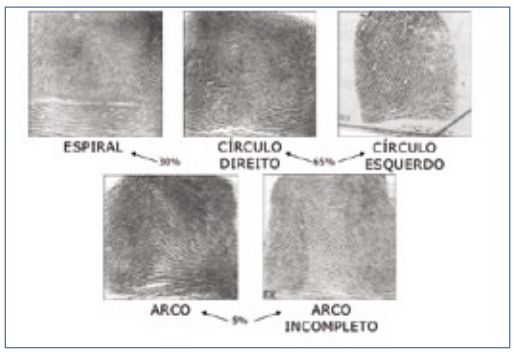


Figura 3 As impressões digitais se enquadram em cinco categorias distintas, mas em todas elas as medições são feitas da mesma forma.

© Linux New Media do Brasil Editora Ltda.

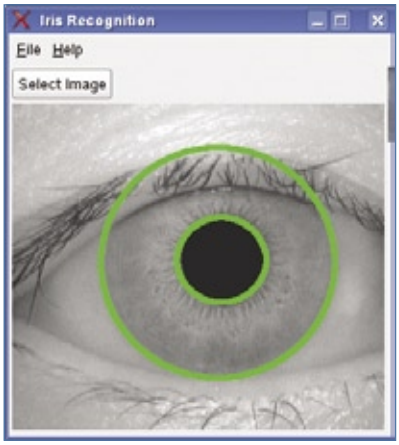


Figura 4 Antes de proceder aos cálculos para identificação da íris, o software precisa definir seus limites.

implementar esse processo em uma máquina, pois não sabemos ao certo como o cérebro humano realiza essa tarefa. O cérebro humano pode identificar corretamente uma pessoa a partir de sua imagem facial mesmo sob as mais diversas condições, como variações de iluminação, observando apenas uma de suas características ou partes, e até mesmo com distorções ou deformações.

Diversos projetos de código aberto, como *Libface* e *Malic* (**figura 2**), trabalham com a tecnologia de reconhecimento facial. Porém, é aconselhável o uso desses projetos apenas para fundamentar conceitos matemáticos e computacionais, pois eles não sofrem atualizações periódicas. Além disso, esses pacotes trabalham com bibliotecas matemáticas voltadas para o uso de visão computacional e reconhecimento de padrões. Para trabalhar com essa tecnologia na plataforma Linux, é imprescindível ter profundos conhecimentos das APIs de vídeo-captura *V4L* (*video for linux*) nas versões 1 e 2, pois a utilização e conversão dos espaços de cores utilizados (RGB,YUV,YUY2) impacta diretamente no consumo de memória e CPU.

Vale a pena ressaltar que essa tecnologia pode ser aplicada a fluxos de vídeo ao vivo (dispositivo de vídeo-captura como uma webcam) e também podemos efetuar o reconhecimento com uma foto armazenada em disco. Assim, desvinculamos a tecnologia de um hardware específico.

A **impressão digital** é formada nas superfícies dos nossos dedos nos primeiros meses de vida. Na verdade, sua constituição acontece ainda quando feto. A impressão digital acompanha a pessoa por toda a sua existência sem apresentar grandes mudanças.

As digitais são classificadas em cinco grupos (mostrados na **figura 3**): círculo esquerdo, círculo direito, arco, espiral e arco incompleto. Ela é composta por linhas formadas pelas elevações da pele. A comparação por impressão digital é um método muito utilizado atualmente como forma de identificação de usuários.

Extraindo os pontos característicos ou "pontos de minúcias" de uma impressão digital, um papiloscopista ou sistemas computadorizados podem identificar pessoas utilizando cálculos bastante confiáveis. Grande parte dos algoritmos trabalham com o princípio de extração dos pontos de minúcias ou pontos característicos. Após a extração, são calculados a relação entre as distâncias desses pontos. Cada algoritmo possui a sua base de cálculo, seja por análise dos pontos entre si ou por agrupamentos de pontos para análise de semelhanças de triângulos com os ângulos internos.

Essa tecnologia está vinculada ao hardware biométrico. Ou seja, os sensores utilizados para obter a imagem da digital impactam na performance do sistema, por causa da resolução da imagem obtida. Existem diversos projetos de código aberto, em particular o promissor projeto *fprint*, que surgiu da união de outros projetos de código aberto. Além disso, a biblioteca fprint se encontra em um estágio de produto e não de prova de conceito.

Embora essa tecnologia apresente um vínculo com o hardware de captura das digitais, o projeto livre fprint apresenta uma compatibilidade com uma ampla variedade de sensores disponíveis no mercado (inclusive os da Microsoft).

A **íris** constitui anéis em torno da pupila delimitados pela parte branca do olho. A íris carrega consigo diversas informações de um indivíduo. Gêmeos univitelinos apresentam íris diferentes. A complexidade da íris do olho humano teoricamente a torna única a cada usuário. A imagem da íris pode ser capturada utilizando-se uma câmera convencional, iluminação adequada e luz infravermelha. A captura pode ser automatizada pelo sistema ou capturada manualmente. No caso de captura automática, o software deve se encarregar do ajuste do foco (**figura 4**), entre outras propriedades da imagem.

O projeto JIRRM, embora não apresente atualizações, reconhece uma íris presente na imagem submetida ao sistema. Na página oficial[1], encontramos informa-

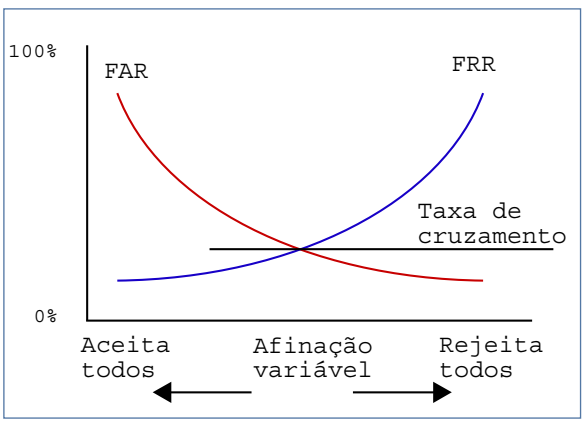


Figura 5 O ponto de cruzamento entre os falsos positivos e falsos negativos é o que se busca no momento de conferir uma medida biométrica.

© Linux New Media do Brasil Editora Ltda.

ções que mencionam planos para processamento e comparação entre amostras. O projeto JIRRM identifica a íris e somente então limita a área para posterior análise. Não se pode deixar de mencionar que essa tecnologia também trata dos problemas de fracasso na leitura (*Failure to Enroll* – FTE).

Precisão e confiabilidade

Na escolha de um sistema de autenticação biométrico, o desempenho deve ser levado em conta, pois também está relacionado à taxa de acertos e erros da biometria. Essas taxas são medidas pelos coeficientes FAR (taxa de falsa aceitação) e FRR (taxa de falsa rejeição). Esses termos são utilizados constantemente em qualquer documentação relacionada a projetos biométricos.

O FAR é o coeficiente que mede e quantifica, em porcentagem, quantas vezes os usuários não cadastrados foram falsamente aceitos no sistema. Já o FRR corresponde à medida de usuários cadastrados que foram rejeitados pelos sistema incorretamente. Como mencionado anteriormente, alguns documentos também trabalham com o FTE (fracasso de leitura), que representa os usuários que não conseguem efetuar o cadastramento. Por exemplo, alguns documentos estatísticos mencionam que, dependendo da região no mundo, entre cinco e dez por cento da população não possuem impressão digital com amostragem suficiente para cadastramento.

Figura 6 É relativamente fácil burlar um sistema de autenticação por impressão digital com materiais e ferramentas simples.

A configuração dessas taxas é fundamental para o desempenho do sistema. A falsa rejeição causa frustração e a falsa aceitação causa fraude.

Muitos sistemas podem ser configurados para fornecer detecção forte (baixo FAR e alto FRR) ou detecção fraca (baixo FRR e alto FAR). A medida crítica é conhecida como taxa de cruzamento (*crossover rate*), e é o ponto onde o FAR e o FRR se cruzam (**figura 5**).

Nada é perfeito

A ciência não é perfeita, e ocasionalmente variações podem causar uma falsa rejeição ou aceitação dependendo do critério na configuração do sistema. Existem maneiras comprovadas para se burlar leitores de impressão digital utilizando uma amostragem digital falsa feita de gelatina ou silicone (**figura 6**). Características físicas da gelatina idênticas à da pele já proporcionaram fraudes ao sistema [2].

Por menor que seja a taxa de erro, ela ainda existe. No ano de 1903, um dos casos mais polêmicos envolvendo identidade enganada foi o de Will West, que foi julgado e condenado por um crime que não havia cometido.

Além da semelhança visual entre Will e o verdadeiro criminoso (confira na **figura 7**), os dois homens também tinham nomes semelhantes. As fórmulas derivadas das medidas de Bertillon também eram quase idênticas, ou seja, encaixavam-se na variação de características aceitável para um mesmo indivíduo.

Com o poder computacional dos dias atuais, a precisão dos algoritmos atingiu um nível de confiabilidade muito alto, principalmente as tecnologias que trabalham diretamente com imagens ao vivo ou estáticas. Porém, para aumentar ainda mais essa margem de acertos, sugere-se a utilização da multi-biometria (utilização de duas ou mais tecnologias biométricas), assim tornando inviável uma fraude em qualquer sistema computacional. Há diversos tutoriais sobre esse assunto no portal Viva o Linux [3]. ■

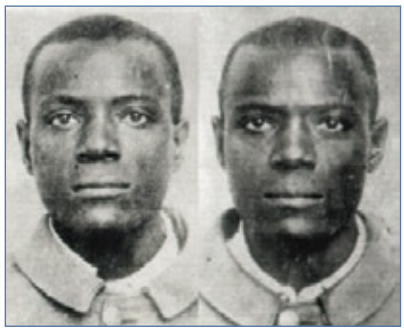


Figura 7 Em 1903, Will West foi condenado erroneamente por um crime que não cometeu – em virtude de um erro do método matemático.

Mais informações

[1] JIRRM: http://jirrm.sourceforge.net/

[2] Sandstrom M., "Liveness Detection in Fingerprint Recognition", 2001: http://liu.diva-portal.org/smash/record.jsf?pid=diva2:19729

[3] Portal Viva o Linux: http://www.vivaolinux.com.br/

Sobre o autor

Alessandro Faria é sócio-proprietário da NETi Tecnologia (http://www.neti-tec.com.br), especializada em desenvolvimento de software e soluções biométricas. Além disso, é consultor biométrico na tecnologia de reconhecimento facial, desenvolve soluções de código aberto desde 1998, é membro colaborador do portal Viva O Linux e mantenedor da biblioteca de código aberto de vídeo captura, entre outros projetos.

© Linux New Media do Brasil Editora Ltda.

O módulo NRPE do Nagios

Olheiro do Nagios

O flexível Nagios é capaz de executar comandos remotos nas máquinas monitoradas. Veja como com o NRPE.

por Vinicius Andrade Marino

A rede ideal não sofre de problemas. Uma vez implantada, ela não apresenta quedas, lentidão, tentativas de invasão ou qualquer outra dificuldade. No entanto, todos sabemos que não existe rede ideal, e por isso é tão importante monitorar as máquinas ligadas a ela, sejam elas servidores, desktops ou qualquer outro aparelho.

Este artigo tem como objetivo abordar a integração do popular software de monitoramento Nagios[1] aos servidores Linux de uma rede, e para isso emprega o módulo *NRPE*.

NSCA x NRPE

O Nagios funciona em uma estrutura servidor-agente. Na máquina responsável pelo monitoramento fica instalado o servidor Nagios, enquanto as máquinas monitoradas (servidores Web, de e-mail etc. – ou ainda desktops) abrigam agentes que informam dados ao servidor.

Atualmente existem dois módulos para o gerenciamento de servidores Linux: o NRPE (*Nagios Remote Plugin Executor*) e o NSCA (*Nagios Service Check Acceptor*). Ambos exercem a mesma função, mas com características distintas. O NSCA faz suas checagens de maneira passiva, ou seja, executa comandos externos em um certo período de tempo e os submete ao servidor Nagios para "interpretação" de seus status (**figura 1**).

Essa monitoração não ocorre em tempo real e não é controlada pelo *daemon* do Nagios, o que dificulta um pouco sua operação.

Normalmente, o NSCA é utilizado para monitorar sistemas de segurança, como é o caso do *Snort*[2]. Nunca se sabe quando e quantos alertas de segurança serão recebidos, e então o trabalho do administrador pode ser bastante facilitador por uma visualização periódica do que está acontecendo.

Vale lembrar que o NSCA pode ser facilmente implementado em ambientes complexos, pois não necessita de qualquer regra adicional no firewall. Isso é bastante útil naqueles ambientes corporativos em que para ter acesso ao firewall é preciso atravessar um corredor com espinhos e gladiadores armados com espadas.

A principal desvantagem do módulo NSCA, no entanto, é facilmente perceptível: o serviço é passivo. Em

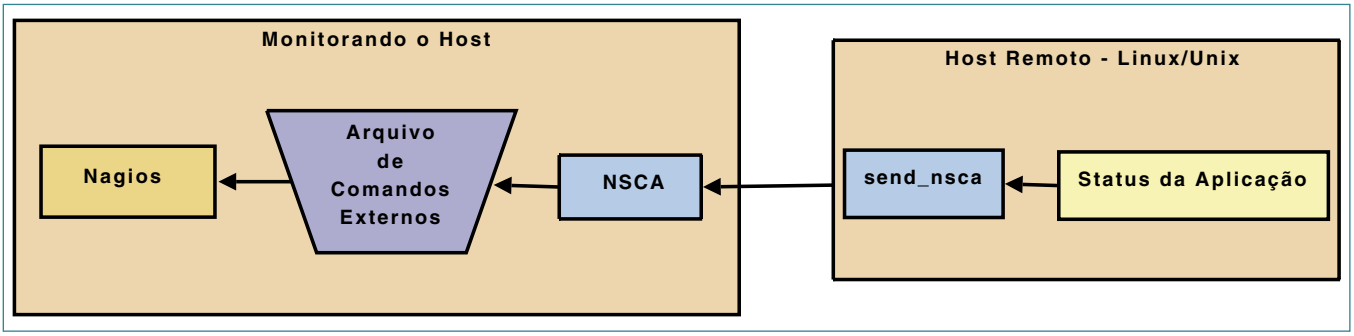


Figura 1 Arquitetura de verificações passivas do plugin NSCA do Nagios.

© Linux New Media do Brasil Editora Ltda.

outras palavras, uma eventual parada do sistema pode causar um maior tempo de *downtime*, pois suas checagens são executadas periodicamente.

Já o NRPE atua de maneira diferente: é um serviço ativo. O Nagios interage com a máquina remota e controla todas as checagens referentes aos serviços. Para isso, ele executa as verificações com o comando `check_nrpe`, que solicita à máquina remota que efetue as ações, finalizando assim o processo com o status do serviço (**figura 2**).

NRPE

O NRPE faz a comunicação entre o servidor e os agentes pela porta 5666 TCP por padrão, o que exige a liberação no firewall. O método de acesso pode ser caracterizado como direto (**figura 2**) ou indireto (**figura 3**). A forma indireta é aplicada quando o Nagios executa a monitoração de um servidor remoto e não consegue acesso aos demais servidores quando estão no mesmo segmento de rede. Nesse caso, a máquina que está sendo monitorada atua como um "proxy" para que o Nagios consiga chegar aos demais servidores que devem ser gerenciados.

Exemplo 1: Compilação e instalação completa do Nagios

```
01 # aptitude install openssl libssl-dev
02 # groupadd nagios
03 # useradd -g nagios nagios
04 # wget http://ufpr.dl.sourceforge.net/sourceforge/nagiosplug/
➥nagios-plugins-1.4.12.tar.gz
05 # tar xzf nagios-plugins-1.4.12.tar.gz
06 # cd nagios-plugins-1.4.12
07 # ./configure && make && make install
08 # chown -R nagios: /usr/local/nagios
```

Exemplo 2: Download e instalação do NRPE

```
01 # wget http://ufpr.dl.sourceforge.net/sourceforge/nagios/
➥nrpe-2.8.tar.gz
02 # tar xzf nrpe-2.8.tar.gz
03 # cd nrpe-2.8
04 # ./configure && make all
05 # make install-plugin
06 # make install-daemon
07 # make install-daemon-config
```

Este tutorial utiliza como base o método direto.

Mão na massa: agente

Compilar os plugins do Nagios e instalar o plugin `check_nrpe` são alguns dos pré-requisitos para o funcionamento do serviço na estação remota.

Como de costume, aplicações que dependem do envio de informações pela Internet normalmente usam algum tipo de tunelamento para garantir a privacidade e a in-

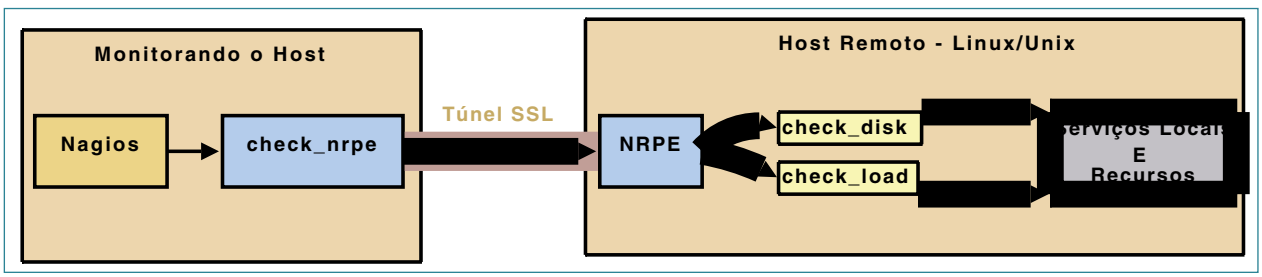


Figura 2 Arquitetura de verificações ativas do plugin NRPE do Nagios.

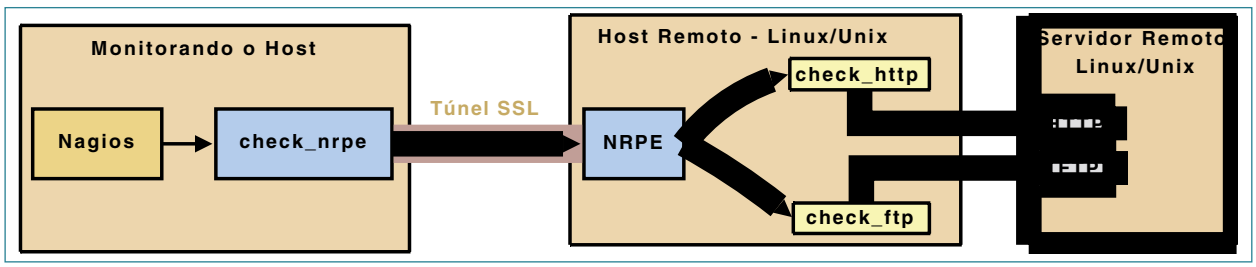


Figura 3 Esquema de acesso indireto pelo plugin NRPE.

© Linux New Media do Brasil Editora Ltda.

Snow666

Exemplo 3: Teste de funcionamento do NRPE

```
01 # /usr/local/nagios/bin/nrpe -c /usr/local/nagios/etc/nrpe.cfg -d
02 # /usr/local/nagios/libexec/check_nrpe -H localhost
```

Exemplo 4: Comandos para o check_nrpe

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

tegridade de seus dados. O NRPE não é diferente, e por isso requer a instalação do pacote *OpenSSL* e dos cabeçalhos SSL para concretizar o túnel criptografado entre cliente e servidor, como mostra o **exemplo 1**. Após a instalação dos pacotes num sistema *Debian* (**linha 1**), criamos o grupo e o usuário para o Nagios (**linhas 2 e 3**), baixamos o código-fonte do Nagios (**linha 4**), que então é descompactado, compilado e instalado (**linhas 5 a 7**). Por último, definimos o usuário dono dos arquivos do Nagios (**linha 8**).

A instalação do plugin NRPE é ainda mais fácil, pois não requer a criação de usuários e grupos, como mostra o **exemplo 2**. No entanto, a instalação dos componentes do NRPE é feita em três etapas: plugin (**linha 5**), daemon ou agente (**linha 6**) e arquivos de configuração (**linha 7**).

Para nos certificarmos de que ocorreu tudo certo, vamos fazer um pequeno teste para estabelecer a primeira comunicação com o daemon (**exemplo 3**). A **linha 1** executa o NRPE usando como arquivo de configuração o `nrpe.cfg` em `/usr/local/nagios/etc/` e operando no modo daemon (opção `-d`). A **linha 2** executa um teste, que consiste em rodar o plugin `check_nrpe` na máquina local (`-H localhost`).

Caso apareça na tela algo como `NRPE v2.8`, significa que a comunicação entre o plugin e o daemon do serviço funcionou.

No arquivo de configuração do NRPE (`/usr/local/nagios/etc/nrpe.cfg`, em nossa instalação) é preciso definir um endereço IP que terá permissão para executar os comandos e obter informações sobre os status dos seus serviços. Para isso, edite o arquivo `nrpe.cfg`, comente a linha `server_address` e acrescente o endereço IP do servidor Nagios ou uma faixa de endereços na linha `allowed_hosts`.

A máquina remota já está pronta para ser gerenciada pelo Nagios. Antes de tudo, acrescente ao arquivo `/etc/rc.local` a linha que inicia o módulo NRPE para que ele seja executado a cada inicialização:

```
/usr/local/nagios/bin/nrpe -c /
➥usr/local/nagios/etc/nrpe.cfg -d
```

Mão na massa: servidor

A configuração no servidor Nagios é ainda mais simples que a do agente. Basta instalar o plugin *check_nrpe* e ajustar os arquivos de configuração para o gerenciamento dos equipamentos. Novamente as **linhas 1 a 4** do **exemplo 2** mostram como baixar, compilar e instalar o NRPE. Porém, somente o plugin precisa ser instalado agora, o que significa que o próximo comando deve ser:

```
make install-plugin
```

Feito isso, o plugin já estará instalado no servidor Nagios. Portanto, vamos fazer um novo teste de comunicação, dessa vez entre o servidor e a máquina cliente:

```
# /usr/local/nagios/libexec/check_
➥nrpe -H ip_da_máquina_cliente
```

A saída do comando resultará novamente em algo parecido com `NRPE v2.8` caso a comunicação tenha funcionado.

Confirmado o sucesso, temos que ajustar os arquivos de configuração do Nagios em `/usr/local/nagios/etc/objects/`. No arquivo `commands.cfg`, acrescente as linhas de acordo com o **exemplo 4** para permitir a execução do *check_nrpe* pelo servidor.

Em seguida, crie um novo arquivo de configuração chamado `nrpe.cfg` no mesmo diretório, com o conteúdo definido no **exemplo 5**. Acrescente ainda a seguinte linha ao arquivo `/usr/local/nagios/etc/nagios.cfg`:

Service Status Details For Host Group 'Linux'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Linux Server	/dev/sda4 Free Space	OK	08-06-2008 18:02:13	0d 0h 11m 47s	1/3	DISK OK - free space: /home 19488 MB (71% inode=99%
	CPU Load	OK	08-06-2008 18:03:28	0d 0h 10m 32s	1/3	OK - load average: 1.23, 0.63, 0.40
	Current Users	OK	08-06-2008 17:54:42	0d 0h 9m 18s	1/3	USERS OK - 4 users currently logged in
	Total Processes	OK	08-06-2008 17:55:57	0d 0h 8m 3s	1/3	PROCS OK: 129 processes
	Zombie Processes	OK	08-06-2008 17:56:39	0d 0h 7m 21s	1/3	PROCS OK: 1 process with STATE = Z

Figura 4 A interface web do Nagios indica que o plugin *check_nrpe* está em funcionamento no cliente.

© Linux New Media do Brasil Editora Ltda.

Exemplo 5: Arquivo nrpe.cfg do servidor

```
define host{
    use         linux-server
    host_name   Linux_Server
    alias       Servidor Linux
    address     ip_da_máquina_a_ser_monitorada
}

define hostgroup{
    hostgroup_name  Linux
    alias           Servidores Remotos
    members         Linux_Server
}

define service{
    use                     generic-service
    host_name               Linux_Server
    service_description     Current Users
    check_command           check_nrpe!check_users
}

define service{
    use                     generic-service
    host_name               Linux_Server
    service_description     CPU Load
    check_command           check_nrpe!check_load
}

define service{
    use                     generic-service
    host_name               Linux_Server
    service_description     /dev/hda1 Free Space
    check_command           check_nrpe!check_hda1
}

define service{
    use                     generic-service
    host_name               Linux_Server
    service_description     Total Processes
    check_command           check_nrpe!check_total_procs
}

define service{
    use                     generic-service
    host_name               Linux_Server
    service_description     Zombie Processes
    check_command           check_nrpe!check_zombie_procs
}
```

```
cfg_file=/usr/local/nagios/etc/
➥objects/nrpe.cfg
```

Finalmente, reinicie o Nagios para aceitar as novas configurações. Com isso, já será possível acessar a interface web do Nagios e verificar que ele já está interagindo diretamente com seu servidor Linux (**figura 4**).

Demais Considerações

Como podemos notar, a configuração do módulo NRPE é simples, feita em um único arquivo (`nrpe.cfg`). Nele são acopladas as chamadas dos comandos, enquanto o plugin *check_nrpe* se encarrega de executá-los nas máquinas remotas e retornar o status de cada execução.

É possível obter maiores detalhes das máquinas remotas servidor por meio da gama de plugins existentes no pacote do próprio *nagios-plugins*, que estão localizados no diretório `/usr/local/nagios/libexec`. Se necessário, pode-se visitar o site oficial do Nagios [1] para encontrar outros plugins, ou o site Nagios Exchange [3] para plugins desenvolvidos por terceiros. ■

Sobre o autor

Vinicius Andrade Marino trabalha em uma empresa de consultoria, sendo o responsável por servidores e infra-estrutura de rede dos clientes. Ele estuda Tecnologia em Redes de Computadores e usa Linux desde 2004. (vinicius777@gmail.com)

Mais informações

[1] Nagios: http://www.nagios.org/

[2] Snort: http://www.snort.org/

[3] Nagios Exchange: http://www.nagiosexchange.com/

© Linux New Media do Brasil Editora Ltda.

Defina até onde um serviço pode ir

Regras de conduta

POSIX Capabilities é um recurso do kernel que permite limitar o que cada serviço pode fazer, reduzindo as conseqüências de um ataque.

por Marlon Luis Petry

O superusuário *root* pode realizar qualquer operação sem restrições, o que muitas vezes é mais que o necessário para executar um serviço. Isso é preocupante se lembrarmos que todos os dias novos *bugs* são encontrados e novos *exploits* são desenvolvidos, possibilitando um ataque do tipo *buffer-overflow* nesses serviços.

Um dos modos para minimizar os efeitos de ataques desse tipo, nos quais o atacante pode conseguir abrir uma sessão do shell, é executar os serviços utilizando um usuário sem privilégios de administrador. Dessa forma, o acesso conseguido usando determinada falha terá alcance restrito aos privilégios do serviço em questão.

A partir da versão 2.1 do Kernel, surgiu o conceito de "capacidades", ou *POSIX capability*, cujo princípio é dividir os privilégios do root em um conjunto de capacidades [1], cobrindo todos os privilégios do super usuário. Por exemplo, quando vamos alterar a hora do sistema, é necessária a capacidade `CAP_SYS_TIME`. Atribuindo essa capacidade ao comando `date`, qualquer usuário poderá alterar a hora do sistema. Esse recurso entrou no Kernel oficial a partir da versão 2.6.24rc2.

Pré-Requisitos

Para verificar se o kernel está compilado com suporte às POSIX capabilities, execute o comando `zgrep '\(XATTR\|CAPA\)' /proc/config.gz` e verifique a sua saída:

```
CONFIG_EXT2_FS_XATTR=y
CONFIG_EXT3_FS_XATTR=y
CONFIG_EXT4DEV_FS_XATTR=y
CONFIG_REISERFS_FS_XATTR=y
# CONFIG_JFFS2_FS_XATTR is not set
CONFIG_CIFS_XATTR=y
CONFIG_SECURITY_CAPABILITIES=y
CONFIG_SECURITY_FILE_
➥CAPABILITIES=y
```

Caso o resultado seja diferente do mostrado, é necessário habilitar essas opções no kernel e recompilá-lo.

Também é necessário possuir a biblioteca *libcap2*, que pode ser baixada no endereço [2] e compilada da forma tradicional:

```
tar -xzf libcap-2.11.tar.gz
cd libcap-2.11
make
make install
```

Ou, se você for usuário da distribuição *Gentoo*:

```
emerge -av =sys-libs/libcap-2.11
```

Privilégios mínimos

Normalmente, o comando `ping` necessita estar com o bit *SUID* habilitado, tendo como dono o usuário root para que um usuário comum consiga executar o comando. Então, vamos remover o bit SUID e colocar a capacidade mínima necessária para executar o comando.

```
chmod u-s /bin/ping
```

```
ping 127.0.0.1
ping: icmp open socket: Operation
➥not permitted
```

Como podemos verificar, removendo o bit SUID do ping, um usuário comum não pode executá-lo. Para tornar a execução possível, atribuiremos a capacidade *CAP_NET_RAW* ao comando `ping`. Essa capacidade permite que um usuário comum abra conexões de rede do tipo *raw* (bruto):

```
setcap cap_net_raw=ep /bin/ping
```

Agora conseguimos executar o comando `ping` com usuário comum sem que o comando esteja com o SUID habilitado:

```
ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84)
➥bytes of data.
64 bytes from 127.0.0.1: icmp_
➥seq=1 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_
➥seq=2 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_
➥seq=3 ttl=64 time=0.035 ms
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received,
➥0% packet loss, time 1998ms rtt
➥min/avg/max/mdev =
0.033/0.033/0.035/0.006 ms
```

Para verificar quais capacidades estão definidas, basta utilizar o comando `getcap` como segue:

```
getcap /bin/ping
```


© Linux New Media do Brasil Editora Ltda.

```
/bin/ping = cap_net_raw+ep
```

Necessidades

No artigo "*POSIX file capabilities: Parceling the power of root* "[3], o autor fornece o código-fonte de um módulo chamado `capable_probe`, que nos ajuda a descobrir as necessidades de cada processo. Sempre que houver uma chamada de sistema para a função `cap_capable()`, ele a intercepta e substitui pela função `cr_capable()`, que mostrará a capacidade exigida e qual processo a está requisitando.

Para utilizar esse módulo, use o comando `zgrep '\(PROBE\)' /proc/config.gz` para verificar a compatibilidade do kernel:

```
zgrep '\(PROBE\)' /proc/config.gz
CONFIG_GENERIC_IRQ_PROBE=y
CONFIG_KPROBES=y
CONFIG_KRETPROBES=y
CONFIG_HAVE_KPROBES=y
CONFIG_HAVE_KRETPROBES=y
# CONFIG_NET_DCCPPROBE is not set
# CONFIG_NET_TCPPROBE is not set
# CONFIG_MTD_JEDECPROBE is not set
CONFIG_KPROBES_SANITY_TEST=y
```

Verifique se as opções mostradas correspondem às mostradas. Em seguida, o módulo `capable_discovery` pode ser instalado da maneira tradicional:

```
tar -xjvf capable_discovery.tar.
➥bz2
cd capable_discovery
make
make install
```

Carregue o módulo com o comando `modprobe capable_discovery`. As mensagens mostradas pelo módulo ao usar o `ping` podem ser monitoradas utilizando o comando `tail -f /var/log/messages | grep ping`, que exibirá a saída:

```
Sep  1 21:35:23 localhost
➥capability 21=CAP_SYS_ADMIN for
➥ping
Sep  1 21:35:23 localhost
➥capability 13=CAP_NET_RAW
➥for ping
Sep  1 21:35:23 localhost
➥capability 7=CAP_SETUID for ping
```

No resultado acima podemos ver de quais capacidades o `ping` necessita:

- *21: CAP_SYS_ADMIN*: Não atribuir, corresponde à capacidade de administração do sistema.
- *13: CAP_NET_RAW*: Permite a comunicação de dados brutos pela rede.
- *7: CAP_SETUID*: Necessária para manipulação de arquivos.

Samba sem root

Antes de fazermos o samba rodar com um usuário comum, temos que descobrir quais são as capacidades exigidas pelo serviço. Para descobrir essas capacidades, usaremos novamente o módulo `capable_discovery`:

```
# modprobe capable_discovery
# tail -f /var/log/messages |grep
➥smbd
```

Em outro terminal, inicie o servidor Samba:

```
# smbd -d
```

No primeiro terminal, podemos verificar as capacidade exigidas pelo Samba:

```
Sep  3 13:59:51 localhost
➥capability 21=CAP_SYS_ADMIN for
➥smbd
Sep  3 13:59:51 localhost
➥capability 7=CAP_SETUID for smbd
Sep  3 13:59:52 localhost
➥capability 24=CAP_SYS_RESOURCE
➥for smbd
Sep  3 13:59:51 localhost
➥capability 6=CAP_SETGID for smbd
Sep  3 13:59:52 localhost
➥capability 10=CAP_NET_BIND_SERVICE
➥for smbd
```


© Linux New Media do Brasil Editora Ltda.

Snow666

PARTICIPE DO PRINCIPAL
EVENTO DE PHP DA AMÉRICA LATINA

php Conference Brasil 08

27, 28 e 29 de Novembro
UNIFIEO • OSASCO-SP

PALESTRANTES INTERNACIONAIS
PRESENÇAS CONFIRMADAS:

- Christopher Jones
  Desenvolvimento de Produto, Oracle
- Todd Trichler
  Gerente Sênior de Produto, Oracle Technology Network
- Luke Crouch
  Engenheiro de Software, Sourceforge.net

Diamond
Borland · LOCAWEB Serviços de Internet · msdn · ORACLE · ScriptCase · INGRAM MICRO · IBM Premier Business Partner

Silver | Hospedagem
dextra Coding your Business · HostNET

Apoio Institucional e Infra-Estrutura
Centro Universitário FIEO UNIFIEO

Apoio
DICAS-L www.dicas-l.com.br · br-linux.org Ano 10 · DINAMIZE · HTML STAFF

Mídia Oficial | Apoio Cultural
Linux Magazine · TEMPO REAL Livraria do Profissional de Informática

Promoção e Realização
TEMPO REAL Eventos

www.phpconf.com.br

Snow666

Repetimos o mesmo procedimento para verificar quais são os requisitos do `nmbd`, obtendo como resposta:

```
Sep  3 14:00:03 localhost
➥capability 21=CAP_SYS_ADMIN for
➥nmbd
Sep  3 14:00:03 localhost
➥capability 10=CAP_NET_BIND_
➥SERVICE
➥for nmbd
```

Por fim, o módulo pode ser descarregado com `rmmod capable_discovery`. É interessante remover o módulo logo após o uso, pois todos os processos que estão rodando sempre estão verificando as capacidades necessárias, haja vista que o módulo utiliza a função `printk` para mostrar as capacidades e isso causa um grande aumento dos arquivos de log.

Prosseguimos criando um usuário e grupo específicos para rodar o Samba:

```
# groupadd samba
# adduser samba -g samba
```

Há diretórios que pertencem ao Samba que também precisam ter dono e grupo alterados:

```
chown samba:samba -R /var/run/samba/
chown samba:samba -R /var/log/
➥samba/
chown samba:samba -R /etc/samba/
chown samba:samba -R /var/cache/
➥samba/
chown samba:samba -R /var/lib/
➥samba/
```

Para evitar que outros usuários possam tentar executar os comandos, alteramos dono e permissão de execução:

```
chown samba:samba /usr/sbin/nmbd
chown samba:samba /usr/sbin/smbd
chmod g-x,o-x /usr/sbin/smbd
chmod g-x,o-x /usr/sbin/nmbd
```

```
chmod u+s /usr/sbin/nmbd /usr/
➥sbin/smbd
ls -la /usr/sbin/*bd
-rwsr--r-- 1 samba samba 1061664
➥Mar 10 22:54 /usr/sbin/nmbd
-rwsr--r-- 1 samba samba 3633876
➥Mar 10 22:54 /usr/sbin/smbd
```

Finalmente, as capacidades necessárias são atribuídas:

```
setcap  cap_net_bind_service,cap_
➥sys_resource=ep /usr/sbin/smbd
setcap  cap_net_bind_service=ep /
➥usr/sbin/nmbd
```

Certifique-se de interromper o serviço e reinicie-o usando o usuário *samba*:

```
# su - samba
$ /usr/sbin/smbd -D
$ /usr/sbin/nmbd -D
```

O comando `ps -uax | grep samba` mostrará o serviços em execução com o usuário samba:

```
samba     9535  0.0  0.2   8876
➥2196 ?        Ss   15:30   0:00 /
➥usr/sbin/smbd -D
samba     9536  0.0  0.0   8876
➥948 ?         S    15:30   0:00 /
➥usr/sbin/smbd -D
```

Neste momento, o samba já funciona com usuário comum utilizando as capacidades que atribuímos aos binários do serviço.

Cada um no seu quadrado

As vantagens de rodar um serviço com alcance restrito são inegáveis, mas todo o procedimento de descobrir as capacidades mínimas e atribuí-las aos serviços não é tarefa das mais triviais. Porém, como toda inovação, não tardará a ser incorporada como recurso padrão nas distribuições mais populares. ■

Mais informações

[1] Lista Capacidades: http://www.gentoo.org/proj/en/hardened/capabilities.xml

[2] Download libcap2: http://ftp.kernel.org/pub/linux/libs/security/linux-privs/kernel-2.6/libcap-2.11.tar.gz

[3] Linux Capabilities: making them work. http://ols.fedoraproject.org/OLS/Reprints-2008/hallyn-reprint.pdf

[4] Módulo personalizado: http://petryx.blogrs.com.br/capable_discovery.tar.bz2

[5] POSIX File Capabilities: http://www.friedhoff.org/posixfilecapsold.html

[6] Introduction to Linux Capabilities and ACL's: http://www.securityfocus.com/infocus/1400

[7] Secure programmer: Minimizing privileges: http://www.ibm.com/developerworks/linux/library/l-sppriv.html

[8] Linux kernel capabilities FAQ: ftp://ftp.kernel.org/pub/linux/libs/security/linux-privs/kernel-2.4/capfaq-0.2.txt

[9] POSIX file capabilities: Parceling the power of root: http://www.ibm.com/developerworks/library/l-posixcap.html

Sobre o autor

Marlon Luis Petry é bacharel em Ciência da Computação graduado pela Unicruz e trabalha com servidores Linux e consultoria para pequenos provedores de Internet, além de manter o blog http://petryx.blogrs.com.br

© Linux New Media do Brasil Editora Ltda.

Servidores virtuais com Server Name Indication

Entrega garantida

Lieferung_malen

A Server Name Indication permite a operação de mais de um serviço protegido por SSL em cada endereço IP.

por Thorsten Fischer

Internautas e programadores web são igualmente devotados ao objetivo de evitar que agressores capturem compras online, obtenham números de cartão de crédito e arrasem contas de usuários. Felizmente, a introdução da *Secure Socket Layer* (SSL[1]), um protocolo para transmissão de dados criptografados e identificação confiável, ajuda a evitar esse cenário de terror por meio da oferta de um meio de proteção para atividades sensíveis, como o acesso a bancos pela Internet.

O protocolo HTTPS integra o SSL ao HTTP para promover a comunicação segura pela Web. Usando parâmetros de criptografia negociados com uso do nome DNS do servidor, o HTTPS estabelece uma conexão segura.

Essa técnica funciona muito bem quando apenas um nome DNS está associado ao endereço IP; porém, cria um problema para qualquer um que deseje usar servidores virtuais com nomes diferentes num único endereço.

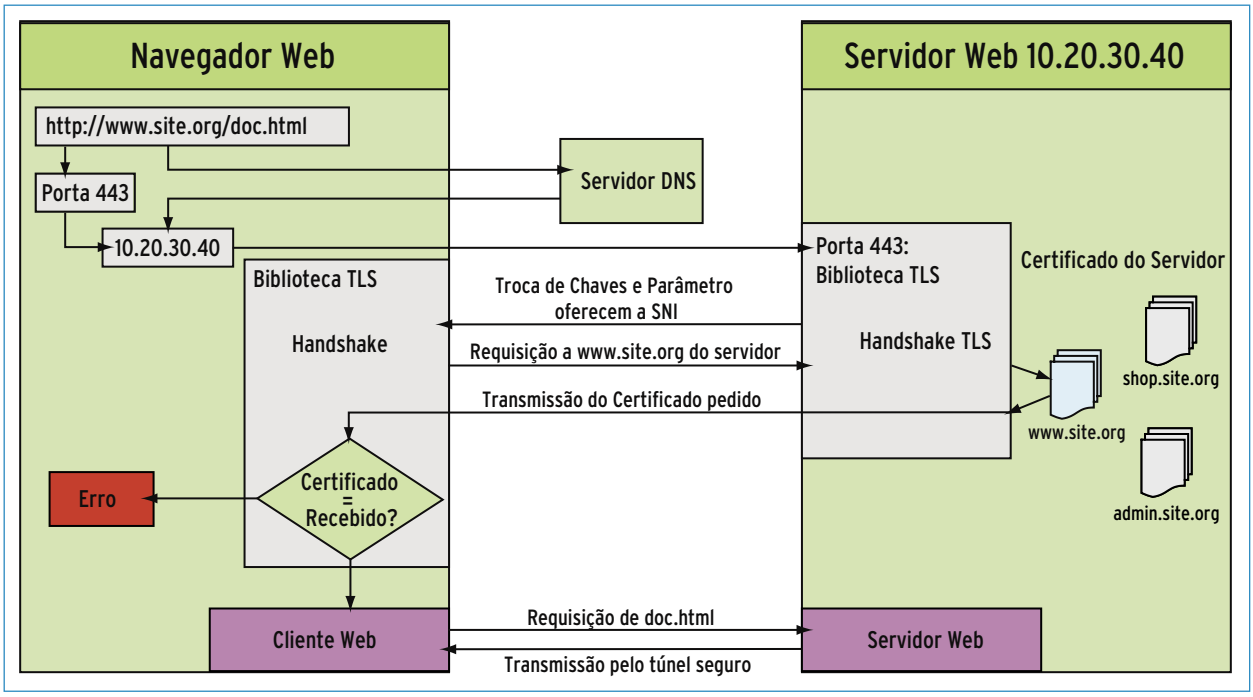


Figura 1 São necessárias várias etapas entre digitar uma URL no navegador e transmitir conteúdo web de forma segura. O cliente usa um servidor DNS para encontrar o endereço IP do nome na URL. O cliente recebe o certificado do endereço IP como parte da sessão SSL. Somente se o certificado for válido e o nome corresponder àquele que consta na requisição a SSL começará a transmitir o conteúdo.

© Linux New Media do Brasil Editora Ltda.

O cliente contacta o servidor SSL por meio do endereço IP especificado e anuncia que deseja criptografar o tráfego. O servidor confirma a requisição, apresenta um certificado e propõe uma combinação de algoritmos suportados tanto por ele quanto pelo cliente. Se as opções agradarem ao cliente, ele aceita o certificado. Os parceiros fzem todas as requisições HTTP posteriores pelo canal criptografado (**figura 1**).

Um dos parâmetros geralmente transmitidos com o certificado é o nome DNS do site, que é acrescentado ao campo `CommonName`. Certificados X.509v3 incluem essas informações no atributo `CN:`. Após receber o certificado, o cliente envia a requisição HTTP. A requisição também contém o nome do servidor ao qual ela é endereçada. Isso significa que se múltiplos sites usarem o mesmo endereço IP, o único que poderá usar comunicações seguras é aquele cujo nome está no certificado.

O cliente não é o único elemento que pode causar confusão por causa de uma requisição ambígua. Por exemplo, se o provedor tiver múltiplos serviços HTTPS num único endereço IP, o servidor também tem um sério problema: depois de estabelecer a conexão segura, o servidor precisa identificar qual chave privada usar para processar a requisição criptografada do cliente.

Para isso, o servidor precisa avaliar o cabeçalho `Host:` da requisição HTTP. É claro que a requisição – incluindo o cabeçalho – é criptografada até o servidor determinar qual chave privada usar.

A recente ênfase na computação virtual e a necessidade de serviços de hospedagem e outros de conservarem seus endereços IP tornaram esse problema urgente. Felizmente, o sucessor do SSL da Internet Engineering Task Force (IETF), o protocolo TLS (*Transport Layer Security*) oferece uma solução por meio da extensão SNI (*Server Name Indication*), descrita na RFC 4366.

Para resolver o problema de operar múltiplos servidores virtuais num único endereço IP, os clientes precisam da possibilidade de especificar o nome com o qual desejam se comunicar no momento em que a conexão SSL é estabelecida.

A SSL convencional não oferece essa opção, mas a extensão SNI suporta a transmissão de mais dados na fase do *handshake* [2]. Para ser mais preciso, um campo opcional pode ser transmitido na etapa `ClientHello` do TLS. O cliente pode usar esse campo para especificar o nome do parceiro com quem quer se comunicar. Depois, quando o servidor transmite o certificado correto na próxima etapa, o cliente sabe qual chave privada usar para o restante da comunicação (veja a **figura 2**).

Para o SNI funcionar, tanto o cliente quanto o servidor precisam suportar esse método. O **quadro 1** resume o suporte oferecido atualmente pelas bibliotecas *Gnutls*, *OpenSSL* e *NSS* (*Network Security Services*).

Em sua maior parte, a SNI é transparente para o usuário. A **tabela 1** mostra um panorama dos clientes e servidores suportados. O Opera foi o primeiro navegador a suportar essa extensão, já na versão 8.0, e o Firefox o fez na versão 2.0. Ambos precisam que o usuário ative a TLS explicitamente, mas a maioria dos especialistas em segurança recomenda o uso dessa configuração de qualquer forma.

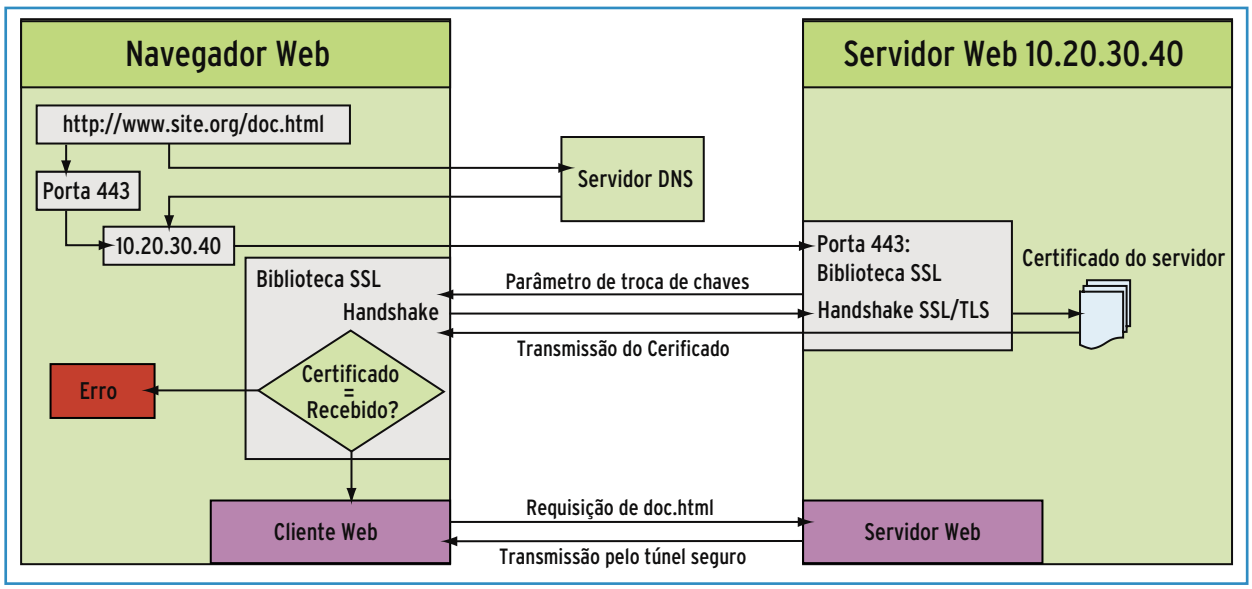


Figura 2 A Server Name Indication (SNI) se baseia na extensão Transport Layer Security (TLS). O cliente passa o nome do servidor requerido na fase do handshake para que o servidor consiga responder com um certificado correspondente.

© Linux New Media do Brasil Editora Ltda.

Tabela 1: Programas suportados

Programa	Papel	Versão	Comentário
Apache	Servidor	2.0.55 e 2.2	Há módulos tanto para *mod_gnutls* quanto *mod_openssl*. Os desenvolvedores do Apache oferecem patches.
Lighttpd	Servidor	1.4.18 e 1.5	Requer um patch que depende da OpenSSL[4].
Firefox	Cliente	2.0	TLS precisa estar ativada.
Opera	Cliente	8.0	TLS 1.1 precisa estar ativada.
Internet Explorer	Cliente	7.0 beta 2	Somente no Windows Vista; não no Windows XP.
Konqueror	Cliente	3.5.1	Requer OpenSSL 0.9.8f; veja o bug do KDE #122433.

Quadro 1: Extensões da biblioteca TLS

Para usar a SNI, é necessário suporte por parte da biblioteca. Três alternativas populares com suporte a SNI incluem a GnuTLS da Free Software Foundation, a NSS do projeto Mozilla e a amplamente utilizada OpenSSL.

A versão 0.5.10 da Gnutls introduziu suporte à SNI em 2002, sob a forma de funções separadas para cliente e servidor. Para o desenvolvedor, basta chamar no cliente `gnutls_server_name_set()` e no servidor `gnutls_server_name_get()` para escrever aplicações compatíveis com SNI. Isso explica por que o módulo *mod_gnutls* do Apache consegue usar SNI.

A OpenSSL introduziu suporte à SNI apenas recentemente, na versão 0.9.8f das extensões TLS. Macros como `SSL_set_tlsext_host_name()` e funções como `SSL_get_servename()` estão disponíveis. O módulo do Apache *mod_ssl* também é capaz de usar SNI.

A biblioteca NSS, usada pelo Firefox, não é tão avançada. A NSS 3.11.1 suporte a SNI no cliente, mas não a parte do servidor. Os planos do projeto afirmam explicitamente que a versão 3.12 não suportará SNI.

A versão 7.0 e posteriores do Internet Explorer também suportam a SNI, mas somente no Vista, não no Windows XP. Para testar as capacidades SNI do navegador, basta visitar a página de teste da SNI em [3].

Segurança importa

A SNI oferece muitos benefícios para ambientes de servidores virtuais, mas assim como qualquer ferramenta poderosa, é importante agir com cuidado.

Em testes de segurança de servidores web, é importante ter em mente que uma configuração incorreta pode fornecer vários vetores de ataque. Por exemplo, um agressor poderia usar a extensão SNI para adivinhar nomes genéricos de servidores virtuais escondidos por trás do IP compartilhado.

Se o servidor web receber uma requisição com o cabeçalho `Host:` modificado (por exemplo, definido como `intranet`), ele pode servir o conteúdo desse site. O método `CONNECT` do HTTP às vezes também pode ser enganado de uma forma parecida para estabelecer conexões proxy internas ilegítimas.

A SNI obviamente não publica deliberadamente documentos sobre redes inseguras, mas dá aos administradores outra oportunidade de cometer erros de configuração. Afinal, espera-se que o servidor web lide com requisições de conteúdo de sites com nomes diferentes.

Conclusão

A SNI resolve um problema que a comunidade de desenvolvedores vem enfrentando sozinha em virtude de seu rápido crescimento. Uma extensão do padrão TLS agora oferece aos administradores de sites a possibilidade de unir múltiplos certificados num único endereço IP. Esse pré-requisito é importante para se executar múltiplos servidores virtuais seguros num único IP.

Os provedores podem economizar dinheiro e recursos com isso, mas os administradores precisam ter cautela ao oferecerem múltiplos servidores web numa única instância de sistema operacional. ■

Mais informações

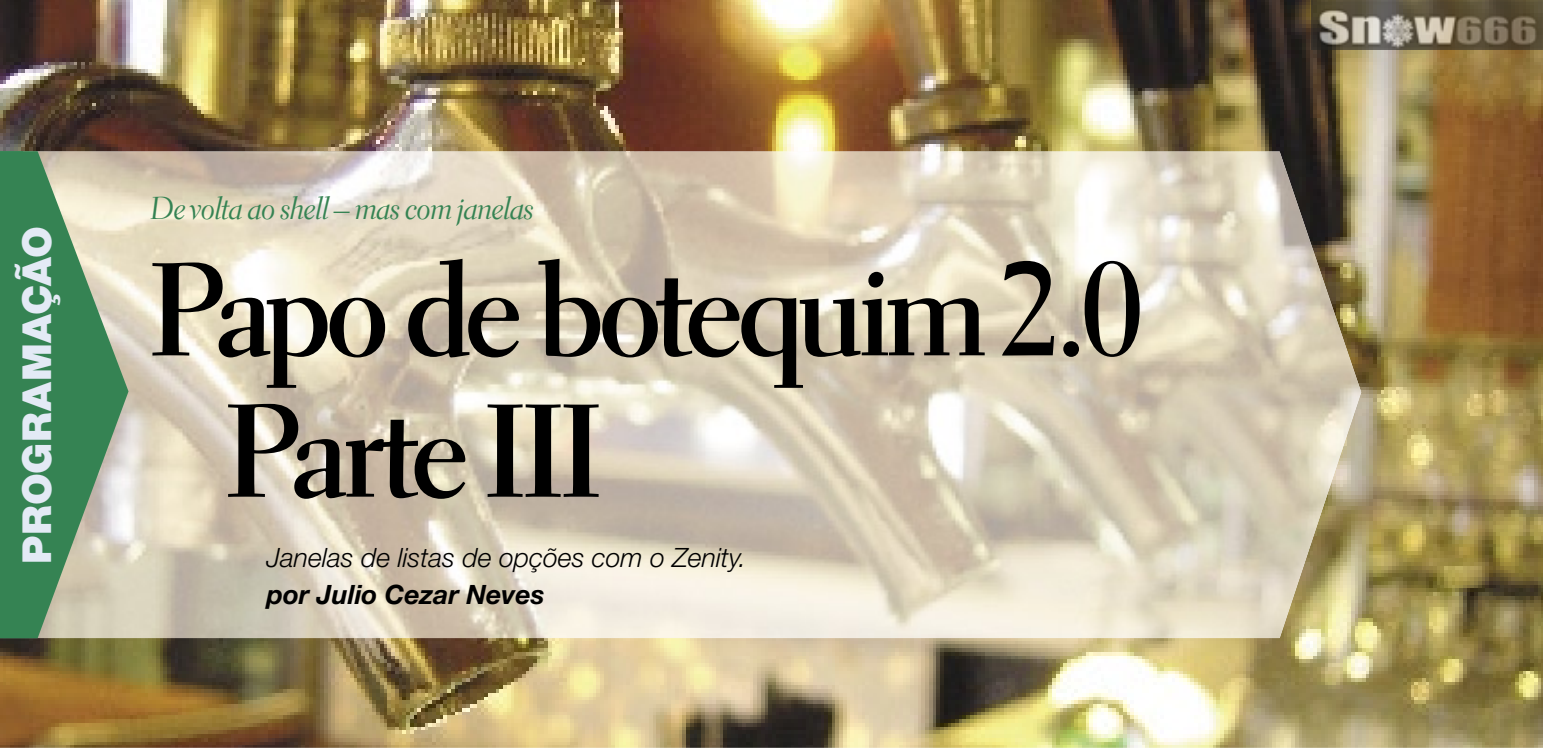
[1] SSL versão 3.0: http://wp.netscape.com/eng/ssl3/draft302.txt

[2] RFC 4366, "Transport Layer Security (TLS) Extensions" (em inglês): http://www.ietf.org/rfc/rfc4366.txt

[3] Site de teste da SNI: https://sni.velox.ch

[4] Patch para SNI no Lighttpd: http://trac.lighttpd.net/trac/ticket/386

© Linux New Media do Brasil Editora Ltda.



De volta ao shell – mas com janelas

Papo de botequim 2.0 Parte III

Janelas de listas de opções com o Zenity.

por Julio Cezar Neves

– Bem, meu amigo "shelleiro". Você fez o exercício que te passei?

– Fiz, mas não sei se está certo. Primeiro fiz de uma forma e depois achei que você tinha posto uma casca de banana para eu escorregar e refiz. O **exemplo 1** mostra como ficou a minha versão final.

Primeiramente, fiz um *loop* de `while` com duas saídas: ou ele sai no `break` caso tenha informado um diretório correto ou encerra o programa no `exit 1` após ter escolhido abandonar na opção `--question` que coloquei.

Em seguida, troco o `IFS` (*Inter Field Separator*), que é o separador do Bash, para que o `for` pegue cada um dos arquivos selecionados. Me lembrei que você disse que o separador padrão era uma barra vertical (`|`) e usei esse macete do Shell. Dentro deste *loop* é que encontrei a pegadinha que você deixou: primeiro pensei que você quisesse que usasse a opção `--confirm-overwrite`, mas isso só seria válido se estivesse escolhendo o caminho completo do arquivo destino. Como estávamos escolhendo os arquivos a serem movidos, tive de fazer uma ginástica (`ls $DirDest | grep $(basename $Arq) > /dev/null`) para ver se cada um dos arquivos selecionados não existia no diretório destino. Era isso mesmo?

– Era, e o exercício ficou muito legal. Vamos pedir os chopes de praxe e aprender a usar a opção `--list` na sua plenitude.

Chico, dois chopes, um sem colarinho!

Hoje falaremos da opção `--list` (**tabela 1**) que, como o nome diz, gera no `zenity` listas de todas as formas, como:

- Listas propriamente ditas;
- Listas de *radio buttons*;
- Listas em *Check Lists*.

Esta opção lhe oferece uma lista para a escolha de um ou mais de seus componentes. Divide-se em três tipos: listas propriamente ditas, *radio list* e *check list*.

Tabela 1: Opção --list

Opção	Efeito
`--text=TEXTO`	Define o texto da caixa.
`--column=TEXTO`	Define os cabeçalhos das colunas (um para cada coluna).
`--checklist`	Coloca *check boxes* na 1ª coluna.
`--radiolist`	Coloca *radio boxes* na 1ª coluna.
`--multiple`	Permite a seleção de diversas linhas.
`--separator=SEPARADOR`	Usado com `--multiple`, especifica o separador quando retornar mais de uma linha.
`--editable`	Permite editar os itens exibidos.
`--print-column=TEXTO`	Especifica qual coluna mandar para a saída primária. O retorno *default* é a 1ª. `ALL` pode ser usado para imprimir todas.
`--hide-column=INT`	Omite a coluna definida por `INT`.

Listas

Vejamos primeiramente o **exemplo 2** de utilização de lista. O resultado é mostrado na **figura 1**.

Mas isso ainda está muito simples. No **exemplo 3** vamos complicar um pouco mais.

© Linux New Media do Brasil Editora Ltda.

Exemplo 1: Exercício da última aula

```
01 #!/bin/bash
02 # Movendo arquivos a partir do diretorio corrente
03 # Escolha do diretorio destino
04 while true
05 do
06     DirDest=$(zenity --file-selection        \
07         --directory                          \
08         --title "Escolha o diretorio de destino")
➥ && break
09     zenity --question                        \
10         --title "Falta diretorio de destino" \
11         --text "Diretorio destino nao informado:
12         - Clique OK para finalizar;
13         - Clique CANCELAR para escolher diretorio
➥ destino" && exit 1
14 done
15 # Escolha dos arquivos
16 Arqs=$(zenity --file-selection                \
17     --title "Escolha arquivos para mover para
➥$DirDest" \
18     --multiple) || {
19         echo Nao foram escolhidos arquivos
20         exit 1
21         }
22 #  Verifica se os arquivos já existem no
23 #+ diretório de destino e move um por um
24 IFS='|'  # A barra (|) é o separador default do
➥ --file-selection
25 for Arq in $Arqs
26 do
27     ls  $DirDest | grep $(basename $Arq) >
➥ /dev/null || {
28         mv $Arq $DirDest
29         continue
30         }
31     zenity --question                \
32         --title "Arquivo ja existe" \
33         --text "Ja existe $(basename $Arq)
➥em $DirDest
34         - Clique em OK para sobregravar ou;
35         - Clique em CANCELAR para desistir"
➥ && mv $Arq $DirDest
36 done
```

Exemplo 2: Lista simples

```
01 until Escolha=$(zenity --list \
02     --column Ímpares          \
03     --column Pares            \
04         1 2                   \
05         3 4                   \
06         5 6                   \
07         7 8)
08 do
09     zenity --error             \
10         --title "Par ou Ímpar" \
11         --text "Escolha uma dupla"
12 done
```

Este é um exemplo ainda bem simples, sem cabeçalho (`--title`) e sem texto explicativo (`--text`). Especifiquei duas colunas (`LoginName` e `UID`) e peguei estes dois campos do `/etc/passwd`, trocando os dois-pontos (`:`) por espaço em branco, para servir como separador de campos do `zenity` (também poderia ter usado `<TAB>`).

Figura 1 Nesse exemplo, se o cara clicar em CANCELAR ou simplesmente fechar a janela da lista, será dada uma mensagem de erro.

O **exemplo 4** mostra como deixar essa lista mais bonita:

Como mostra a **figura 2**, agora a lista tem cabeçalho (`--title`) e texto explicativo (`--text`). Tá ficando bom! Mas, peraí, e se eu quiser escolher mais de um? Assim como na seleção de arquivos (`--file-selection`), as listas também permitem mais de uma escolha, e é para isso que serve a opção `--multiple` (**exemplo 5**). O resultado é mostrado na **figura 3**.

Quando usamos esse recurso, é legal que ele venha acompanhado de `--separator` (**exemplo 6**) para especificar qual será o caractere que servirá como separador entre as respostas recebidas. Se não usarmos essa opção, as nossas escolhas virão separadas por barras verticais (`|`).

Um último exemplo bastante interessante. Veja esse arquivo incompleto de UFs:

```
$ cat UFs
MG
PA
RJ
SP
```

O **exemplo 7** mostra uma forma de capturar uma UF da tela e, ao mesmo tempo, incrementar esse arquivo:

Nesse momento, se você der um duplo clique em *Nova UF* (que será

© Linux New Media do Brasil Editora Ltda.

o primeiro item da lista, como mostra a **figura 4**), e escrever, por exemplo, `SC`, a variável `$UF` receberá esse valor. O que permite isso é a opção `--editable`. O mesmo pode ser feito (e acho até que de forma mais amigável e óbvia) usando a opção `--entry`, sob a forma de *ComboBox*.

Exemplo 3: Opções extraídas de arquivo

```
01 zenity --list \
02     --column LoginName \
03     --column UID \
04     $(cut -f1, 3 -d: /etc/passwd | tr : ' ')
```

Exemplo 4: Usando as opções --title e --text

```
01 zenity --list                                  \
02     --title "Usuários Cadastrados"             \
03     --text "Selecione o usuário desejado"      \
04     --height 300                               \
05     --column LoginName                         \
06     --column UID                               \
07         $(cut -f1,3 -d: /etc/passwd | tr : ' ')
```

Exemplo 5: Usando a opção --multiple

```
01 SO=$(zenity --list \
02     --title "Sistemas Operacionais" \
03     --text "Quais podemos chamar de sistemas
➥operacionais?" \
04     --height 230 \
05     --multiple \
06     --column "Sistema Operacional" \
07         "M$ Vista" \
08         "M$ XP" \
09         Linux \
10         Unix)
11 echo $SO
12 Linux|Unix
```

Exemplo 6: Podemos determinar o separador para as respostas dadas com a opção --separator

```
01 SO=$(zenity --list
02     --title "Sistemas Operacionais" \
03     --text "Quais podemos chamar de sistemas
➥sistemas operacionais?" \
04     --height 230 \
05     --multiple \
06     --separator ^ \
07     --column "Sistema Operacional" \
08         "M$ Vista" \
09         "M$ XP" \
10         Linux \
11         Unix)
12 echo $SO
13 Linux^Unix
```

O **exemplo 8** mostra como testar se o valor informado já existia no arquivo `UFs` e em seguida atualizá-lo.

A opção `-q` (*quiet*) do `grep` serve para que ele não mande a saída para a tela, caso a UF informada tenha sido encontrada no arquivo `UFs`.

Radio Lists

A múltipla escolha não é possível se a lista for uma *radio list*. A **tabela 2** mostra algumas opções para esse tipo de diálogo.

Algumas vezes não exibimos uma coluna, mas queremos seu valor como retorno. O **exemplo 9** mostra uma escolha de resoluções de telas (**figura 5**).

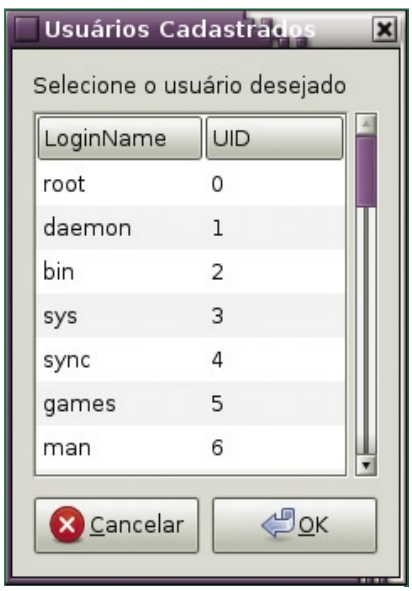


Figura 2 Janela de opções com título e informação personalizados.

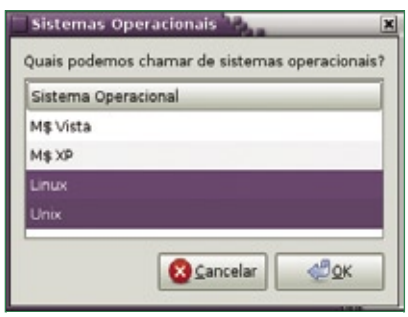


Figura 3 Escolha de múltiplas opções.

© Linux New Media do Brasil Editora Ltda.

Exemplo 7: A opção --editable

```
01 UF=$(zenity --list                                    \
02      --editable                                       \
03      --title="UFs"                                    \
04      --text "Pegue uma UF ou escolha uma nova" \
05      --column="UFs" "Nova UF" $(cat UFs))
```

Tabela 2: Opções do tipo radio

A opção	Define
`--radiolist`	Uma lista com botões de rádio
`--column`	Os cabeçalhos das colunas
`TRUE ou true`	Um botão inicialmente marcado
`FALSE ou false`	Um botão inicialmente desmarcado

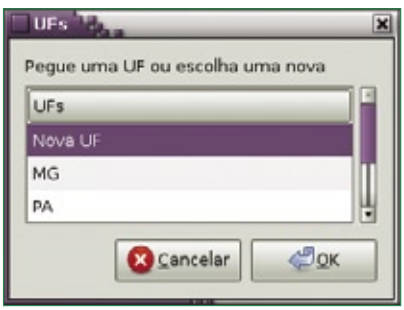


Figura 4 Inclusão de opção na lista.

Nesse exemplo, você deve ter notado que existem três colunas, mas a segunda foi colocada somente para facilitar a programação posterior. Assim sendo, ela não deveria ser exibida e para isso usamos a opção `--hide-column`.

Vimos ainda que a segunda coluna é o valor retornado por padrão. Isso pode ser alterado com a opção `--print-column`, como mostrado no **exemplo 10**.

Quando escolhi o melhor sistema operacional (**figura 6**), se não tivesse usado a opção `--print-column=3`, a variável `$SO` teria recebido `Comunidade`, que por ser a segunda coluna é a padrão. Graças a essa opção, a variável recebeu "Linux".

Caso tivesse especificado `--print-column 2,3`, a resposta obtida seria `Comunidade|Linux`.

Check Lists

Nas *check lists* é comum termos mais de uma opção e por isso é desnecessário usarmos `--multiple`. Nesse caso, o uso de `--separator` é encorajado (**exemplo 11**).

A **figura 7** mostra o diálogo mais básico obtido com a opção `--checklist`. O **exemplo 12** é um pouco mais completo e complexo e mostra a janela da **figura 8**.

Como o `-o` é a condição *ou* do comando `find`, a saída já está prontinha para usar como `find . -type f $Usus`.

Após a substituição de variáveis feita pelo *Shell*, o comando executado será `find . -type f -user root -o -user julio`.

Vamos analisar o **exemplo 12**:

O primeiro comando `cut -f1,3 -d: /etc/passwd` retira o primeiro e o terceiro campos `login` e `UID`, separados por dois-pontos `:` de todos os usuários registrados em `/etc/passwd`. Após esse comando, a primeira linha recebida de `/etc/passwd` ficaria `root:0`.

Exemplo 8: Incrementar o arquivo com a opção fornecida

```
01 grep -q "^$UF" UFs ||
02      {
03      echo $UF >> UFs
04      sort UFs -o UFs
05      }
```

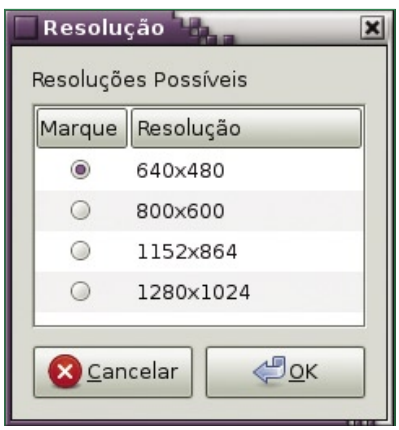


Figura 5 Lista de opções usando o tipo *radio*.

Exemplo 9: Escolha de resolução de tela

```
01 Resolucao=$(zenity --list          \
02      --height 230                  \
03      --title "Resolução"           \
04      --text "Resoluções Possíveis" \
05      --radiolist                   \
06      --hide-column 2               \
07      --column "Marque"             \
08      --column ""                   \
09      --column "Resolução"          \
10          TRUE  0 "640x480"         \
11          FALSE 1 "800x600"         \
12          FALSE 2 "1152x864"        \
13          FALSE 3 "1280x1024")
```


© Linux New Media do Brasil Editora Ltda.

Exemplo 10: Utilização da opção --print-column

```
01 SO=$(zenity --list \
02      --title "Sistemas Operacionais"
03      --text "Opine sobre o melhor
➥Sistema Operacional"\
04      --radiolist \
05      --width 350 \
06      --height 265 \
07      --print-column 3 \
08      --column "Escolha" \
09      --column "Fabricante" \
10      --column "Sistema Operacional" \
11          TRUE  IBM        AIX \
12          FALSE HP         HP-UX \
13          FALSE MicroSoft  rWindows \
14          FALSE Comunidade Linux \
15          FALSE Apple      MacOSx )
16 echo $SO
17 Linux
```

Exemplo 11: Exemplo simples de Check lists

```
01 zenity --list                                \
02      --title "Compras na quitanda"           \
03      --text "Marque o que precisa comprar na
➥quitanda" \
04      --checklist                             \
05      --column  Escolha                       \
06      --column  Frutas                        \
07          true  Pera                          \
08          true  Uva                           \
09          true  Maçã                          \
10          false Melancia
11 Pera|Uva|Maçã
```

Exemplo 12: Exemplo simples de Check lists

```
01 Usus='-user '$(zenity --list \
02      --checklist \
03      --title "Pesquisa de arquivos por usuário" \
04      --text "Selecione usuários para listar
➥arquivos" \
05      --height 400 \
06      --width 260 \
07      --separator ' -o -user ' \
08      --column Marque \
09      --column "Login Name" \
10      --column UID \
11          $(cut -f1,3 -d: /etc/passwd | sort | \
12              tr : ' ' | xargs -L1 echo FALSE))
13 echo $Usus
14 -user root -o -user julio
```

- A saída é então redirecionada para um `tr`, que troca os dois-pontos `:` por um espaço em branco. Após esse comando, a primeira linha recebida de `/etc/passwd` ficaria `root 0`.
- Esses dois campos separados por um espaço em branco vão para o comando `xargs` que, com a opção `-L1`, joga uma linha de cada vez para o final do `echo`.
- Após este comando, a primeira linha recebida de `/etc/passwd` ficaria `FALSE root 0`, criando dessa forma as três colunas para serem listadas.

Figura 6 Janela de opções em três colunas.

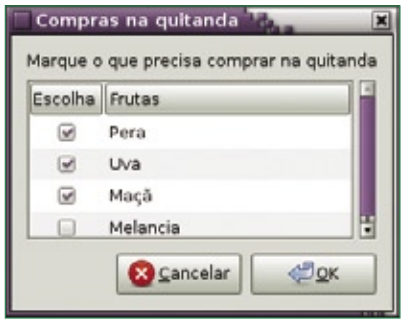


Figura 7 Diálogo básico usando *Check lists*.

Repare ainda no **exemplo 12** que o separador (`--separator`) não precisa ter somente um caractere.

O **exemplo 13** mostra como gerar a listagem dos arquivos, que produz a janela da **figura 9**.

Aqui tem uma pegadinha: o `find` sempre retorna *true* mesmo quando não acha arquivo algum que atenda aos seus critérios. Então tive de guardar a sua saída na variável `$Arqs` para testar se ela possui conteúdo (`[ $Arqs ]`) quando a defino como uma coluna do zenity. Caso contrário, abro uma caixa de atenção para dizer que o `find` não deu nenhum retorno. Poderia nesse ponto colocar também um `exit 1` para não aparecer a lista de arquivos vazia.

© Linux New Media do Brasil Editora Ltda.

Exemplo 13: Listagem de arquivos

```
01 zenity --list            \
02     --column Arquivos    \
03     $(Arqs=$(find . -type f $Usus); [ "$Arqs" ]
  && echo "$Arqs" ||
04         zenity --warning \
05             --text "Usuário sem arquivos")
```

Tabela 3: Formato de arquivo usado na próxima aula

Campo	Data de Nascimento	Nome	Endereço de e-mail	Telefone
Formato	AAAAMMDD	Xxxx Xxxx	usuário@dominio	(DD) NNNN-NNNN

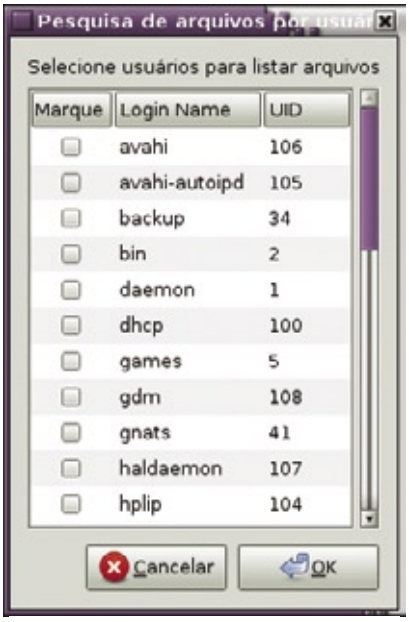


Figura 8 Janela *Check list* em três colunas.

Figura 9 Janela *Check list* em três colunas.

– Cara, quanto tempo perdi fazendo interface a caractere. Esse tal de zenity é legal mesmo!

– É, ele é muito legal, mas não é a panacéia universal. Para muitas aplicações, a interface a caractere ainda é a mais indicada.

Por hoje chega, mas antes vou te deixar um exercício para você consolidar o que aprendemos dessa vez. No primeiro dia que conversamos sobre o zenity, te pedi para fazer um programa para ler um arquivo com o formato mostrado na **tabela 3**.

Pois é, pegue esse arquivo e monte uma lista para que você escolha as pessoas que você quer convidar para o seu aniversário. Detalhe: você deverá poder escolher várias pessoas ao mesmo tempo. A lista exibirá os nomes para seleção, mas retornará os emails das pessoas selecionadas, para que você possa enviar-lhes o convite. ■

Sobre o autor

Julio C. Neves trabalha no SERPRO, que ele descreve como empresa exemplo do uso de Software Livre no Governo Federal. Ele também dá cursos de Shell e Zenity em São Paulo, Brasília ou turmas fechadas em qualquer localidade.

Snow666

Uma empresa tão livre quanto a sua imaginação.

Pensando na sua liberdade de pensamento, a F13 Tecnologia oferece produtos, soluções e serviços em Linux e Softwares livres, como suporte técnico presencial ou remoto e cursos de formação com certificação, tais como:

- Formação Linux com ênfase na LPI (4 módulos totalizando 160 horas)
- Formação PHP (3 módulos totalizando 120 horas)
- Firewall Avançado (40 horas)
- Controle de versões com CVS, SVN e Trac (8 horas)
- Virtualização com Xen (40 horas)
- Serviço de diretórios com OpenLdap (40 horas)
- Correio Eletrônico Avançado (40 horas)
- Voip & Asterisk com ênfase em DialPlan (40 horas - Curso ministrado por instrutor com certificação DCAP)
- Administração de Bancos de Dados Livres (PostgreSQL e MySQL - 40 horas)

Linux Professional Institute Approved Training Partner

F13 TECNOLOGIA

(85) 3252.3836

www.f13.com.br

© Linux New Media do Brasil Editora Ltda.

PROGRAMAÇÃO

Desenvolvimento de aplicativos multimídia com DCCP

Controle de congestionamento

O protocolo DCCP oferece aos desenvolvedores multimídia uma alternativa poderosa ao TCP e ao UDP.

por Leandro Melo de Sales

Nos últimos anos, os desenvolvedores promoveram o desenvolvimento de uma nova geração de aplicações de rede que transmitem e recebem conteúdo multimídia pela Internet. Novas aplicações multimídia baseadas em tecnologias como Voz sobre IP, rádio pela Internet, jogos online e videoconferência estão se tornando cada vez mais populares, graças à disponibilidade de bibliotecas de desenvolvimento e à abundância de redes de alta velocidade, incluindo os novos padrão de redes sem-fio WiMax e as redes 3G.

Até pouco tempo atrás, a maioria das aplicações via Internet tinha o protocolo TCP ou o UDP como opções para implementar o gerenciamento de transmissão de dados na camada de transporte da pilha TCP/IP, mas os desenvolvedores multimídia agora têm uma alternativa a esses dois protocolos. A IETF (*Internet Engineering Task Force*) padronizou recentemente o *Datagram Congestion Control Protocol*, ou DCCP (RFC4340)[1], um novo protocolo de transporte com suporte a controle de congestionamento projetado para transmitir conteúdos multimídia pela rede.

O DCCP está se tornando popular para transmitir dados multimídia, principalmente por ser mais eficaz que o UDP no compartilhamento da largura de banda disponível na rede, permitindo que outros fluxos de dados, como os transmitidos pelo TCP, sejam transmitidos com sucesso. Este artigo examinará o protocolo DCCP e mostrará como ativá-lo no Linux. Além disso, explicará como usar o plugin DCCP do *GStreamer* para criar uma aplicação cliente-servidor que utiliza o protocolo DCCP.

O DCCP foi especificado por Kohler e colaboradores em julho de 2001 no grupo de transporte da IETF. O protocolo DCCP fornece recursos projetados para resolverem alguns dos problemas que os desenvolvedores geralmente encontram ao desenvolver aplicações multimídia com TCP e UDP, como o tratamento e a medição corretos do atraso e do *jitter* causados pelo congestionamento na rede. O DCCP oferece uma camada de transporte orientada à conexão com suporte a controle de congestionamento durante a transmissão dos dados, porém não garante entrega de dados, tal como o protocolo UDP. Além disso, o DCCP permite a adição de novos mecanismos de controle de congestionamento. A aplicação pode selecionar um desses mecanismos durante o estabelecimento da conexão ou negociá-lo durante uma conexão já estabelecida, informando ao sistema remoto qual o mecanismo de controle de congestionamento que deseja utilizar.

O DCCP fornece também um mecanismo para obter as estatísticas da conexão, controle de congestionamento com suporte à Notificação Explícita de Congestionamento (ECN) e um método para descoberta de PMTU (*Path Maximum Transmission Unit*). O protocolo herda do TCP a orientação à conexão, o que permite melhor funcionamento em redes privadas, como aquelas que utilizam NAT (*Network Address Translation*).

A propósito, diferentemente do UDP e do DCCP, o TCP oferece um serviço de transmissão confiável de dados, um recurso que pode limitar a taxa de transmissão para uma dada conexão TCP. Quando os pacotes são perdidos, o TCP diminui a taxa de transmissão e volta a aumentá-la gradativamente quando consegue enviar pacotes ao sistema remoto. Para implementar esse serviço de transmissão confiável de dados, o TCP retransmite todos os pacotes que são perdidos. Nesse caso, enquanto os pacotes perdidos não tiverem sido entregues, os novos dados gerados pela aplicação são armazenados numa fila até que todos os pacotes perdidos sejam enviados. Por um

© Linux New Media do Brasil Editora Ltda.

lado, com essa forma de implementar a transmissão confiável, o TCP pode levar a um grande atraso do fluxo contínuo de dados, tal como ocorre em transmissões em tempo real. Com isso, é possível que o usuário experimente interrupções auditivas ou visuais no conteúdo multimídia sendo transmitido caso a rede esteja congestionada e o protocolo TCP precise retransmitir muitos pacotes.

Por outro lado, o UDP é um protocolo simples que implementa as mínimas funções para transportar dados de um computador para outro. É um protocolo que não estabelece conexão, não trata a entrega de pacotes e tampouco fornece controle de congestionamento de rede. Além disso, o UDP não reordena pacotes no receptor. Por causa da falta de qualquer tipo de controle de congestionamento, o UDP pode levar a um colapso de congestionamento da rede. Portanto, aplicações UDP podem enviar tantos dados quantos quiserem, mas muitos deles podem ser perdidos ou descartados pelos roteadores em virtude do congestionamento da rede.

Antes do DCCP, os desenvolvedores de aplicações multimídia precisavam optar entre o TCP ou o UDP. Se usassem TCP, os usuários poderiam experimentar longos atrasos de transmissão causados pela retransmissão de pacotes. Se usassem UDP, o resultado poderia ser um colapso de rede ou a má qualidade de transmissão. O DCCP foi desenvolvido para unir os melhores recursos desses dois protocolos e fornecer recursos para transmissão de dados multimídia de forma eficiente, compartilhando de forma justa a largura de banda disponível da rede[2] com outros protocolos.

Controle de congestionamento

O DCCP oferece dois algoritmos de controle de congestionamento, chamados CCIDs (*Congestion Control IDentifiers*). Os CCIDs são os componentes responsáveis por oferecer o controle de congestionamento em conexões DCCP. No Linux, os CCIDs são módulos do kernel que funcionam sobre o núcleo da implementação do DCCP. Como tal, podem ser carregados e descarregados a qualquer momento, e as aplicações podem selecionar um CCID adequado para a tarefa. Por exemplo, aplicações VoIP são caracterizadas pela transmissão de rajadas de pequenos pacotes seguidas de períodos de silêncio, enquanto aplicações de vídeo sob demanda geralmente transmitem conteúdo multimídia a taxas constantes. Nesse caso, para uma aplicação VoIP é melhor usar uma técnica de controle de congestionamento criada para VoIP.

Atualmente há dois CCIDs padronizados CCID-2 e CCID3. O CCID-2 (RFC 4341)[3] é melhor para aplicações que usem toda a banda de rede disponível e se adaptem a alterações súbitas de banda. Ele é semelhante ao controle de congestionamento do TCP, que se baseia no conceito de janela de congestionamento. O tamanho dessa janela dita quantos pacotes o remetente tem permissão para enviar pela rede. Isso significa que quanto maior for a janela de congestionamento, mais pacotes o TCP envia pela rede. Por um lado, quando o CCID-2 detecta que um pacote foi perdido, ele diminui à metade a janela de congestionamento, o que caracteriza uma mudança abrupta na taxa de transmissão, principalmente para aplicações multimídia. No estado inicial de transmissão, a janela de congestionamento aumenta de forma exponencial conforme os pacotes enviados são confirmados, até alcançar a fase de contenção do congestionamento, quando a taxa de transmissão aumenta linearmente até quando acontecer o primeiro evento de perda de pacote.

Por outro lado o CCID-3 (RFC 4342) [4] implementa um algoritmo de controle de congestionamento baseado no receptor, em que o remetente tem sua taxa controlada pelo receptor. Periodicamente, este envia ao remetente pacotes de informação relatando eventos de perda e outras estatísticas de conexão que são inseridas na equação do TFRC (*TCP-Friendly Rate Control*) (RFC 3448)[5], cujo resultado informa o valor da taxa de transmissão que o DCCP deverá utilizar para os próximos envios de pacotes.

O TFRC é razoavelmente justo quando compete por banda com fluxos TCP, mas tem uma menor variação da taxa de transmissão ao longo do tempo quando comparado a outros mecanismos de controle de congestionamento do TCP. Isso o torna mais adequado a aplicações como telefonia, para as quais é importante uma taxa de envio relativamente suave.

Ambiente

Para começar a explorar o mundo do DCCP no Linux, primeiro é preciso ativar o protocolo no kernel e depois instalar alguns aplicativos para testar o ambiente. Como o DCCP é um protocolo novo, ele está em constante desenvolvimento. Para testar as alterações mais recentes da implementação do protocolo no kernel, é preciso baixar o código-fonte do Linux do repositório git de desenvolvimento do DCCP [6]. Após a instalação do git – ele está disponível na maioria dos repositórios de pacote das distribuições – deve-se baixar toda a árvore com o código-fonte do kernel, incluindo a subárvore do DCCP:

```
git-clone git://eden-feed.erg.
➥abdn.uk/dccp_exp meu_dccp
```

O argumento `meu_dccp` é o diretório onde o git colocará o código-fonte baixado. Esse diretório não deve existir antes do comando ser executado. Caso já exista uma árvore git local e relativamente recente, é possível ace-

© Linux New Media do Brasil Editora Ltda.

Snow666

lerar o processo de download usando o diretório dessa árvore como parâmetro para o comando `git-clone`:

```
git-clone --reference arvore_git_
➥local git://eden-feed.erg.abdn.
➥ac.uk/dccp_exp meu_dccp
```

Nos dois casos, o `git-clone` levará algum tempo para baixar os fontes do kernel pela rede. Essa pode ser uma boa hora para ler sobre o DCCP no wiki do Linux [7] para aprender mais sobre o protocolo. Quando o git terminar o download, entre no diretório criado por ele (`meu_dccp`, no exemplo) e faça um *check-out* do ramo (*branch*) do DCCP:

```
git-checkout --track -b dccp
➥origem/dccp
```

Esse comando buscará as alterações mais recentes do código-fonte do DCCP. Para futuras atualizações do código-fonte do DCCP, execute o seguinte comando no diretório de origem:

```
git-pull git://eden-feed.erg.abdn.
➥ac.uk/dccp_exp dccp
```

O argumento `dccp` não é um diretório, mas o ramo criado antes com o `git_checkout`.

Com o código-fonte do Linux contendo as últimas alterações da sub-árvore do DCCP, é preciso configurar o kernel de acordo com a arquitetura da máquina [8]. O DCCP é habilitado nas opções de rede (seção *Networking*):

```
Networking -->
    Network options -->
      The DCCP Protocol -->
```

Dentro dessa opção, é possível especificar os CCIDs e algumas outras opções do DCCP. Após selecionar todo o necessário, compile o kernel. Depois de reiniciar a máquina com ele, é possível alternar entre os CCIDs e mudar o número de seqüência da janela de seqüência com os seguintes comandos:

```
sudo sysctl -w net.dccp.default.
➥seq_window=1000
sudo sysctl -w net.dccp.default.
➥rc_ccid=2
sudo sysctl -w net.dccp.default.
➥tx_ccid=2
```

Isso define `1000` como número da seqüência da janela de congestionamento e o CCID-2 nas duas direções para todas as conexões iniciadas com DCCP. Note que também é possível especificar esses parâmetros com o uso de uma linguagem de programação usando a função de socket `setsockopt`.

Exemplo 1: Servidor DCCP em Python (dccp_server.py)

```
01 import socket
02
03 socket.SOCK_DCCP = 6
04 socket.IPPROTO_DCCP = 33
05 endereco = (socket.gethostname(),12345)
06
07 server = socket.socket(socket.AF_INET, socket.SOCK_DCCP,socket.
➥IPPROTO_DCCP)
08
09 server.bind(endereco)
10 server.listen(1)
11 s,a = server.accept()
12 print s.recv(1024)
```

Exemplo 2: Cliente DCCP em Python (dccp_client.py)

```
01 import socket
02
03 socket.SOCK_DCCP = 6
04 socket.IPPROTO_DCCP = 33
05 endereco = (socket.gethostname(),12345)
06
07 cliente = socket.socket(socket.AF_INET, socket.SOCK_DCCP,socket.
➥IPPROTO_DCCP)
08
09 cliente.connect(endereco)
10 cliente.send("Hello World")
```

Testando

O *IPerf* é uma ferramenta de medição de rede originalmente criada para funcionar com TCP e UDP. Porém, graças a um patch de Gerrit Renker, ela também suporta o DCCP e portanto pode ser usada tanto como cliente quanto como servidor DCCP.

Para usar o IPerf com suporte ao DCCP, primeiro deve-se baixar e instalar a ferramenta [9] (`make` e `make install` resolverão essa etapa sem complicações). O site também fornece informações úteis sobre o IPerf com DCCP.

© Linux New Media do Brasil Editora Ltda.

Para testar o DCCP, inicie um servidor com os seguintes argumentos:

```
iperf -s -d -l 1424 -i 1
```

Esse comando informa ao IPerf para iniciar uma conexão DCCP (opção `-d`) e agir como servidor (`-s`). O servidor vai transmitir pacotes de dados com 1424 bytes (`-l 1424`) e exibir relatórios sobre a transmissão a cada um segundo (`-i 1`). Para executar um cliente IPerf que se conectará ao servidor especificado, execute o seguinte comando:

```
iperf -c IP_DO_SERVIDOR -d -l 1424
➥-i 1 -t 100
```

A opção `-c` especifica que o IPerf deve agir como cliente e é seguida do IP do servidor ao qual deve se conectar. A opção `-t` define a duração da transmissão em segundos. Para uma rápida introdução ao DCCP, considere um aplicativo simples em *Python* que envia um *hello world* a uma aplicação remota. O código do servidor DCCP em Python é mostrado no **exemplo 1**, com o cliente no **exemplo 2**.

Na **linha 7 do exemplo 1**, a criação do socket é feita com uso dos valores de `socket.SOCK_DCCP` e `socket.IPPROTO_DCCP`. O valor de `socket.IPPROTO_DCCP` é `33`, que é o número alocado ao protocolo DCCP pelo IANA (*Internet Assigned Numbers Authority*). As outras linhas são muito semelhantes à implementação de uma conexão TCP por socket. O cliente do **exemplo 2** se conecta ao servidor implementado no **exemplo 1**.

Agora que o servidor e o cliente estão se comunicando, é hora de adicionar alguns novos recursos multimídia com ajuda da plataforma GStreamer.

Quadro 1: Instalação do plugin DCCP do GStreamer

O plugin do DCCP para o GStreamer faz parte do projeto *E-Phone* e DCCP para a plataforma *Maemo*, da Nokia [11]. Depois de baixar o plugin[12], execute os seguintes comandos:

```
./autogen --prefix=/usr
make
make install
```

Exemplo 3: Inicialização (gst_dccp_server.c)

```
01 #include <string.h>
02 #include <math.h>
03 #include <gst/gst.h>
04
05 int main (int argc, char **argv) {
06     GMainLoop *loop;
07     GstElement *pipeline, *filesrc, *mp3parse,
➥*dccpserversink;
08     GstBus *bus;
09
10     /* inicializa o GStreamer */
11     gst_init (&argc, &argv);
12     loop = g_main_loop_new(NULL, FALSE);
13
14     /* verifica os argumentos recebidos*/
15     if (argc != 3) {
16         g_print ("Uso: %s
➥porta local_do_arquivo_mp3\n",argv[0]);
17         return -1;
18     }
19     return 0;
20 }
```

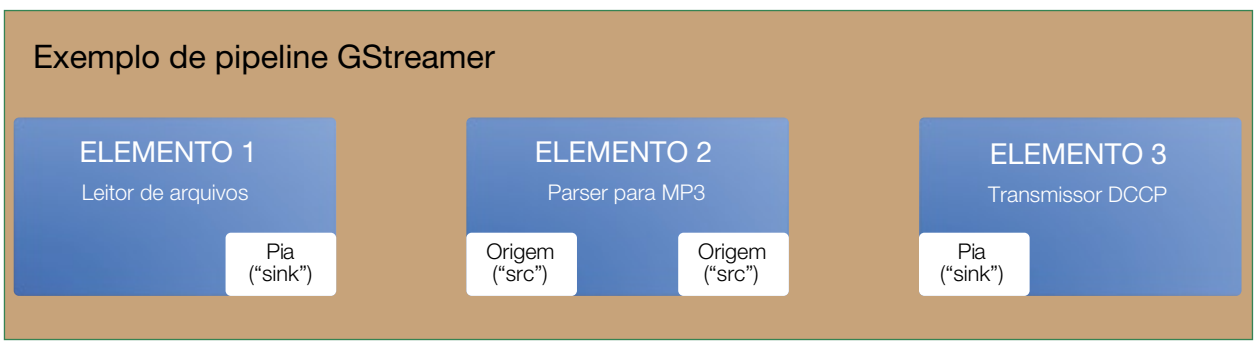


Figura 1 Exemplo de pipeline GStreamer com três elementos: um leitor de arquivo, um codificador MP3 e um transmissor DCCP.

© Linux New Media do Brasil Editora Ltda.

Snow666

O GStreamer é uma plataforma multimídia de código aberto que permite ao proramador escrever vários tipos de aplicações com streaming [10]. Diversos aplicativos populares o utilizam, como *Kaffeine*, *Amarok*, *Phonon*, *Rhythmbox* e *Totem*. A plataforma GStreamer facilita o processo de escrita de aplicações multimídia, abrangendo desde a reprodução de áudio e vídeo até o streaming de conteúdo multimídia.

Exemplo 4: Barramento do GStreamer (gst_dccp_server.c)

```
01 static gboolean bus_event_callback (GstBus
➥*bus,GstMessage *msg,gpointerdata){
02
03      GMainLoop *loop =(GMainLoop *) data;
04
05      switch (GST_MESSAGE_TYPE(msg)) {
06          case GST_MESSAGE_EOS: {
07              g_print("End-of-stream\n");
08              g_main_loop_quit(loop);
09              break;
10          }
11          case GST_MESSAGE_ERROR: {
12              gchar *debug;
13              GError *err;
14              gst_message_parse_error
➥(msg, &err, &debug);
15              g_free (debug);
16              g_print ("Error:%s\n",
➥err->message);
17              g_error_free (err);
18              g_main_loop_quit(loop);
19              break;
20          }
21          default:
22          break;
23      }
24
25      return TRUE;
26 }
```

Exemplo 5: Elementos do GStreamer

```
01 /* definição dos elementos */
02 pipeline = gst_pipeline_new (“dccp-audio-sender”);
03 filesrc = gst_element_factory_make (“filesrc”, “file-source”);
04 mp3parse = gst_element_factory_make (“mp3parse”, “mp3parse”);
05 dccpserversink = gst_element_factory_make(“dccpserversink”,
➥“server-sink”);
```

Exemplo 6: Verificação dos elementos

```
01 if (!pipeline || !filesrc|| !mp3parse ||!dccpserversink) {
02     g_print (“Um ou mais elementos nao puderam ser
➥ instanciados\n”);
03     return -1;
04 }
```

Plugin do GStreamer

O GStreamer se baseia em plugins e cada plugin contém elementos. Cada um desses elementos fornece uma função específica – tal como codificação, exibição ou renderização –, assim como a capacidade de ler ou escrever arquivos. Ao combinar esses elementos, o programador é capaz de criar um *pipeline* para realizar funções mais complexas. Por exemplo, é possível criar um para ler um arquivo MP3, decodificar seus conteúdos e reproduzir o áudio.

A **figura 1** representa um pipeline do GStreamer composto por três elementos. Os dados fluem do *Elemento 1* para o *Elemento 2* e por último para o *Elemento 3*. O primeiro é o de origem, responsável por fornecer dados ao pipeline, enquanto o terceiro é responsável por consumir os dados do pipeline. Entre os elementos de origem e o da “pia” (*sink*), o pipeline pode usar outros elementos tais como o *Elemento 2* (mostrado na **figura 1**). Esses elementos intermediários são responsáveis por processar e modificar o conteúdo conforme os dados passam ao longo do pipeline.

O plugin DCCP para GStreamer foi desenvolvido para lidar com a transmissão de dados usando o protocolo DCCP. Esse plugin possui quatro elementos: `dccpserversrc`, `dccpserversink`, `dccpclientsrc` e `dccpclientsink`.

Os elementos de origem (`dccpserversrc` e `dccpclientsrc`) são responsáveis por ler os dados de um socket DCCP e enviá-los para o pipeline, enquanto que os elementos de destino (*sink* ou “pia”) (`dccpserversink` e `dccpclientsink`) são responsáveis por receber os dados do pipeline e escrevê-los num socket DCCP.

© Linux New Media do Brasil Editora Ltda.

Os elementos `dccpserversrc` e `dccpserversink` se comportam como o servidor, mas somente o `dccpserversink` é capaz de transmitir, enquanto somente o `dccpserversrc` é capaz de receber dados. Quando o elemento servidor é inicializado, ele permanece em modo de espera, o que significa que o elemento é capaz de aceitar uma nova conexão a partir de um elemento cliente. O elemento `dccpclientsink` pode se conectar ao `dccpserversrc` e o `dccpclientstc` pode se conectar ao `dccpserversink`.

Para enviar dados do servidor para o cliente, é preciso usar os elementos `dccpclientsrc` e `dccpserversink`. Para o sentido contrário, os elementos necessários são `dccpclientsink` e `dccpserversrc`. Uma maneira bastante simples de praticar o uso desses elementos é utilizando o comando `gst-launch`.

Esse comando do GStreamer suporta a criação de pipelines e também é usado para depurar plugins. Sua sintaxe básica é:

```
gst-launch <parâmetros do gst-
➥launch> <elemento> <parâmetros do
➥elemento> ! <elemento> <parâmetros
➥do elemento> ! <elemento>
<parâmetros do elemento> ...
```

Note o caractere `!` que separa os elementos do plugin: ele é semelhante aos *pipes* (|) do shell. Isso significa que a saída de um elemento é a entrada do próximo.

Como exemplo do comando `gst-launch`, considere dois pipelines para transmitir áudio em MP3 pela rede com DCCP: um funciona como um servidor DCCP que envia o áudio e o segundo pipeline é associado a um cliente DCCP que se conecta ao servidor DCCP remoto e reproduz o conteúdo de áudio recebido.

Para fazer o exemplo funcionar, é preciso instalar o GStreamer. Nesse caso, são necessários os pacotes *gstreamer-core*, *gst-base/plugins* e *gst-ugly-plugins*. Não se preocupe com a instalação do GStreamer; ele é amplamente usado e está disponível na grande maioria das distribuições. Assim que for instalado o GStreamer, a última etapa é compilar e instalar o seu plugin do DCCP (veja o **quadro 1**). Note, no entanto, que o pacote *gst-bad-plugins*, a partir da versão 0.10.9, dispensará o procedimento descrito no **quadro 1**, pois já incluirá o plugin DCCP.

O exemplo do `gst-launch` a seguir executa um servidor que aceita conexões DCCP. Após um cliente se conectar, o servidor começa o streaming do arquivo de áudio chamado `música.mp3`. Note que é possível especificar o CCID com o parâmetro `ccid`.

```
gst-launch -v filesrc
➥location=música.mp3 ! mp3parse !
➥dccpserversink port=9011 ccid=2
```

Esse pipeline inicia o servidor na porta 9011 DCCP. O servidor ficará esperando a conexão de algum cliente. Quando ocorre a conexão, o servidor começa a transmitir o streaming usando o CCID-2. O elemento `mp3parse` é responsável por identificar o padrão MP3 presente no arquivo `música.mp3` e repassar os dados no formato `.mp3` para o elemento `dccpserversink`. Para mais informações sobre o `dccpser-`

Exemplo 7: Definição de parâmetros

```
01 g_object_set (G_OBJECT(dccpserversink), "port",atoi(argv[1]),
➥NULL);
02 g_object_set (G_OBJECT(filesrc), "location",argv[2], NULL);
```

Exemplo 8: Vínculo de bus_event_callback

```
01 bus = gst_pipeline_get_bus (GST_PIPELINE (pipeline));
02 gst_bus_add_watch (bus, bus_event_callback, loop);
03 gst_object_unref (bus);
04
05 gst_bin_add_many (GST_BIN(pipeline), filesrc, mp3parse,
➥dccpserversink, NULL);
06 /* Vincular os elementos no pipeline */
07 gst_element_link_many(filesrc, mp3parse,dccpserversink, NULL);
```

Exemplo 9: Execução do pipeline

```
01 /* Reproduzir */
02 g_print ("Configurado para TOCAR\n");
03 gst_element_set_state(pipeline, GST_STATE_PLAYING);
04 g_print ("Rodando\n");
05 g_main_loop_run (loop);// inicia o loop do GStreamer
06
07 /* Liberar recursos */
08 g_print ("Retornou, parando a reproducao\n");
09 gst_element_set_state(pipeline, GST_STATE_NULL);
10 g_print ("Apagando o pipeline\n");
11 gst_object_unref (GST_OBJECT (pipeline));w
```


© Linux New Media do Brasil Editora Ltda.

Snow666

Exemplo 10: Aplicativo cliente DCCP (continua na página seguinte)

```
01 #include <string.h>
02 #include <math.h>
03 #include <gst/gst.h>
04
05 static gboolean bus_event_callback (GstBus *bus, GstMessage *msg, gpointer
➥data){
06
07     GMainLoop *loop =(GMainLoop *) data;
08
09     switch (GST_MESSAGE_TYPE(msg)) {
10         case GST_MESSAGE_EOS:
11             g_print("Fim da transmissao\n");
12             g_main_loop_quit(loop);
13             break;
14         case GST_MESSAGE_ERROR: {
15             gchar *debug;
16             GError *err;
17             gst_message_parse_error(msg, &err, &debug);
18             g_free (debug);
19             g_print ("Erro: %s\n",err->message);
20             g_error_free (err);
21             g_main_loop_quit(loop);
22             break;
23         }
24         default:
25         break;
26     }
27
28     return TRUE;
29 }
30
31 int main (int argc, char *argv){
32     GMainLoop *loop;
33     GstElement *pipeline, *dccpclientsrc, *decodebin, *alsasink;
34     GstBus *bus;
35
36     /* inicializar o GStreamer */
37     gst_init (&argc, &argv);
38     loop = g_main_loop_new(NULL, FALSE);
39
40     /* verificar argumentos recebidos */
41         if (argc != 3) {
42         g_print ("Uso: %shostServidor portaServidor\n",argv[0]);
43         return -1;
44     }
45
46     /* criar os elementos */
47     pipeline = gst_pipeline_new ("audio-sender");
48     dccpclientsrc = gst_element_factory_make("dccpclientsrc","client-source");
49     decodebin = gst_element_factory_make ("decodebin","decodebin");
50     alsasink = gst_element_factory_make ("alsasink","alsa-sink");
51
52     if (!pipeline || !alsasink || !decodebin || !dccpclientsrc) {
53         g_print ("Um ou mais elementos nao puderam ser instanciados\n");
54         return -1;
55     }
56
57     // define host e porta para o servidor escutar
```


© Linux New Media do Brasil Editora Ltda.

Exemplo 10: Aplicativo cliente DCCP (continuação)

```
58      g_object_set (G_OBJECT(dccpclientsrc), "host",argv[1], NULL);
59      g_object_set (G_OBJECT(dccpclientsrc), "port",atoi(argv[2]), NULL);
60
61      /* joga todos os elementos numa lata */
62      gst_bin_add_many (GST_BIN(pipeline), dccpclientsrc,decodebin, alsasink,
➥NULL);
63
64      gst_element_link_many(dccpclientsrc, decodebin,alsasink, NULL);
65
66      bus = gst_pipeline_get_bus(GST_PIPELINE (pipeline));
67      gst_bus_add_watch (bus,bus_event_callback, loop);
68      gst_object_unref (bus);
69
70      /* Agora vamos tocar e iterar. */
71      g_print ("Configurado para TOCAR\n");
72      gst_element_set_state(pipeline, GST_STATE_PLAYING);
73      g_print ("Rodando\n");
74      g_main_loop_run (loop);
75
76      /* clean up nicely */
77      g_print ("Retornou, parando a reproducao\n");
78      gst_element_set_state(pipeline, GST_STATE_NULL);
79      g_print ("Apagando o pipeline\n");
80      gst_object_unref (GST_OBJECT (pipeline));
81
82      return 0;
83  }
84
```

versink, use o comando gst-inspect dccpserversink.

A seguir, inicie o cliente correspondente:

```
gst-launch -v dccpclientsrc
➥host=192.168.1.55 port=9011 ccid=2
➥! decodebin ! alsasink
```

Esse pipeline do GStreamer inicia o cliente e se conecta à máquina 192.168.1.55 na porta 9011. Assim que se conecta, o cliente começa a receber o streaming MP3, decodifica-o usando o elemento decodebin e envia o resultado para o elemento alsasink, que reproduz o conteúdo multimídia no dispositivo de áudio padrão.

Aplicativo multimídia

Agora vamos escrever um aplicativo multimídia completo usando o plugin DCCP. O exemplo a seguir utiliza o plugin DCCP de forma embutida no aplicativo. Criaremos o pipeline mostrado nos exemplos anteriores, mas dessa vez em C e com a biblioteca *GObject*, disponível para o desenvolvimento de aplicativos e plugins com GStreamer.

Vamos começar inicializando as configurações do GStreamer, como mostra o **exemplo 3**. Note que este exemplo também define os elementos filesrc, mp3parse e dccpserversink.

O passo seguinte é instanciar uma função de *callback* para escutar os eventos do pipeline GStreamer. O GStreamer se encarrega de encaminhar mensagens do pipeline para o aplicativo por meio de um conceito conhecido por barramento (*bus*). A idéia é criar um manipulador de mensagens no barramento que permita ao aplicativo controlar o pipeline quando necessário. A função do **exemplo 4** deve ser inserida acima da função main do **exemplo 3**.

Toda vez que ocorrer um evento no pipeline, o GStreamer chama a função gboolean bus_call. Por exemplo, se for implementada uma interface gráfica para o aplicativo, é possível exibir uma mensagem para anunciar o fim do streaming ou desativar o botão de parada quando o tipo de mensagem do barramento GStreamer for GST_MESSAGE_EOS. Agora vem a parte mais importante desse exemplo – definir os elementos e criar o pipeline GStreamer. Insira o código do **exemplo 5** na função main (após a parte que verifica o número de parâmetros).

O **exemplo 5** primeiro instancia um novo pipeline, dccp-audio-sender, que pode ser usado para futuras referências no código. Depois, o código instancia o elemento filesrc com o nome file-source. Esse elemento será usado para ler o arquivo MP3 especificado como um argumento do aplicativo. Use o mesmo processo

© Linux New Media do Brasil Editora Ltda.

Snow666

para instanciar os elementos `mp3parse` e `dccpserversink`. Assim que todos os elementos necessários tenham sido instanciados, certifique-se de que todos estejam corretamente carregados. Para esse caso, faça como mostra o **exemplo 6**.

A próxima etapa é definir os parâmetros respectivos do elemento, como mostra o **exemplo 7**. Para esse aplicativo, precisamos especificar dois parâmetros: a porta onde o servidor escutará e aceitará conexões de clientes e também o caminho do arquivo de áudio, representado pelo parâmetro `location`. Todo este procedimento que estamos fazendo manualmente é realizado de forma automática pelo comando `gst-launch`.

Quando todos os elementos forem instanciados e os parâmetros definidos, é hora de vincular o callback do barramento definido no **exemplo 4**. Além disso, é preciso adicionar os elementos ao pipeline e ligá-los na mesma ordem em que ligamos ao executar o comando `gst-launch` (**exemplo 8**). O **exemplo 9** mostra como executar o pipeline. Note que o GStreamer roda num loop (**linha 5**). Isso significa que quando o loop termina – por exemplo, quando o usuário digita **[Ctrl]+[C]** –, é necessário liberar recursos de memória não mais utilizados (**linhas 9 e 11**). A parte mais fácil é compilar esse aplicativo servidor – basta executar o seguinte comando, que fará o link das bibliotecas do GStreamer ao aplicativo de exemplo:

```
gcc -Wall $(pkg-config --cflags
➥--libs gstreamer-0.10) gst_dccp_
➥dccp_server.c -o gst_dccp_server
```

Para rodar o aplicativo `gst_dccp_server`, basta digitar o seguinte comando:

```
./gst_dccp_server 9011 música.mp3
```

Note que o exemplo usa a porta 9011, que o servidor utilizará para abrir o socket DCCP e transmitir o streaming pela rede para o cliente DCCP remoto.

Agora vamos compilar o aplicativo cliente correspondente que atuará exatamente como o cliente `gst-launch` mencionado anteriormente. O aplicativo cliente DCCP é semelhante ao servidor (**exemplo 10**). Basicamente, é preciso inicializar o GStreamer, verificar os parâmetros de linha de comando, instanciar os elementos necessários e vinculá-los para compilar o pipeline do GStreamer.

Por último, para compilar e executar o aplicativo cliente, basta o comando:

```
gcc -Wall $(pkg-config --cflags
➥--libs gstreamer-0.10) gst_
➥dccp_ client.c -o gst_dccp_client
./gst_dccp_client localhost 9011
```

Conclusão

Este artigo apresentou os conceitos básicos do protocolo DCCP – como ativá-lo no Linux e como criar um aplicativo baseado nesse protocolo com uso do plugin do GStreamer. As ferramentas de análise e teste de redes, como *TTCP*, *tcpdump* e *Wireshark*, já oferecem supote ao DCCP, e ferramentas multimídia como o *VLC* sabem usar streaming sobre esse protocolo. Conforme os desenvolvedores comecem a conhecer seus benefícios, o DCCP será mais difundido nos próximos anos e talvez venha a ser o padrão para multimídia na Internet. ■

Mais informações

[1] RFC 4340 – DCCP: http://tools.ietf.org/html/rfc4340

[2] Leandro M. Sales, Hyggo O. Almeida, Angelo Perkusich and Marcello Sales Jr: "On the Performance of TCP, UDP, and DCCP over 802.11g Networks": http://portal.acm.org/citation.cfm?id=1363686.1364187

[3] RFC 4341 – CCID-2: http://tools.ietf.org/html/rfc4341

[4] RFC 4342 – CCID-3: http://tools.ietf.org/html/rfc4342

[5] RFC 3448 – TFRC: http://tools.ietf.org/html/rfc3448

[6] Repositório git do DCCP: git://eden-feed.erg.abdn.ac.uk/dccp_exp

[7] DCCP no wiki Linux: http://www.linux-foundation.org/en/Net:DCCP

[8] Documentação do kernel: http://kernel.org/doc/

[9] IPerf: http://www.erg.abdn.ac.uk/users/gerrit/dccp/apps/#iperf

[10] GStreamer: http://gstreamer.freedesktop.org/

[11] Maemo: http://www.maemo.org/

[12] Plugin DCCP no GStreamer: https://garage.maemo.org/frs/?group_id=297

Sobre o autor

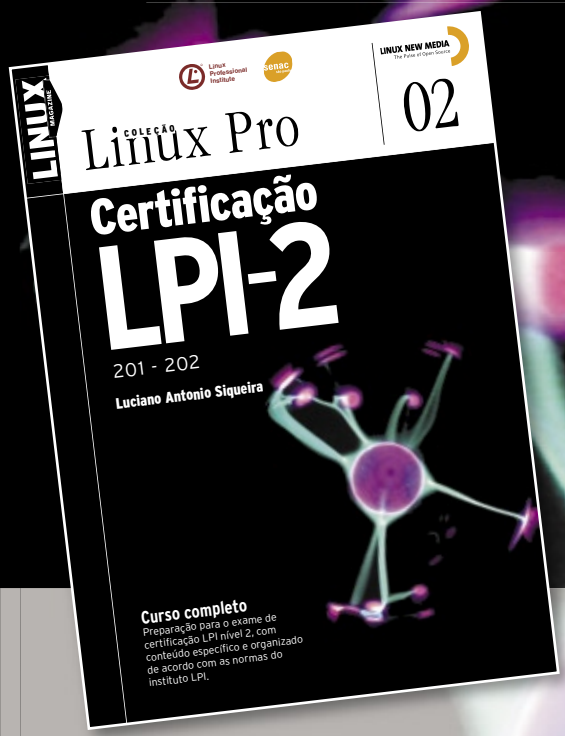
Leandro Melo de Sales contribui para o DCCP no Linux desde 2006 com foco em dispositivos embarcados. É mantenedor do DCCP na plataforma Maemo da Nokia e está trabalhando no CCID-4 e numa variação de cliente VoIP baseada em DCCP. Ele agradece a outros colaboradores: Angelo Perkusich, Arnaldo Carvalho, Erivaldo Xavier, Felipe Coutinho, Hyggo Almeida, Marcello Júnior e Thiago Santos.

© Linux New Media do Brasil Editora Ltda.

Snow666

Coleção Linux Pro

Prepare-se para a principal certificação profissional do mercado Linux



O primeiro volume traz informações referentes à LPI-1 e é o primeiro passo para a certificação. Estude para a prova de acordo com o conteúdo programático estabelecido pelo LPI.

Pautado conforme o roteiro estabelecido pelo próprio Linux Professional Institute e por este recomendado, o segundo volume é voltado à preparação do exame para a LPI-2.

Certifique-se para entrar em um mercado de trabalho em pleno crescimento no Brasil e no mundo.

Só a LPI garante a formação que o mercado espera para lidar com os ambientes mais diversos.
A qualidade destes volumes é atestada pelos selos do LPI e do SENAC, que os utilizam como material didático em seus cursos.

A venda nas melhores livrarias, no site www.linuxmagazine.com.br, ou pelo telefone (11) 4082-1300.

LINUX NEW MEDIA
The Pulse of Open Source

© Linux New Media do Brasil Editora Ltda.

Linux.local

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

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

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
Ceará										
F13 Tecnologia	Fortaleza	Rua Coronel Solon, 480 – Bairro de Fátima Fortaleza - CE - CEP: 60040-270	85 3252-3836	www.f13.com.br		✔	✔		✔	✔
Espírito Santo										
Linux Shopp	Vila Velha	Rua São Simão (Correspondência), 18 – CEP: 29113-120	27 3082-0932	www.linuxshopp.com.br	✔	✔		✔	✔	
Megawork Consultoria e Sistemas	Vitória	Rua Chapot Presvot, 389 – Praia do Canto – CEP: 29055-410 sl 201, 202	27 3315-2370	www.megawork.com.br			✔		✔	✔
Spirit Linux	Vitória	Rua Marins Alvarino, 150 – CEP: 29047-660	27 3227-5543	www.spiritlinux.com.br			✔		✔	✔
Minas Gerais										
Instituto Online	Belo Horizonte	Av. Bias Fortes, 932, Sala 204 – CEP: 30170-011	31 3224-7920	www.institutoonline.com.br				✔		✔
Linux Place	Belo Horizonte	Rua do Ouro, 136, Sala 301 – Serra – CEP: 30220-000	31 3284-0575	corporate.linuxplace.com.br		✔	✔		✔	✔
Microhard	Belo Horizonte	Rua República da Argentina, 520 – Sion – CEP: 30315-490	31 3281-5522	www.microhard.com.br	✔	✔	✔		✔	✔
TurboSite	Belo Horizonte	Rua Paraíba, 966, Sala 303 – Savassi – CEP: 30130-141	0800 702-9004	www.turbosite.com.br	✔				✔	✔
Paraná										
iSolve	Curitiba	Av. Cândido de Abreu, 526, Cj. 1206B – CEP: 80530-000	41 252-2977	www.isolve.com.br		✔	✔			✔
Mandriva Conectiva	Curitiba	Rua Tocantins, 89 – Cristo Rei – CEP: 80050-430	41 3360-2600	www.mandriva.com.br			✔	✔	✔	✔
Telway Tecnologia	Curitiba	Rua Francisco Rocha 1830/71	41 3203-0375	www.telway.com.br					✔	✔
Rio de Janeiro										
Múltipla Tecnologia da Informação	Rio de Janeiro	Av. Rio Branco, 37, 14° andar – CEP: 20090-003	21 2203-2622	www.multipla-ti.com.br	✔		✔		✔	✔
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4º andar Centro – CEP: 20030-012	21 2220-7055	www.nsi.com.br				✔		✔
Open IT	Rio de Janeiro	Rua do Mercado, 34, Sl, 402 – Centro – CEP: 20010-120	21 2508-9103	www.openit.com.br				✔		✔
Unipi Tecnologias	Campos dos Goytacazes	Av. Alberto Torres, 303, 1ºandar – Centro – CEP: 28035-581	22 2725-1041	www.unipi.com.br			✔	✔	✔	✔
Rio Grande do Sul										
4up Soluções Corporativas	Novo Hamburgo	Pso. Calçadão Osvaldo Cruz, 54 sl. 301 CEP: 93510-015	51 3581-4383	www.4up.com.br		✔	✔		✔	✔
Definitiva Informática	Novo Hamburgo	Rua General Osório, 402 - Hamburgo Velho	51 3594 3140	www.definitiva.com.br	✔		✔		✔	✔
Solis	Lajeado	Av. 7 de Setembro, 184, sala 401 – Bairro Moinhos CEP: 95900-000	51 3714-6653	www.solis.coop.br		✔	✔	✔	✔	✔
DualCon	Novo Hamburgo	Rua Joaquim Pedro Soares, 1099, Sl. 305 – Centro	51 3593-5437	www.dualcon.com.br	✔		✔		✔	✔
Datarecover	Porto Alegre	Av. Carlos Gomes, 403, Sala 908, Centro Comercial Atrium Center – Bela Vista – CEP: 90480-003	51 3018-1200	www.datarecover.com.br	✔		✔			
LM2 Consulting	Porto Alegre	Rua Germano Petersen Junior, 101-Sl 202 – Higienópolis – CEP: 90540-140	51 3018-1007	www.lm2.com.br			✔		✔	✔
Lnx-IT Informação e Tecnologia	Porto Alegre	Av. Venâncio Aires, 1137 – Rio Branco – CEP: 90.040.193	51 3331-1446	www.lnx-it.inf.br	✔		✔		✔	✔
Plugin	Porto Alegre	Av. Júlio de Castilhos, 132, 11º andar Centro – CEP: 90030-130	51 4003-1001	www.plugin.com.br	✔		✔		✔	
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3286-3799	www.tehospedo.com.br	✔	✔				
São Paulo										
Ws Host	Arthur Nogueira	Rua Jerere, 36 – Vista Alegre – CEP: 13280-000	19 3846-1137	www.wshost.com.br	✔		✔		✔	
DigiVoice	Barueri	Al. Juruá, 159, Térreo – Alphaville – CEP: 06455-010	11 4195-2557	www.digivoice.com.br	✔	✔	✔		✔	✔
Dextra Sistemas	Campinas	Rua Antônio Paioli, 320 – Pq. das Universidades – CEP: 13086-045	19 3256-6722	www.dextra.com.br			✔		✔	✔
Insigne Free Software do Brasil	Campinas	Av. Andrades Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignesoftware.com			✔		✔	✔
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	www.microcamp.com.br				✔		✔
PC2 Consultoria em Software Livre	Carapicuíba	Rua Edeia, 500 - CEP: 06350-080	11 3213-6388	www.pc2consultoria.com	✔					✔
Savant Tecnologia	Diadema	Av. Senador Vitorino Freire, 465 – CEP: 09910-550	11 5034-4199	www.savant.com.br	✔	✔	✔			✔
Epopéia Informática	Marília	Rua Goiás, 392 – Bairro Cascata – CEP: 17509-140	14 3413-1137	www.epopeia.com.br						✔
Redentor	Osasco	Rua Costante Piovan, 150 – Jd. Três Montanhas – CEP: 06263-270	11 2106-9392	www.redentor.ind.br	✔					
Go-Global	Santana de Parnaíba	Av. Yojiro Takaoca, 4384, Ed. Shopping Service, Cj. 1013 – CEP: 06541-038	11 2173-4211	www.go-global.com.br			✔		✔	✔
AW2NET	Santo André	Rua Edson Soares, 59 – CEP: 09760-350	11 4990-0065	www.aw2net.com.br			✔		✔	✔
Async Open Source	São Carlos	Rua Orlando Damiano, 2212 – CEP 13560-450	16 3376-0125	www.async.com.br	✔				✔	✔

© Linux New Media do Brasil Editora Ltda.

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
São Paulo (continuação)										
Delix Internet	São José do Rio Preto	Rua Voluntário de São Paulo, 3066 9º – Centro – CEP: 15015-909	11 4062-9889	www.delixhosting.com.br	✔		✔		✔	
4Linux	São Paulo	Rua Teixeira da Silva, 660, 6º andar – CEP: 04002-031	11 2125-4747	www.4linux.com.br					✔	✔
A Casa do Linux	São Paulo	Al. Jaú, 490 – Jd. Paulista – CEP: 01420-000	11 3549-5151	www.acasadolinux.com.br			✔		✔	✔
Accenture do Brasil Ltda.	São Paulo	Rua Alexandre Dumas, 2051 – Chácara Santo Antônio – CEP: 04717-004	11 5188-3000	www.accenture.com.br			✔		✔	✔
ACR Informática	São Paulo	Rua Lincoln de Albuquerque, 65 –Perdizes – CEP: 05004-010	11 3873-1515	www.acrinformatica.com.br	✔					✔
Agit Informática	São Paulo	Rua Major Quedinho, 111, 5º andar, Cj. 508 – Centro – CEP: 01050-030	11 3255-4945	www.agit.com.br	✔	✔				✔
Altbit - Informática Comércio e Serviços LTDA.	São Paulo	Av. Francisco Matarazzo, 229, Cj. 57 – Água Branca – CEP 05001-000	11 3879-9390	www.altbit.com.br	✔		✔		✔	✔
AS2M -WPC Consultoria	São Paulo	Rua Três Rios, 131, Cj. 61A – Bom Retiro – CEP: 01123-001	11 3228-3709	www.wpc.com.br			✔		✔	✔
Big Host	São Paulo	Rua Dr. Miguel Couto, 58 – Centro – CEP: 01008-010	11 3033-4000	www.bighost.com.br	✔				✔	✔
Blanes	São Paulo	Rua André Ampére, 153 – 9º andar – Conj. 91 CEP: 04562-907 (próx. Av. L. C. Berrini)	11 5506-9677	www.blanes.com.br	✔	✔	✔		✔	✔
Commlogik do Brasil Ltda.	São Paulo	Av. das Nações Unidas, 13.797, Bloco II, 6º andar – Morumbi – CEP: 04794-000	11 5503-1011	www.commlogik.com.br	✔	✔	✔		✔	✔
Computer Consulting Projeto e Consultoria Ltda.	São Paulo	Rua Vergueiro, 6455, Cj. 06 – Alto do Ipiranga – CEP: 04273-100	11 5062-3927	www.computerconsulting.com.br	✔		✔		✔	✔
Consist Consultoria, Sistemas e Representações Ltda.	São Paulo	Av. das Nações Unidas, 20.727 – CEP: 04795-100	11 5693-7210	www.consist.com.br			✔	✔	✔	✔
Domínio Tecnologia	São Paulo	Rua das Carnaubeiras, 98 – Metrô Conceição – CEP: 04343-080	11 5017-0040	www.dominiotecnologia.com.br	✔					✔
EDS do Brasil	São Paulo	Av. Pres. Juscelino Kubistcheck, 1830 Torre 4 - 5º andar	11 3707-4100	www.eds.com		✔	✔			✔
Ética Tecnologia	São Paulo	Rua Nova York, 945 – Brooklin – CEP:04560-002	11 5093-3025	www.etica.net	✔		✔		✔	✔
Getronics ICT Solutions and Services	São Paulo	Rua Verbo Divino, 1207 – CEP: 04719-002	11 5187-2700	www.getronics.com/br			✔		✔	✔
Hewlett-Packard Brasil Ltda.	São Paulo	Av. das Nações Unidas, 12.901, 25º andar – CEP: 04578-000	11 5502-5000	www.hp.com.br	✔		✔	✔	✔	✔
IBM Brasil Ltda.	São Paulo	Rua Tutóia, 1157 – CEP: 04007-900	0800-7074 837	www.br.ibm.com	✔		✔		✔	✔
iFractal	São Paulo	Rua Fiação da Saúde, 145, Conj. 66 – Saúde – CEP: 04144-020	11 5078-6618	www.ifractal.com.br			✔		✔	✔
Integral	São Paulo	Rua Dr. Gentil Leite Martins, 295, 2º andar Jd. Prudência – CEP: 04648-001	11 5545-2600	www.integral.com.br	✔				✔	
Itautec S.A.	São Paulo	Av. Paulista, 2028 – CEP: 01310-200	11 3543-5543	www.itautec.com.br	✔	✔	✔		✔	✔
Kenos Consultoria	São Paulo	Av: Fagundes Filho, 13, Conj 53 – CEP: 04304-000	11 40821305	www.kenos.com.br					✔	✔
Konsultex Informatica	São Paulo	Av. Dr. Guilherme Dumont Villares, 1410 6 andar, CEP: 05640-003	11 3773-9009	www.konsultex.com.br			✔		✔	✔
Linux Komputer Informática	São Paulo	Av. Dr. Lino de Moraes Leme, 185 – CEP: 04360-001	11 5034-4191	www.komputer.com.br	✔		✔		✔	✔
Linux Mall	São Paulo	Rua Machado Bittencourt, 190, Cj. 2087 – CEP: 04044-001	11 5087-9441	www.linuxmall.com.br	✔			✔	✔	
Livraria Tempo Real	São Paulo	Al. Santos, 1202 – Cerqueira César – CEP: 01418-100	11 3266-2988	www.temporeal.com.br				✔	✔	✔
Locasite Internet Service	São Paulo	Av. Brigadeiro Luiz Antonio, 2482, 3º andar – Centro – CEP: 01402-000	11 2121-4555	www.locasite.com.br	✔				✔	✔
Microsiga	São Paulo	Av. Braz Leme, 1631 – CEP: 02511-000	11 3981-7200	www.microsiga.com.br			✔		✔	✔
Novatec Editora Ltda.	São Paulo	Rua Luis Antonio dos Santos, 110 – Santana – CEP: 02460-000	11 6979-0071	www.novateceditora.com.br				✔		
Novell América Latina	São Paulo	Rua Funchal, 418 – Vila Olímpia	11 3345-3900	www.novell.com/brasil			✔		✔	✔
Oracle do Brasil Sistemas Ltda.	São Paulo	Av. Alfredo Egídio de Souza Aranha, 100 – Bloco B – 5º andar – CEP: 04726-170	11 5189-3000	www.oracle.com.br					✔	✔
Proelbra Tecnologia Eletrônica Ltda.	São Paulo	Av. Rouxinol, 1.041, Cj. 204, 2º andar Moema – CEP: 04516-001	11 5052- 8044	www.proelbra.com.br	✔		✔			✔
Provider	São Paulo	Av. Cardoso de Melo, 1450, 6º andar – Vila Olímpia – CEP: 04548-005	11 2165-6500	www.e-provider.com.br			✔		✔	✔
Red Hat Brasil	São Paulo	Av. Brigadeiro Faria Lima, 3900, Cj 81 8º andar Itaim Bibi – CEP: 04538-132	11 3529-6000	www.redhat.com.br			✔		✔	✔
Samurai Projetos Especiais	São Paulo	Rua Barão do Triunfo, 550, 6º andar – CEP: 04602-002	11 5097-3014	www.samurai.com.br			✔		✔	✔
SAP Brasil	São Paulo	Av. das Nações Unidas, 11.541, 16º andar – CEP: 04578-000	11 5503-2400	www.sap.com.br			✔		✔	✔
Simples Consultoria	São Paulo	Rua Mourato Coelho, 299, Cj. 02 Pinheiros – CEP: 05417-010	11 3898-2121	www.simplesconsultoria.com.br			✔		✔	✔
Smart Solutions	São Paulo	Av. Jabaquara, 2940 cj 56 e 57	11 5052-5958	www.smart-tec.com.br		✔	✔		✔	✔
Snap IT	São Paulo	Rua João Gomes Junior, 131 – Jd. Bonfiglioli – CEP: 05299-000	11 3731-8008	www.snapit.com.br			✔		✔	✔
Stefanini IT Solutions	São Paulo	Av. Brig. Faria Lima, 1355, 19º – Pinheiros – CEP: 01452-919	11 3039-2000	www.stefanini.com.br			✔		✔	✔
Sun Microsystems	São Paulo	Rua Alexandre Dumas, 2016 – CEP: 04717-004	11 5187-2100	www.sun.com.br	✔		✔		✔	✔
Sybase Brasil	São Paulo	Av. Juscelino Kubitschek, 510, 9º andar Itaim Bibi – CEP: 04543-000	11 3046-7388	www.sybase.com.br					✔	✔
The Source	São Paulo	Rua Marquês de Abrantes, 203 – Chácara Tatuapé – CEP: 03060-020	11 6698-5090	www.thesource.com.br			✔		✔	✔
Unisys Brasil Ltda.	São Paulo	R. Alexandre Dumas 1658 – 6º, 7º e 8º andares – Chácara Santo Antônio – CEP: 04717-004	11 3305-7000	www.unisys.com.br	✔		✔		✔	✔
Utah	São Paulo	Av. Paulista, 925, 13º andar – Cerqueira César – CEP: 01311-916	11 3145-5888	www.utah.com.br			✔		✔	✔
Visuelles	São Paulo	Rua Eng. Domicio Diele Pacheco e Silva, 585 – Interlagos – CEP: 04455-310	11 5614-1010	www.visuelles.com.br			✔		✔	✔
Webnow	São Paulo	Av. Nações Unidas, 12.995, 10º andar, Ed. Plaza Centenário – Chácara Itaim – CEP: 04578-000	11 5503-6510	www.webnow.com.br	✔		✔		✔	
WRL Informática Ltda.	São Paulo	Rua Santa Ifigênia, 211/213, Box 02– Centro – CEP: 01207-001	11 3362-1334	www.wrl.com.br	✔		✔		✔	
Systech	Taquaritinga	Rua São José, 1126 – Centro - Caixa Postal 71 – CEP: 15.900-000	16 3252-7308	www.systech-ltd.com.br	✔	✔			✔	
2MI Tecnologia e Informação	Embu	Rua José Bonifácio, 55 – Jd. Independência – SP CEP: 06826-080	11 4203-3937	www.2mi.com.br		✔	✔		✔	✔

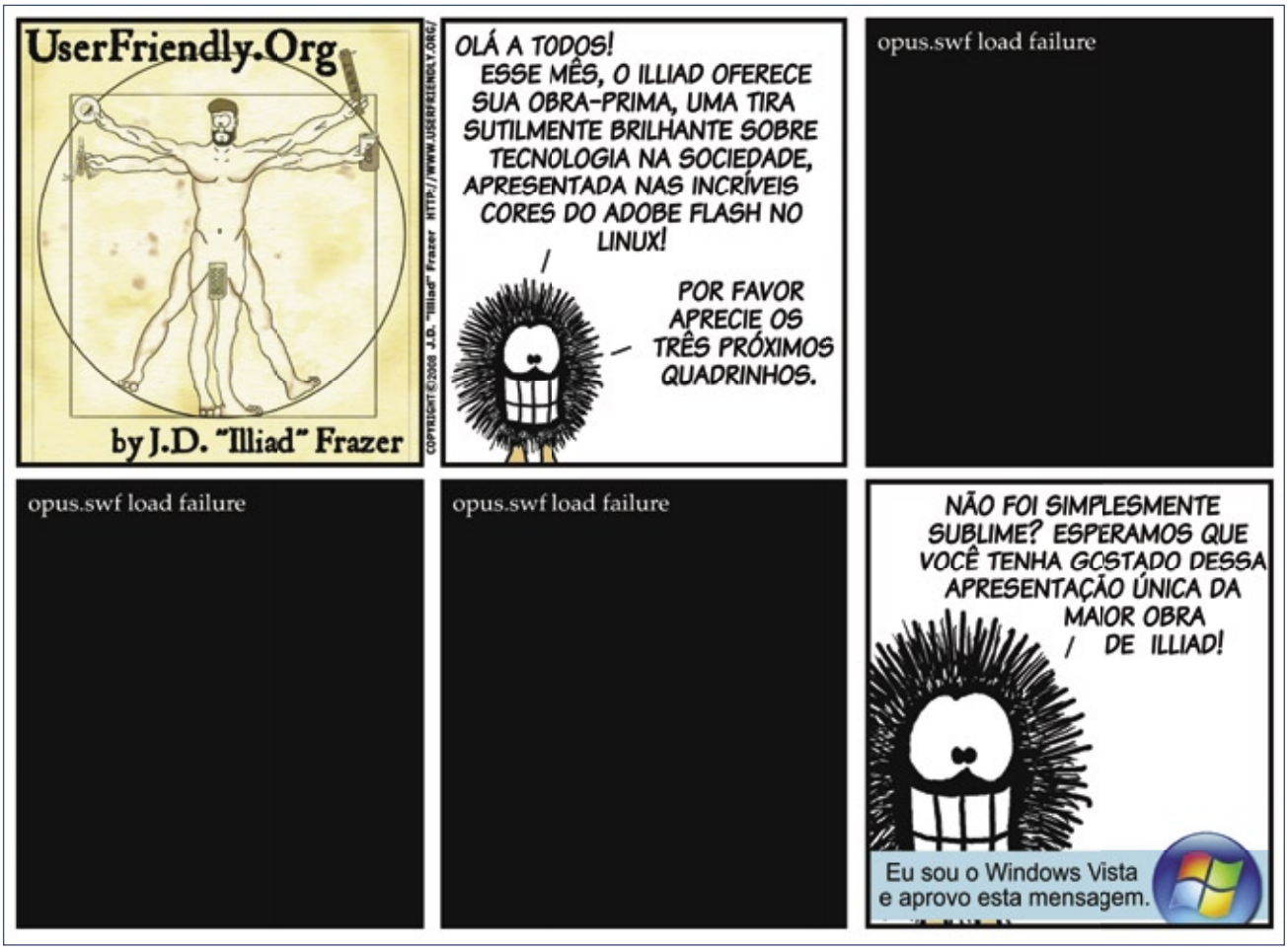
© Linux New Media do Brasil Editora Ltda.

Calendário de eventos

Evento	Data	Local	Website
Yahoo! Open Hack Day	8 e 9 de novembro	São Paulo, SP	www.hackday.org/
Conferência Blender Pro	9 de novembro	Belo Horizonte, MG	www.blender.pro.br/
PHP Conference Brasil	27, 28 e 29 de novembro	Osasco, SP	www.phpconf.com.br
The Developer's Conference	29 de novembro	Florianópolis, SC	www.thedevelopers conference.com.br

Índice de anunciantes

User Friendly – Os quadrinhos mensais da Linux Magazine



© Linux New Media do Brasil Editora Ltda.

Snow666

Mar del Plata, Argentina

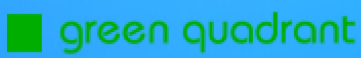
02 - 17 August 2008

http://debconf8.debconf.org

DebConf 8

MAR DEL PLATA - ARGENTINA

The Debian project would like to thank the generous sponsors who helped make its 2008 conference.



© Linux New Media do Brasil Editora Ltda.

Snow666

PREVIEW

Na Linux Magazine #49

DESTAQUE

TI verde

O novo ambiente móvel de trabalho e o aumento no cu energia vêm ocasionando inovações no campo da efi gética e da redução do consumo. Usuários de laptops desejam uma maior duração da bateria após uma recarga e os gerentes de TI precisam reduzir a parcela dos servidores na conta de luz.

Além da virtualização dos servidores e de sua migração para a "nuvem" fora da empresa, os próprios PCs podem contribuir para a diminuição do gasto energético da estrutura de TI da empresa.

Na Linux Magazine 49, mostraremos como medir e reduzir o consumo de energia dos PCs e explicaremos como utilizar a computação em nuvem, ou *cloud computing*, para aumentar a eficiência energética da empresa. Ensinaremos ainda como usar o recurso *Elastic Computer Cloud* (EC2) da Amazon para tirar o melhor proveito dos recursos computacionais disponíveis sob demanda e com altíssima disponibilidade. ■

SEGURANÇA

Snort

Varreduras de portas, ou *port scans*, muitas vezes começam a ocorrer imediatamente no momento em que conectamos um servidor à Internet. Nesse cenário tão hostil, uma rede pode ser invadida rapidamente, tornando-se uma plataforma de lançamento de ataques contra outras redes ou até para cometer crimes gravíssimos.

Um bom sistema de segurança, portanto, é fundamental, e o famoso *Snort* constitui uma ótima opção de IDS de código aberto e altamente competente. Aprenda a instalar e configurar adequadamente o Snort para manter sua rede a salvo dos cibercriminosos. ■

Na EasyLinux #14

Monitores gigantes

Os monitores LCD de 19 polegadas já têm preços bem melhores que há um ano. Será que já chegou o momento de você comprar aquele monitor cinematográfico? Quais são as vantagens e desvantagens do LCD em relação aos antigos monitores de tubo? Até onde 21 polegadas valem mais que 19? Na Easy Linux 14, vamos comparar marcas, modelos e tecnologias de monitores à venda no Brasil para orientar suas compras. ■

A melhor parte de todos os sistemas

Empresas como Apple e Microsoft investem pesado em design para deixarem seus sistemas mais atraentes. Como resultado, tanto o Mac OS quanto o Windows Vista têm forte apelo visual. Porém, engana-se quem pensa que é impossível alcançar um grau de beleza semelhante no Linux. Na Easy Linux 14, vamos mostrar o caminho das pedras para deixar seu Linux com a cara do Mac OS X, do Vista e do Windows XP, seja por pura diversão ou para facilitar o uso do Linux por quem já está habituado a esses sistemas e tem dificuldade de adaptação ao pingüim. ■

© Linux New Media do Brasil Editora Ltda.

Snow666

© Linux New Media do Brasil Editora Ltda.

Snow666

IBM

ECO CONSCIENTE.
CFO CONSCIENTE.

O Smart SOA™ da IBM pode ajudar você a aumentar o controle e a visibilidade de seus processos de negócios e ao mesmo tempo reduzir o impacto da emissão de carbono. Com a ajuda da IBM, empresas como o Citigroup reduziram de duas semanas para dois dias o tempo de processamento de suas aplicações. A eficiência cresce. Os custos com energia diminuem. Um mundo mais verde começa com empresas mais verdes. Empresas mais verdes começam com a IBM.

SISTEMAS. SOFTWARE. SERVIÇOS. PARA UM MUNDO MAIS VERDE.
Assista ao nosso Webcast sobre processos mais verdes em **ibm.com**/green/br/soa

IBM, o logo IBM, ibm.com e Smart SOA são marcas registradas ou de titularidade da International Business Machines Corporation nos Estados Unidos da América, em outros países ou em ambos. Caso estes e outros termos protegidos, na primeira vez em que aparecem nesta informação, estejam marcados com os símbolos ® ou ™, isto significa que os mesmos constituem marcas registradas ou marcas comerciais de titularidade da IBM nos Estados Unidos da América na ocasião em que esta informação foi publicada. Tais marcas podem também constituir marcas registradas ou marcas comerciais em outros países. Uma relação atualizada das marcas de titularidade da IBM está disponível no Web site "Informações sobre direitos autorais e marcas" ibm.com/legal/copytrade.shtml

© Burn Now Media do Brasil Editora Ltda.