

MADDOG p.30
Formatos de arquivos de imagens ultrapassados

TAURION p.32
Situação atual do ODF e do OpenXML

LOJA DE APLICATIVOS p.16
São o futuro da distribuição de softwares?

74 Janeiro 2011



LINUX MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

Interoperabilidade

MINIMIZE OS PROBLEMAS DE CONVIVÊNCIA ENTRE SISTEMAS OPERACIONAIS E INTEGRE RECURSOS DO WINDOWS E DO LINUX p.33

- » Diretórios virtuais p.34
- » Acesso a partições NTFS a partir do Linux p.42
- » Samba com LDAP p.44
- » Administração centralizada com OpenLDAP p.48
- » Gerenciamento de LDAP com G0sa² p.52
- » Integração: Samba, LDAP e G0sa² p.56

SUA REDE ESTÁ SEGURA? p.62

Conheça algumas ferramentas que os agressores utilizam para fugir da detecção de intrusão

NTOP p.68

Descubra problemas de lentidão e monitore a rede com esta poderosa ferramenta

VEJA TAMBÉM NESTA EDIÇÃO:

- » VoIP com Asterisk – parte III p.58
- » Programação Shell Script: pipes p.72
- » Monitoramento de daemons p.75



exemplar de
Assinante
venda proibida



MELHOR QUE SERVIDOR DEDICADO. É CLOUD SERVER DA REDEHOST.



O Cloud Server da RedeHost é a solução com melhor relação custo/benefício para aplicações que necessitem de um servidor dedicado. Por ser desenvolvido sobre conceitos de Cloud Computing utiliza da alta disponibilidade oferecida pela "nuvem computacional" com flexibilidade de expandir a capacidade de seu servidor conforme a necessidade de seu negócio.

■ ESCALABILIDADE

Aumente os recursos de processamento, memória, disco, e banda quando desejar.

■ PERFORMANCE

Memória, disco e banda 100% garantidos.

■ DISPONIBILIDADE

Em caso de falha os recursos são automaticamente realocados.

■ MENOR CUSTO

Melhor que um servidor dedicado com menor custo.

www.redehost.com.br

SP <small>11</small> 4062.0909	RJ <small>21</small> 4062.0909	MG <small>31</small> 4062.0909
RS <small>51</small> 4062.0909	SC <small>48</small> 4062.0909	PR <small>41</small> 4062.0909

RedeHost

Expediente editorial

Diretor Geral

Rafael Peregrino da Silva
rperegrino@linuxmagazine.com.br

Editora

Flávia Jobstraibizer
fjobs@linuxmagazine.com.br

Editora de Arte

Paola Viveiros
pviveiros@linuxmagazine.com.br

Colaboradores

Alexandre Borges, Augusto Campos, Marcos Amorim, Adriano Matos Meier, Cesar Taurion, Kurt Seifried, e Harald Zisler.

Tradução

Pablo Hess

Editores internacionais

Uli Bantle, Andreas Bohle, Jens-Christoph Brendel, Hans-Georg Eßer, Markus Feilner, Oliver Frommel, Marcel Hilzinger, Mathias Huber, Anika Kehler, Kristian Klübing, Jan Kleinert, Daniel Kottmair, Thomas Leichtenstern, Jörg Luther, Nils Magnus.

Anúncios:

Rafael Peregrino da Silva (Brasil)
anuncios@linuxmagazine.com.br
Tel.: +55 (0)11 3675-2600

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

Amy Phalen (América do Norte)
aphalen@linuxpromagazine.com

Hubert Wiest (Outros países)
hwiest@linuxnewmedia.de

Diretor de operações

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.es – Espanha
www.linux-magazine.pl – Polônia
www.linux-magazine.co.uk – Reino Unido
www.linuxpromagazine.com – América do Norte

Apesar de todos os cuidados possíveis terem sido tomados durante a produção desta revista, a editora não é responsável por eventuais imprecisões nela contidas ou por consequências que advieram 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.

*Rua São Bento, 500
Conj. 802 – Sé
01010-001 – São Paulo – SP – Brasil
Tel.: +55 (0)11 3675-2600*

Direitos Autorais e Marcas Registradas © 2004 - 2011 –

Linux New Media do Brasil Editora Ltda.

*Impressão e Acompanhamento: RR Donnelley
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

Decisores

No âmbito das atividades precípuas para manutenção das operações e da saúde financeira da empresa responsável pela publicação da Linux Magazine, a Linux New Media do Brasil, uma das que demandam especial atenção é a comercialização de publicidade, seja ela nos veículos impressos ou onlines da editora. E, apesar da estranheza inicial de gestores de marketing em empresas e agências de publicidade por ocasião de um primeiro contato com o título da revista – com a consequente afirmação: “Não tenho nada para Linux!” – após um diálogo inicial, fica claro que o título da publicação e a veiculação de publicidade nela não têm necessariamente muito a ver com a existência de produtos e serviços em Linux ou em Software Livre e de Código Aberto (apesar de ofertas de soluções nesses segmentos serem ainda mais aderentes ao perfil do nosso leitor). Muito mais do que isso, o que conta – ou deveria contar – realmente para anunciantes da Linux Magazine é a possibilidade de falar com decisores: aquelas pessoas-chave dentro das empresas, responsáveis pela contratação de soluções e serviços e pela aquisição de produtos.

Isso dá o que pensar: via de regra, os anunciantes, especialmente os de produtos e serviços de tecnologia, tendem a imaginar que os veículos em que anunciam devem ser dirigidos a um leitor cujo cargo esteja situado no que se convencionou chamar de *C-level* – CIOs, CEOs, COOs e CFOs (respectivamente, diretores de tecnologia, executivo, de operações e financeiro); esperam, no mínimo, que tais publicações atinjam a camada intermediária da gerência de tecnologia. A ideia parece infalível: se expõe meus produtos e serviços ao expoente máximo da cadeia de decisão, é mais provável que o anúncio gere retorno (leia-se, negócios). Em que pese a força inicial dessa ideia, ela tem um componente simplista e falacioso que mascara a face do verdadeiro decisior dentro das empresas, especificamente no departamento de tecnologia: o administrador de redes e sistemas.

É esse o profissional que, efetivamente, “faz acontecer” dentro do setor de tecnologia da empresa. Os bons gestores de tecnologia de mais alto nível já ocuparam essa posição por anos no passado, e justamente por isso ascenderam hierarquicamente dentro das companhias. Hoje, esses profissionais de mais alto escalão estão principalmente envolvidos com as estratégias “macro” de definição do tipo de tecnologia de que a empresa necessita para funcionar de maneira mais eficiente. Entretanto, quem homologa, analisa, procura, compara, sugere e, finalmente, implementa soluções e configura produtos de tecnologia dentro do ambiente corporativo é o administrador de redes e sistemas. E, normalmente, o administrador que se destaca é aquele que detém o melhor domínio e entendimento das tecnologias de que a empresa precisa para ser bem sucedida em seu segmento de atuação – e isso inequivocamente passa pela necessidade da existência de um profundo conhecimento do Linux e do Software Livre, que requer mais do que simplesmente saber apontar e clicar: há que se deter o conhecimento conceitual de todas as tecnologias com a qual se tem contato.

Assim, esse profissional não aceita a adoção de soluções *top-down*, e está não só e intrinsecamente envolvido em toda a cadeia decisória dentro da empresa, como é efetivamente aquele que dirige todo o processo de aquisição de produtos e soluções e de contratação de serviços, desonerando o seu superior. Vida longa ao administrador! ■

Rafael Peregrino da Silva
Diretor de Redação



CAPA

Convivência harmoniosa

33



Diretórios virtuais

34

Aprenda a integrar a autenticação no Linux com múltiplos domínios Microsoft Active Directory por meio do Fedora 389 Directory Server, com encadeamento e autenticação de tráfego.



Obstáculos superados

42

Se você precisa acessar partições NTFS do Windows XP, Vista ou Seven a partir de um sistema GNU/Linux, aprenda como utilizar o Ntfs-3g, que permite acesso de leitura e escrita a partições NTFS com rapidez e agilidade.



União perfeita

44

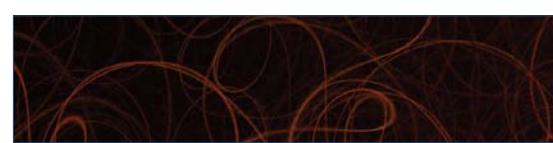
A união das poderosas tecnologias Samba e LDAP, proporciona agilidade e simplicidade no gerenciamento de usuários de redes Linux e Windows.



Administração centralizada com OpenLDAP

48

Entenda como funciona o LDAP e aprenda como montar seu próprio servidor, com o propósito de usufruir deste maravilhoso serviço.



Mais que uma interface bonita

52

Poderosa ferramenta para gerenciamento de contas e sistemas de bancos de dados LDAP.



Administração versátil

56

Você já aprendeu como instalar e configurar os aplicativos Samba, OpenLDAP e a interface web GOsia. Agora aprenda a integrar todos eles de uma só vez, com a finalidade de obter um sistema completo e versátil.

COLUNAS

Klaus Knopper	10
Charly Kühnast	12
Zack Brown	14
Augusto Campos	16
Kurt Seifried	20
Alexandre Borges	22

NOTÍCIAS

Geral	24
♦ Dell lança notebooks Inspiron 14 com Ubuntu	
♦ Novo cliente de torrents Tribler 5.3 facilita a vida do usuário	
♦ iPad chinês vem com câmera e sistema Android	
♦ Google vai distribuir notebooks para testar sistema operacional na nuvem	
♦ Netbooks distribuídos à rede pública de ensino portarão o Mandriva Linux	



CORPORATE

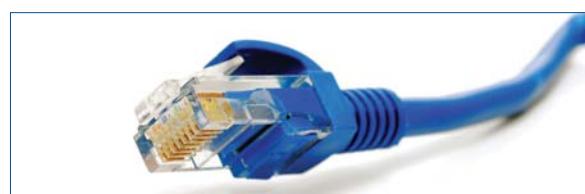
Notícias	26
♦ Oracle pede à Apache que volte ao comitê executivo do Java	
♦ BMC Software e Salesforce.com ampliam parceria para cloud computing	
♦ Red Hat adquire Makara e acelera estratégia de PaaS	
♦ Executivo confirma que Microsoft tentou comprar Facebook por US\$ 15 bilhões	

Coluna: Jon "maddog" Hall	30
---------------------------	----

Coluna: Cesar Taurion	32
-----------------------	----

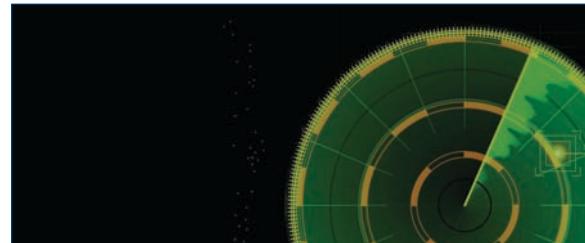
TUTORIAL

VoIP com Asterisk – parte III	58
O sistema telefônico ultrapassado, presente até pouco tempo atrás nas empresas, é prolífico em cobranças: cada novo recurso ativado requer uma nova ativação de serviço, com o preço adicionado ao pagamento mensal. É hora de mudar. É hora de criar sua própria central VoIP.	



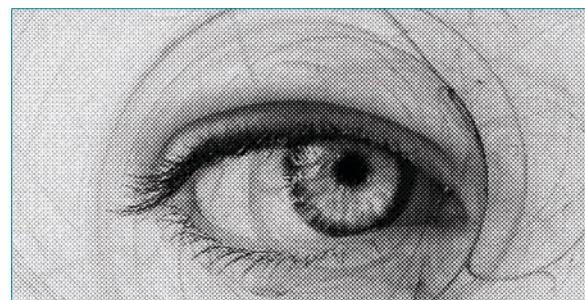
SEGURANÇA

Sob o radar	62
Ferramentas de detecção de intrusão como o Snort ajudam a rastrear invasores, mas é melhor não ficar confortável demais. Conheça algumas ferramentas que os agressores utilizam para fugir da detecção de intrusão.	



REDES

De olho na rede	68
Descubra o que está gerando lentidão em sua rede, a origem e o destino do tráfego, protocolos utilizados e muito mais com o NTOP, ferramenta simples e útil.	



PROGRAMAÇÃO

Shell script: trabalhando com pipes	72
Ferramentas especiais do shell auxiliam na combinação de comandos para criar aplicativos de maior complexidade.	



Monitore os daemons	75
Os administradores geralmente escrevem programas personalizados de monitoramento para garantir que seus daemons ofereçam a funcionalidade pretendida. Mas as ferramentas simples do shell também são bem adaptadas para essa tarefa, e não apenas para sistemas com poucos recursos.	

SERVIÇOS

Editorial	03
Emails	06
Linux.local	78
Preview	82

Emails para o editor

Permissão de Escrita

Proteção contra invasão ☐

Olá pessoal da Linux Magazine. Há muito tempo sou leitor da revista e possuo (quase) todos os exemplares. Gostaria de sugerir que publiquem mais artigos sobre proteção contra invasão, como os publicados na edição #22, sobre invasão. Obrigado!

Edson M. Macedo

Resposta

Edson, agradecemos a sua fidelidade como leitor. Não deixe de completar a sua coleção de revistas! Aproveitamos para lembrar que a edição #64 da revista, também veio recheada de artigos sobre segurança. Coincidente mente, nesta edição da **Linux Magazine**, também estamos publicando um artigo tratando sobre o tema detecção de intrusão, na seção de Tutoriais. Boa leitura!



Escreva para nós! ☐

Sempre queremos sua opinião sobre a Linux Magazine e nossos artigos. Envie seus emails para cartas@linuxmagazine.com.br e compartilhe suas dúvidas, opiniões, sugestões e críticas. Infelizmente, devido ao volume de emails, não podemos garantir que seu email seja publicado, mas é certo que ele será lido e analisado.

Entrevistas ☐

Sou leitor da **Linux Magazine** aqui em Portugal e gosto muito da revista. Gostaria de ver mais entrevistas com empresários, empresas e profissionais do mercado de TI brasileiro.

Manoel Pascoal de Alencar

Resposta

Caro Manoel, estimamos muito nossos leitores (cada vez em maior quantidade) de Portugal. Aproveitamos para agradecer ao país o prestígio que nos dá. Certamente traremos mais entrevistas durante este ano de 2011, aguarde!



Gerencie o seu servidor
Linux

A PARTIR DE
59,99
MÊS

Cloud Hosting

HOSPEDAGEM NA NUVEM

IDEAL PARA:

- Sites que requerem a instalação de componentes específicos, como bibliotecas de programação
 - Sites de missão crítica ou de alto tráfego
 - Revendas de hospedagem de sites



CentralServer

0800 701 1993 • www.centralserver.com.br



A Globo.com completou 10 anos.

E a história dessa marca foi construída
por muitas marcas.

9



co



s
g
l
o
b
o
.
c
o
m

Esses 10 anos foram escritos pelo Globoesporte.com, pela Revista Época, pelo Multishow, pelo BBB, pelo Jornal Nacional, pelo EGO, pela CBN, pelas novelas da Globo, pelo O Globo, pela Quem, pelo Paparazzo, pelo G1, pelo GNT, pelo Zorra Total, pelo Jornal Hoje e por tantas outras marcas que formam uma única grande marca: a Globo.com. Mas essa história não acabou. Isso é só o começo. **Globo.com, 10 anos. Vem muita coisa por aí.**

anos
globo
.com



Coluna do Klaus

Pergunte ao Klaus

Klaus Knopper responde suas dúvidas de Linux.

Configuração de hora

Estou com problemas para configurar a hora e o fuso horário. Consigo configurá-los, mas eles sempre voltam a ficar incorretos na próxima vez em que logo na máquina.

Resposta

O computador possui dois relógios: o da placa-mãe (também chamado de “hora da BIOS”) e um relógio virtual que só é executado como serviço do sistema enquanto o sistema operacional está em funcionamento.

Aparentemente, você conseguiu configurar a hora corretamente no relógio do sistema. Eu uso o comando `rdate ntp.fu-berlin.de` para isso. Para salvar a hora no relógio da placa-mãe do seu computador – e fazê-la persistir até a próxima reinicialização – é preciso executar o comando `hwclock -w` como usuário `root` (ou com o comando `sudo` na frente). Se sua configuração local estiver usando a hora universal (isto é, o fuso horário UTC), adicione a opção `-u` para acertar o desvio do seu fuso horário.

Na próxima reinicialização, a maioria das distribuições Linux lerá a hora a partir do relógio persistente e a utilizará no relógio do sistema. Após salvar corretamente a hora, ela deve funcionar novamente.

Privilégios de root

Como posso fazer o Knoppix iniciar com o usuário `root` logado no ambiente gráfico ou algo com privilégios semelhantes?

Resposta

Privilégios de sistema significam, na maioria das distribuições Linux modernas, que você pode fazer menos, e não mais, pois os programas estão cientes dos riscos

potenciais e se recusam a iniciar no ambiente gráfico se você for `root`.

O Knoppix utiliza uma técnica diferente: você é logado automaticamente como usuário normal, mas esse usuário é membro de todos os grupos necessários para acessar dispositivos como som, vídeo e scanners. Se você realmente precisar modificar o sistema (como no comando `hwclock` mencionado na questão anterior), pode se tornar `root` para um único comando, digitando `sudo comando` sem necessidade de fornecer senha.

Unir PDFs

Preciso unir vários arquivos PDF em um único arquivo, mas as ferramentas como o utilitário `mpage` adicionam bordas ou desorganizam a geometria da página. Não existe nenhuma forma de simplesmente concatenar arquivos PDF no Linux?

Resposta

O mecanismo padrão de manipulação de Postscript (PS), Ghostscript (GS), permite ler vários arquivos PDF e PS e gravá-los em um único. Como script de shell (chame-o de `pdfcat`), ele poderia ser assim:

```
#!/bin/bash
gs -q -sPAPERSIZE=a4 -dNOPAUSE -dBATCH ➔
-aDEVICE=pdfwrite -sOutputFile=- "$@"
```

Este script poderia ser executado da seguinte forma:

```
pdfcat arquivo1.pdf arquivo2.pdf arquivo3.pdf ... > ➔
todos.pdf
```

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

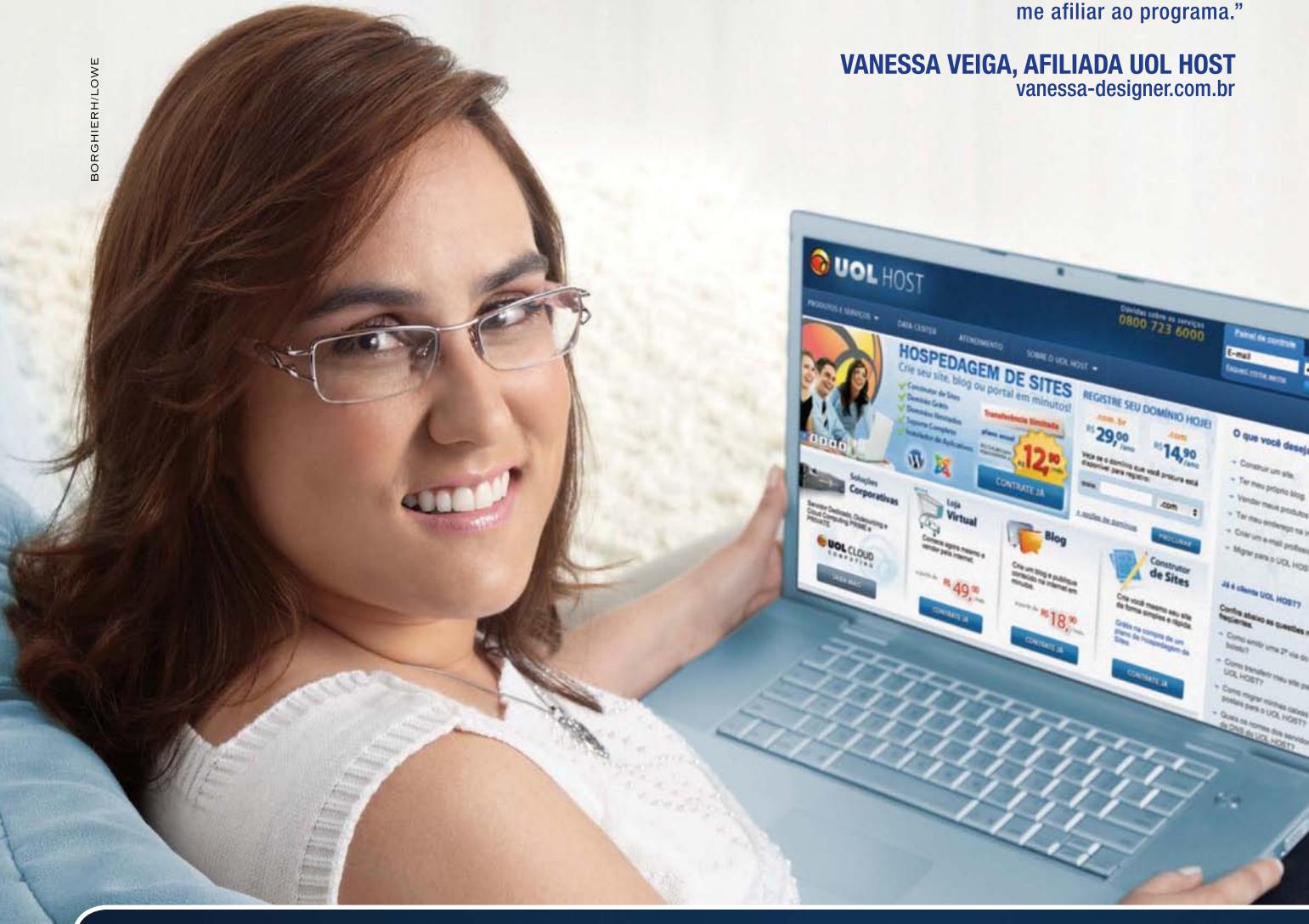
Programa de Afiliados

UOL Host. Participe, ganhe dinheiro* e indique qualidade para seus clientes.

BORGHIERI/LOWE

“Eu trabalho com desenvolvimento web há mais de 10 anos e muitos dos meus clientes tinham problemas constantes com servidores de hospedagem e e-mails corporativos. Após a parceria com o UOL HOST, nunca mais tive dores de cabeça e, por isso, decidi me afiliar ao programa.”

VANESSA VEIGA, AFILIADA UOL HOST
vanessa-designer.com.br



Ganhe dinheiro indicando aos seus clientes produtos com a qualidade e a credibilidade UOL.

Participe do Programa de Afiliados UOL HOST. Além de ter o atendimento diferenciado e a credibilidade do UOL, o Programa pode pagar 30 reais* por sua indicação, mais 10% da receita total** gerada por ela. Ou seja, dinheiro direto na sua conta corrente por indicar a melhor hospedagem.

*Após o 3º pagamento recebido pelo UOL HOST
**Consulte as informações no hotsite do programa: uolhost.com.br/afiliados

uol.com.br/host



UOL HOST



Coluna do Charly

O mundo é um palco

Shakespeare Programming Language: a linguagem de programação definitiva para leitores lentos de páginas.

Mesmo que a frase “Ser ou não ser” (do inglês “To be or not to be”) possa ser traduzida para uma expressão regular como `/(bb|[^b]{2})/`, a ligação entre Shakespeare e os administradores de sistemas não é imediatamente aparente. Então, deixemos o Perl e terminal Bash de lado por alguns minutos e vamos conhecer uma linguagem de programação cheia de drama e poesia.

A estrutura da linguagem de programação Shakespeare (SPL) [1] segue a de uma peça de teatro. O desenvolvedor declara as variáveis, que aparecem na forma de personagens de um drama:

Caesar, a successful and soon dead Roman emperor
Othello, a Venetian general

O parser se lembra dos nomes e os utiliza como variáveis inteiras e como não avalia o texto após a vírgula, é possível fazer uma descrição com todos os floreios que se desejar.

A técnica de dividir o código do programa em atos e cenas também é típica do teatro. Esses divisores não apenas organizam visivelmente o programa como também marcam o equivalente teatral do comando `go-to`:

Act I: A battle of words
Scene I: Caesar insults Othello

Antes de atribuir um valor a uma variável, o personagem primeiramente precisa entrar no palco:

[Enter Caesar and Othello]
Caesar: You stupid rotten beggar!

O valor atribuído à variável é definido pela amistosidade das falas do ator. Substantivos representam um valor 1 caso a fala seja amigável ou neutra, ou -1 se as palavras possuírem conotação negativa.

No exemplo anterior o valor é -1. Cada adjetivo anterior multiplica o valor por dois. Em outras palavras, *Stupid rotten beggar* significa $-1*2*2=-4$. Como Caesar também está falando com Othello, um valor de -4 é atribuído à variável *Othello*.

Claro que a saída é igualmente elegante: o comando `Open your heart!` gera uma saída de valor numérico. `Speak your mind!` exibe as letras cujo valor ASCII corresponde a esse número. Comandos `go-to` são igualmente fáceis:

Othello: Let us then proceed to Act II!

O personagem pode adicionar uma condição ao comando `go-to` fazendo uma pergunta, o que faz uma comparação das variáveis e pula para uma cena ou ato, dependendo dos resultados:

Caesar: Am I better than you?

Othello: If not, let us return to Scene I.

Não há exatamente um compilador SPL, mas existe o `spl2c`, um tradutor de SPL para C que foi escrito em Flex e Bison. Devido a sua natureza poética, programas na linguagem Shakespeare Programming podem ser incrivelmente longos. Até um clássico “Hello world” precisa de algumas centenas de linhas. ■

Mais informações

[1] Linguagem de programação Shakespeare:
<http://shakespearelang.sourceforge.net>

Charly Kühnast é administrador de sistemas Unix no data center de Moers, Alemanha. Suas tarefas incluem segurança e disponibilidade de firewalls e DMZ. Ele divide seu tempo livre nos setores quente, molhado e oriental, nos quais se diverte com culinária, aquários de água doce e aprendizado de japonês, respectivamente.



Segurança de Rede Integrada



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

Linha de Appliances

Porte de LANs:

Pequenas	Médias	Grandes	Enterprise
1 a 50 users	até 1.000	até 5.000	A partir 10.000

Linha de Appliances: Edge, XTM2, Core, XTM5, Peak, XTM8 e XTM10

Importante: Consulte canais certificados para dimensionar o(s) appliance(s) necessário(s) para seu projeto.

- Múltiplos Links de Internet (até 16)
- Load Balancing
- Drag-N-Drop VPN
- VPN Failover
- Traffic Shaping
- Qos
- VLANs
- Proxy Server
- 100% Interface Gráfica

- Server Load Balancing
- Suporte e Segurança à Voip
- Relatórios
- Servidores de Log
- Servidor de Quarentena
- Monitoramento "real time"
- Alta Disponibilidade
- Gerenciamento Centralizado
- Outras



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

Consulte políticas especiais:

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



Coluna do Zack

Crônicas do kernel

O cronista Zack Brown faz um relatório das mais recentes notícias, visões, dilemas e desenvolvimentos dentro da comunidade do kernel Linux.

Novo union filesystem

Miklos Szeredi anunciou sua própria tentativa de criar um *union filesystem*, que em outras palavras significa: dois sistemas de arquivos distintos que se comportam como um único. Os dois sistemas de arquivos são chamados de *upper* (superior) e *lower* (inferior), de forma que se um arquivo em um sistema de arquivos possuir o mesmo nome de um arquivo no outro sistema, somente aquele do sistema superior será exibido para o usuário. Porém, se um diretório em um sistema de arquivos tiver o mesmo nome de um diretório no outro, os dois diretórios serão apresentados como um único. Somente os arquivos possuem esse método de seleção de superior e inferior. Neil Brown explicou essas ideias e várias outras coisas na documentação que postou em resposta ao código de Miklos e este ficou muito feliz com isso – na verdade, a documentação de Neil imediatamente ajudou a expor alguns bugs em seu código, que ele prometeu corrigir no mesmo momento.

Após escrever a documentação, o passo seguinte de Neil foi criticar o código em si, e ele e Miklos tiveram um ativo debate sobre várias questões técnicas, essencialmente esclarecendo por que certas coisas não funcionariam e por que outras coisas eram mais fáceis do que haviam suposto. Al Viro e vários outros se juntaram à conversa e a discussão passou por toda a lista.

Verificador de console

O Dr. Werner Fink programou um recurso para adicionar um arquivo /proc/tty/consoles no sistema, que mostraria os dispositivos de caracteres em uso pelo console do sistema. Então, por exemplo, /dev/ttys0 e /dev/ttys0 podem ser listados em /proc/tty/consoles. Não houve muitos comentários sobre o código, nem qual-

quer questionamento; então, ainda é um mistério se o recurso será incluído no kernel.

Quando kernels são liberados

Piotr Hosowicz escreveu um script para ser informado quando um novo kernel estiver disponível. Porém, o script fazia requisições aos servidores do site kernel.org, o que causava problemas porque às vezes ele recebia informações do servidor mestre, e outras vezes de um dos servidores em espelho. O resultado foi que algumas vezes seu script relatava uma nova versão do kernel quando ela não existia. Ele pediu ajuda para identificar o servidor mestre de fato; mas Jiri Kosina respondeu que Piotr não estava usando a melhor técnica. Jiri recomendou executar `finger @kernel.org` para obter as informações mais atualizadas. Mas Arnd Hannemann também afirmou que essa também não é a forma correta. Aparentemente, o *daemon finger* estava tão sobrecarregado que, já em 2003, ele congelava com frequência. Randy Dunlap ofereceu um link para seu próprio script [\[1\]](#) que lê os dados do anúncio do *finger*, presentes em <http://xenotime.net/linux/scripts/kcurrent??> e relata as alterações. Aparentemente, usar o script de Randy ou simplesmente consultar a URL do anúncio do *finger* é a melhor solução.

Podcast do kernel

Jon Masters anunciou o retorno de seu projeto, o *Kernel Podcast* [\[2\]](#) com transcrições [\[3\]](#). Sua principal motivação para o trabalho é se forçar a acompanhar o incrivelmente alto volume de tráfego da lista do kernel. É uma tarefa desafiadora, e com “alto risco de sobrecarga”, como ele mesmo disse. Ele optou por fazer uma pausa em vez de desistir de vez, e forneceu algumas estatísticas de quantas pessoas baixavam os novos podcasts até o momento. Desde maio de 2009, ele já teve um total de 200.000 downloads. Bem vindo de volta, Jon!

Mantenedor do IRQ

Ocasionalmente, uma nova entrada é adicionada ao arquivo [MAINTAINERS](#), não porque há um novo recurso no kernel, mas porque há alguma parte antiga do kernel para a qual um novo responsável acaba de surgir. Recentemente, Joe Perches sugeriu que o subsistema de IRQ recebesse sua própria entrada no arquivo, listando Thomas Gleixner como mantenedor oficial. O patch de Joe mostrava que Thomas submeteu quase 50% de todos os patches desse subsistema, enquanto que o segundo contribuidor mais prolífico submeteu somente 13%. Não houve discussão ou discordância quanto ao patch, e os patches de Joe para o arquivo [MAINTAINERS](#) parecem ser aceitos na maioria das vezes; então, esperamos em breve ver o nome de Thomas lá. ■

Mais informações

- [1] Script de Randy Dunlap: <http://www.xenotime.net/linux/scripts/kcurrent/>
- [2] Projeto Kernel Podcast: <http://podcasts.jonmasters.org/kernel/kernel.xml>
- [3] Transcrições do Kernel Podcast: <http://www.kernelpodcast.org/>

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.

ESPECIAL

EXTENDVOIP p.22
Uma história de sucesso na implantação da solução.

MOBILIDADE COM ECONOMIA p.10
Ampia gama de soluções de tecnologia em comunicações.

#4 Setembro 2010

LINUX

MAGAZINE

VoIP

A TECNOLOGIA QUE REVOLUCIONOU O MERCADO DAS TELECOMUNICAÇÕES

Panorama do mercado, os melhores fornecedores, artigos e tutoriais completos para quem deseja montar, gerenciar e economizar com seu próprio PABX Asterisk.

TELEFONIA OPENSOURCE DO FUTURO p.58
Aprenda a utilizar o FreeSWITCH para criação de centrais PABX.

EM SINTONIA p.68
Utilize o Skype em servidores de telefonia livre Asterisk.

ASTERISK DESCOMPLICADO p.62
Monte instâncias de um PABX Asterisk independente do sistema operacional.

CENTRAL TELEFÔNICA INTELIGENTE p.47
Entenda o funcionamento do piano de discagem.

WWW.LINUXMAGAZINE.COM.BR

LINUX MAGAZINE ESPECIAL VOIP

Panorama do mercado, os melhores fornecedores, artigos e tutoriais completos para quem deseja montar, gerenciar e economizar com seu próprio PABX Asterisk.

Asterisk
FreeSWITCH
PABX
Wireshark
Skype
Wondershaper
Webhtb
Opensips

A tecnologia que revolucionou o mercado das telecomunicações. Adquira o seu exemplar nas bancas de todo o país ou pelo site da Linux Magazine.



Coluna do Augusto

Loja de aplicativos em código aberto

Lojas de aplicativos são o futuro da distribuição de softwares?

O anúncio de lançamento de uma loja de aplicativos (*App Store*) da Fundação Mozilla, apresentada como protótipo em outubro e confirmada com mais detalhes no relatório anual de atividades da fundação, causou bastante confusão entre usuários acostumados a associar a expressão ao modelo fechado praticado em determinadas linhas de *tablets* e *smartphones*.

Mas a *App Store* da Fundação Mozilla tem algumas características que a diferenciam profundamente, e nem poderia ser diferente: ela está alinhada à missão da Fundação Mozilla associada à manutenção da web como uma plataforma aberta.

E a abertura da plataforma começa pela questão da interoperabilidade, em seu sentido real: desde a versão protótipo, os aplicativos da loja da Fundação Mozilla são compatíveis com os painéis oferecidos em todos os navegadores com suporte suficientemente atualizado aos padrões da web: além do óbvio Firefox (incluindo

Um modelo flexível que possa oferecer aplicativos interoperáveis para os usuários da cada vez mais presente plataforma web parece ser uma boa ideia para a qual existe demanda.

sua versão para plataformas móveis), a lista inclui Chrome, Safari, Opera, IE e WebKit Mobile.

Essa interoperabilidade nasce nas tecnologias empregadas para construir os aplicativos: JavaScript, HTML e CSS – os mesmos elementos dos *Google Gadgets* ou dos aplicativos do Mac OS X, por exemplo.

O nome *App Store* ou loja de aplicativos pode dar algumas impressões erradas, a começar pela questão da venda: embora o modelo suporte a comercialização (desde que usando padrões abertos, como o *OpenID*), não há qualquer ênfase nela, e o oferecimento gratuito de softwares livres é completamente suportado (ao contrário do que ocorre com a loja da Apple, por exemplo, que tem termos considerados incompatíveis com a *GPL*).

Outra impressão errada gerada pelo nome é a ideia de que vá existir uma loja ou repositório centralizado, no qual estarão disponíveis todos os aplicativos oferecidos para a plataforma (de forma similar ao que ocorre com a *iTunes Store*, mas uma vez). Mas a proposta é diferente: o modelo permite que o desenvolvedor ofereça e entregue os aplicativos diretamente ao usuário final, sem intermediários ou aprovações, se ambos desejarem.

Um modelo flexível que possa oferecer aplicativos interoperáveis para os usuários da cada vez mais presente plataforma web parece ser uma boa ideia para a qual existe demanda. O protótipo atual é voltado aos desenvolvedores, mas em breve veremos com mais clareza o que a Fundação Mozilla tem em mente. Boa sorte! ■

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



COLEÇÃO ACADEMY

Conheça a nova coleção de livros da Linux New Media

Os livros da Coleção Academy são roteiros práticos e objetivos, com didática adequada tanto ao profissional quanto ao estudante da área de TI.



COLEÇÃO ACADEMY

Luciano Antonio Siqueira

Infraestrutura de Redes



Passo a passo da montagem de uma rede de computadores, desde o cabeamento e roteadores até a configuração das máquinas clientes.

Configuração e manutenção de serviços essenciais como DNS, compartilhamento de arquivos e acesso remoto.



COLEÇÃO ACADEMY

Paulo Henrique Alkmin da Costa

Samba: com Windows e Linux



Como permitir a comunicação de diferentes sistemas operacionais em rede: Windows, Linux, Mac OS X etc. Definição de compartilhamentos de arquivos, impressoras – incluindo a instalação automática de drivers – e utilização do Samba como controlador de domínio (PDC) também para clientes Windows Vista e Windows 7.



COLEÇÃO ACADEMY

Luciano Antonio Siqueira

Máquinas virtuais com VirtualBox



Administração de infraestrutura de máquinas virtuais com Sun VirtualBox*. Como trabalhar com sistemas operacionais – Windows, Linux etc – na mesma máquina e simultaneamente.

Criação de diferentes modalidades de conexões virtuais, exportação/importação de máquinas virtuais e criação de pontos de recuperação (snapshots).

O conteúdo e o formato dos livros foram desenvolvidos a partir da experiência prática e educacional de seus autores, com foco principal no desenvolvimento de competências, através de conceitos, exemplos detalhados e dicas de quem realmente entende do assunto. O material é indicado tanto para autodidatas que desejam se aperfeiçoar quanto para utilização em escolas. O professor irá se sentir confortável para desenvolver as atividades a partir do livro, que procura atender tanto à expectativa do aprendiz quanto à demanda profissional do mercado de TI.

Disponível no site www.LinuxMagazine.com.br





Coluna do Kurt

Gerenciamento de senhas

Organizar todas as suas senhas pode ser difícil, mas como Kurt diz: mantenha seus amigos perto e suas senhas mais perto ainda.

Eficiente se deparar com situações em que não podemos usar o mesmo nome de usuário (por exemplo, quando seu nome já foi usado por outro usuário ou quando o próprio sistema determina o nome de usuário), e certamente não é recomendável usar a mesma senha (basta um dos sistemas ser comprometido para que um potencial agressor tenha acesso a todas as suas contas). Como todos nós temos múltiplas contas com diferentes nomes de usuários, senhas, perguntas de segurança, números de PIN e o que mais houver, acabamos com senhas demais, termo conhecido como “Fadiga de senhas” [1]. Quanto à perguntas de segurança, nunca se deve usar informações “reais” (como seu CEP, por exemplo), pois essas informações são fáceis de descobrir e usar para redefinir ou recuperar a senha no provedor de serviço. Para se manter em segurança, é preciso escolher uma senha forte e diferente para cada site acessado. Eu pessoalmente, tenho aproximadamente 350 senhas, perguntas de segurança e assim por diante, das quais uso, provavelmente, de 50 a 100 com regularidade. E isso me deixa maluco.

Então, a pergunta óvia é: como armazenar todas essas senhas e as informações relacionadas a elas (nome

de usuário, nome do site, perguntas de segurança etc.) de forma segura? Há três opções principais: pode-se confiar na aplicação para armazenar a senha, mas há casos e casos (algumas o fazem bem; outras são horríveis nisso); é possível usar um mecanismo de armazenamento de senhas fornecido pelo sistema (posso citar como exemplos o KDE Wallet ou o chaveiro de senhas do Gnome), o que funciona com múltiplos aplicativos e oferece armazenamento muito seguro de senhas; ou se pode usar um mecanismo de armazenamento de senhas fornecido por terceiros, o que pode ir desde um programa dedicado até uma planilha ou lista impressa. Todas estas técnicas possuem vantagens e desvantagens.

Armazenamento de senhas do sistema

Provavelmente a forma mais fácil a longo prazo é usar um sistema como o KDE Wallet ou o chaveiro de senhas do Gnome, caso todos os seus aplicativos os suportem. Estes dois sistemas oferecem recursos bastante seguros para o armazenamento de senhas (já foram extensamente auditados porque são componentes do núcleo do sistema) e geralmente possuem interfaces fáceis de usar. Além disso, diferentemente da maioria dos aplicativos de terceiros, eles fornecem senhas automaticamente para softwares do seu sistema. Então, você faz login, digita sua senha mestra e, a partir daí, todos os seus programas usam os dados de autenticação sem perturbá-lo(a) constantemente.

KWallet Manager

O KWallet Manager [2] é a interface padrão do KDE Wallet, e tenho que dizer que não é tão ruim. As operações básicas são funcionais; é possível importar e exportar chaves, unificar duas carteiras de contas

Para se manter em segurança, é preciso escolher uma senha forte e diferente para cada site acessado. Eu pessoalmente, tenho aproximadamente 350 senhas.

(wallets) e assim por diante. Além disso, ele possui um plugin para o Firefox, atualizado em janeiro de 2010, que realmente funciona muito bem. A interface suporta múltiplas carteiras com diferentes senhas (útil caso se deseje usar um conjunto de senhas pessoais e outro conjunto de senhas de trabalho no mesmo sistema, mas separados).

Entretanto, falta um recurso importante: não é possível adicionar notas às senhas (isto é, criar um lembrete sobre para que serve a senha ou as perguntas de recuperação associadas a ela). Todavia, como o aplicativo possui um plugin atualizado e funcional para Firefox, eu lhe daria uma nota B+ na escala de notas de A a F.

Seahorse

O *Seahorse* [3] é a interface padrão para o chaveiro de senhas do Gnome e é muito semelhante ao KWallet na maioria dos aspectos. Apesar de ter as funções básicas (importar e exportar), não possui função de mesclar bases, então não tenho muita certeza se ele lida bem com a sincronização de arquivos. Entretanto, o Seahorse pode compartilhar senhas na rede, algo que o KWallet

não consegue fazer. Então, dependendo da sua configuração, pode ser desnecessário sincronizar múltiplos sistemas, o que é sempre bom.

A grande desvantagem do Seahorse é a falta de um plugin atual para o Firefox. A última versão do plugin *Gnome-keyring password integration* para Firefox saiu em agosto de 2008 e, para fazê-la funcionar no Firefox 3.6, é preciso baixar o código-fonte, alterá-lo manualmente e depois compilá-lo e instalá-lo. O Seahorse também possui a mesma falha do KWallet no sentido das anotações de senhas. Devido ao plugin ausente (que sei que não é uma falha do projeto Gnome), eu daria ao chaveiro de senhas do Gnome apenas uma nota C, e espero que o plugin volte em breve a ser ativamente suportado.

Estas duas opções são bem funcionais, principalmente quando se deseja configurar detalhadamente seus aplicativos. Para a maioria de nós, a integração com o navegador, cliente de e-mail, cliente SSH e GnuPG supre a maioria das nossas necessidades de senhas. Além disso, qualquer aplicativo local que queira usar o chaveiro do Gnome ou o KWallet será capaz de fazê-lo, evidentemente.

Certificação LPI, Novell CLA e Impacta

Por que escolher a Impacta?

Eleita pela 5º vez o maior centro de treinamentos do Brasil pela Computerworld.

Eleita por 3 anos consecutivos como a melhor instituição de ensino de TI pela Editora Segmento.

Eleita 4 vezes consecutivas pelo Prometric Testing Center como o maior centro certificador da América Latina.

Somente no maior centro de treinamentos do Brasil você encontra pacotes de treinamentos que preparam, simultaneamente, para as principais certificações do mercado: Linux LPI, Novell Certified Linux Administrator e Impacta Certified Specialist.

Preparatórios para LPI 101, LPI 102, LPI 201 e LPI 202

Linux módulo 1 - Princípios do Linux

Linux módulo 2 - Configurando e administrando servidores Linux

Linux módulo 3 - Implementando uma infraestrutura de rede Linux

Preparatórios para LPI 301 e LPI 302

Linux módulo 4 - Implementando soluções Samba no Linux

Linux módulo 5 - Implementando servidores de autenticação LDAP no Linux

Preparatório para LPI 303

Linux módulo 6 - Implementando segurança em servidores Linux



Gerenciamento de senhas no Firefox

Vou iniciar a abordagem sobre o armazenamento de senhas especificamente focando o aplicativo que provavelmente possui a maioria das senhas armazenadas: seu navegador web (mais especificamente, o Firefox). Como a maioria dos navegadores web, o Firefox armazena senhas e, se você digitar uma senha mestra, ele as criptografa (usando 3DES em modo CBC). Então, se você usar uma senha mestra forte, estará em segurança. Se você não usar uma senha mestra, no entanto, as senhas serão armazenadas em um modo ofuscado que pode ser visto facilmente por um invasor (basta carregar o arquivo em uma cópia do Firefox e ler as senhas!).

Falta no gerenciamento de senhas do Firefox a capacidade de exportar e importar senhas; é possível copiar os arquivos manualmente, mas mesclá-los, ou – realizar qualquer outro tipo de operação – não é fácil. Felizmente, um bom plugin chamado *Password Exporter* permite exportar senhas para um arquivo e depois importá-las (permitindo também mesclar manualmente os arquivos por meio da importação de outro sistema seguida de exportação do conjunto completo de senhas). Porém, assim como o KWallet e o Seahorse, não há qualquer forma fácil de adicionar anotações às senhas. Isto significa que ainda é preciso guardar as respostas das perguntas secretas em algum outro local.

Armazenamento ruim – FileZilla

Não é só porque existem formas seguras e frequentemente aceitas de lidar com senhas que todo mundo as usa. O FileZilla (um bom cliente de FTP/SFTP/etc. de código aberto), por exemplo, faz cache do nome de usuário e da senha em texto puro por padrão caso você use a opção de conexão rápida. Não vejo nenhuma forma, na interface gráfica, de desativar esse comportamento, nem há qualquer alerta de que isso esteja ocorrendo. Apesar de ser possível desativar isso, só é possível fazê-lo criando um arquivo de configuração personalizado. Em outras palavras, saiba que seus aplicativos podem fazer coisas perigosas sem que você seja avisado.

Armazenamento terceirizado de senhas

Como você provavelmente precisa criar respostas falsas às perguntas secretas (por exemplo, a cidade onde você nasceu – informação fácil de encontrar publicamente), é preciso possuir um local seguro para guardar essas respostas. Há alguns bons aplicativos nesse segmento – notavelmente o KeePass [4] e o KeePassX [5] – que,

apesar de terem nomes muito semelhantes, são projetos completamente diferentes.

Ambos são de código aberto e estão disponíveis para vários sistemas operacionais (Windows, Mac OS X e Linux), mas o KeePass também suporta diversas plataformas (iPhone, Blackberry, PalmOS, Android etc.). Recomendo fortemente evitar aplicativos proprietários para armazenar senhas por um único e simples motivo: a maioria é horrivelmente falha e insegura (por exemplo, fazem coisas como não criptografar de verdade os dados).

Soluções de longo prazo

Uma lição que a maioria das pessoas não aprenderá antes que seja tarde demais é que, embora você possa morrer, suas senhas sobreviverão. Se, por exemplo, você for a única pessoa com a senha da conta de administração do DNS ou do servidor de *backup*, é provável que mais alguém precise ter acesso às suas senhas (e, como visto no caso de Terry Childs [6], reter senhas pode se tornar uma tarefa muito complicada).

Além disso, se você possui uma família, será muito mais fácil eles desativarem contas e lidarem com a perda caso consigam acessar suas senhas. Muitas empresas possuem procedimentos notoriamente lentos para lidar com clientes que não os pagam mais. Provavelmente, a forma mais fácil de lidar com isso em um nível pessoal é imprimir suas senhas ou sua senha mestra e colocá-la num cofre seguro que seus entes próximos consigam acessar.

A forma mais fácil de reduzir a fadiga de senhas é reduzir o número de contas e senhas necessárias. Felizmente, há algumas novas tecnologias e sistemas de autenticação que possibilitam isso. ■

Mais informações

- [1] Fadiga de senhas: http://en.wikipedia.org/wiki/Password_fatigue/
- [2] KWallet manager: <http://utils.kde.org/projects/kwalletmanager/>
- [3] Seahorse: <http://projects.gnome.org/seahorse/>
- [4] KeePass: <http://keepass.info/>
- [5] KeePassX: <http://www.keepassx.org/>
- [6] Terry Childs: http://en.wikipedia.org/wiki/Terry_Childs

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

DECISÕES CERTAS PODEM MUDAR O RUMO DE SUA CARREIRA

Inclua em seu currículo a principal certificação Linux no mundo – LPI.



Em tempos de crise, soluções de código aberto – como o Linux – se destacam na adoção por empresas de todos os tamanhos, como solução ideal para aumentar eficiência nos negócios e reduzir custos. Atualmente há no mercado uma carência por profissionais certificados para atender a essa demanda crescente. Aproveite essa oportunidade e inclua em seu currículo a principal certificação Linux no mundo.



**Inscrições e
mais informações:**

www.lpi-brasil.org
treinamentos@vectory.com.br
Tel (11) 3675-2600



Coluna do Alexandre

O mundo de Terracotta

Lidar com gigantescos volumes de dados não é mais uma tarefa tão complicada e ponto de não haver solução.

Udados todos os dias, como Amazon, Facebook, eBay etc., estão sempre às voltas com problemas de escalabilidade e com a preocupação de manter o desempenho, possuindo tolerância à falhas. Em geral, as soluções conhecidas hoje em dia para melhorar os aplicativos nesse ambiente de crescente demanda é acrescentar mais servidores, redesenhar os softwares para aumentar sua capacidade e adicionar cache para depender cada vez menos de acesso ao banco de dados.

Essa última abordagem levanta o conceito de cache elástico que nada mais é do que serviços de caching de dados distribuídos entre dois ou mais servidores, sendo que, quando a aplicação não encontra os dados que procura no cache local, busca a mesma informação no cache distribuído entre alguns nós que estão dispostos em forma de *cluster*. Isso de fato é muito parecido com produtos NoSQL, porém com a diferença de que estes focam a persistência dos dados.

É nesse contexto de cache elástico que entram softwares como o *Terracotta* [1], criado em Java, competindo com grandes fabricantes como Oracle, GigaSpaces, IBM e VMware (que adquiriu a GemStone). O que particularmente me atrai no software *Terracotta* é que a empresa

ce, facilitando a integração com outros frameworks Java, assim como um modelo de licenciamento interessante (além da versão paga, é oferecida uma versão mais simples para uso e testes que não incluem suporte, atualizações e patches, por exemplo) e são ao mesmo tempo muito fáceis de instalar, levando em conta ainda o fato de serem pouco invasivos. O framework do *Terracotta* (**figura 1**) é formado basicamente por 3 componentes: *Terracotta Server*, *Ehcache* e *BigMemory*.

Em linhas gerais, imagine 10 máquinas executando uma mesma aplicação Java, que sempre procura suas informações no cache da máquina local (conhecido como L1, nos termos do *Terracotta*). O *Ehcache*, percebendo que a informação não é encontrada, atua como uma interface e faz a busca dos dados ou objetos nos servidores *Terracotta* (que podem ser diversos atuando em conjunto – conhecido como cache nível L2), e que distribuem os dados do cache entre eles como se fossem um RAID0, só que em memória.

Se a informação não é localizada nesses servidores, os dados são buscados a partir de um banco de dados. Quando esta informação é trazida do banco de dados para o cache L2 (no servidor *Terracotta*), ela fica dis-

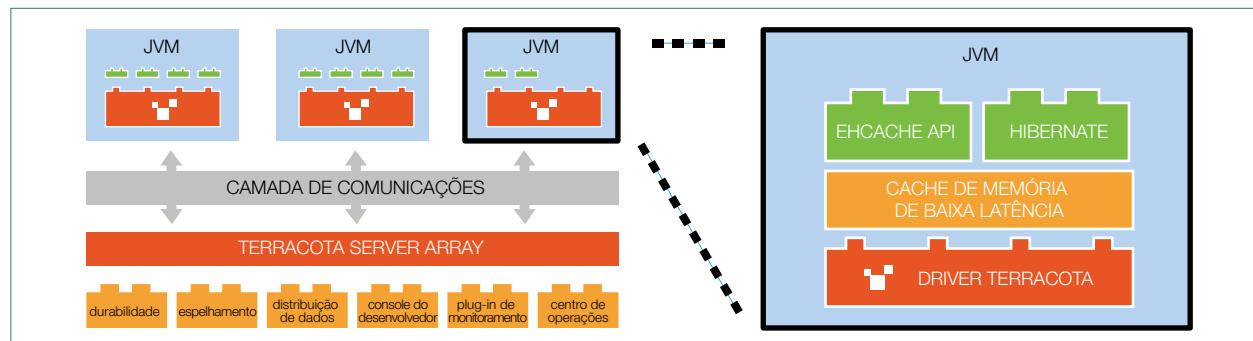


Figura 1 Arquitetura do *Terracotta*.

ponível para todas as máquinas que rodam o mesmo aplicativo, através do Ehcache, que acaba sendo responsável pela coerência das informações. Os ganhos com essa estrutura são elevados pois permitem mais de 10.000 transações por segundo, diminuindo a latência do aplicativo em torno de até 90% e ainda um ganho de desempenho linear e em memória.

O BigMemory é um plugin do Ehcache que trata de um dos maiores problemas do *Garbage Collector* (GC) da JVM (*Java Virtual Machine*): a extrema dificuldade de tratar grandes quantidades de memória *heap*, sendo que o GC provoca grandes pausas nas aplicações, para irritação de desenvolvedores e empresas, sendo que alguns deles preferem distribuir seus aplicativos em diversas JVMs (fazendo uma espécie de particionamento e balanceamento de carga dos dados), promover ajustes do GC da JVM quando configurando suas aplicações, ou ainda manter a memória *heap* reduzida.

É justamente neste ponto que o BigMemory viabiliza o uso de grandes quantidades de memória, para que possa fazer cache de uma quantidade maior, aumentando o desempenho, sem fragmentações, sem contenção de locks, escalonando ao máximo em termos de cpu e *threads*, sem qualquer alteração no código fonte do aplicativo, e, quem diria, totalmente feito em Java.

E como o BigMemory consegue este feito? Os profissionais do Terracotta criaram um gerenciador de memória otimizado que, com uso da feature *direct memory buffer store* do Java, permite fazer uso de uma memória *off-heap*, ainda dentro do espaço de endereçamento do processo Java, para armazenar seus dados e objetos, possibilitando assim eliminar de uma vez a necessidade do GC realizar sua limpeza em grandes espaços de memória e, ao mesmo tempo, tornando viável o uso pelos aplicativos de grandes espaços de memória como cache, evitando a todo custo o acesso ao banco de dados.

Terracotta é isso: uma ideia simples, fantástica e com resultados expressivos para profissionais obcecados por desempenho. Até o mês que vem. ■

Mais informações

- [1] Site do projeto Terracotta:
<http://www.terracotta.org/>

Alexandre Borges (alex_sun@terra.com.br, twitter: @ale_sp_brazil) é Especialista Sênior em Solaris, OpenSolaris e Linux. Trabalha com desenvolvimento, segurança, administração e performance desses sistemas operacionais, atuando como instrutor e consultor. É pesquisador de novas tecnologias e assuntos relacionados ao kernel.

Você está com a cabeça nas nuvens? Nós também.

AntiSpam SaaS UNODATA

30 DIAS
GRÁTIS!

ENVIE UM E-MAIL PARA
LINUXMAGAZINE@UNODATA.COM.BR
E GANHE + 1 MÊS GRÁTIS DE ANTIISPAM

Para empresas que não querem ou não
podem administrar sua infra-estrutura de e-mail
o AntiSpam SaaS UNODATA é uma ótima opção.

- › Disponível em Software, nuvem e Appliance
- › 3 em 1 - AntiSpam, AntiVírus e AntiFraude
- › Instalação em menos de 15 minutos

→ Dell lança notebooks Inspiron 14 com Ubuntu

A Dell, uma das maiores fabricantes mundiais de computadores e notebooks, lança a linha Inspiron 14, agora equipada de fábrica com uma versão OEM do Ubuntu 9.10. Com 14 polegadas e possibilidade de escolha entre os processadores Intel Celeron e Intel Dual Core, as máquinas já estão à venda no site brasileiro da fabricante por preços extremamente competitivos, com frete grátis e entregas em todo o território nacional.

Com beleza surpreendente, os notebooks ainda podem ser personalizados através da loja virtual da Dell, que oferece possibilidades de escolha da quantidade de memória RAM, tamanho do disco rígido e outros opcionais. ■



► Novo cliente de torrents Tribler 5.3 facilita a vida do usuário

O BitTorrent é o protocolo p2p mais famoso do mercado, mas ainda precisa de vários servidores centralizados *trackers*, para que os usuários possam encontrar os arquivos que estão procurando. Houve várias tentativas de tornar o BitTorrent mais descentralizado até agora sem muito sucesso. A versão 5.3 do Tribler é o primeiro cliente de BitTorrent que não necessita de trackers ou motores de busca, de acordo com o TorrentFreak.

O Tribler oferece algumas tecnologias muito interessantes, e a última versão permite aos usuários pesquisar e baixar arquivos a partir do próprio aplicativo, através de um mecanismo de busca interno. Outros clientes também oferecem recursos de pesquisa, como o uTorrent, mas os resultados do Tribler vêm dos clientes de outros usuários ao invés de apenas um motor de busca dedicado. Os usuários podem pesquisar e baixar conteúdo sem um servidor, pois tudo é feito entre os pares, sem a necessidade de um tracker BitTorrent ou de um indexador de busca. Isso significa que o arquivo `.torrent` de BitTorrent não é mais necessário. Normalmente, os usuários precisam encontrar o arquivo `.torrent` correspondente ao conteúdo que desejam baixar. O arquivo contém a URL do tracker BitTorrent, que, como o próprio nome indica, controla todos os downloads e uploads do conteúdo em questão.

O Tribler é um cliente de BitTorrent novo, e possui um número significativamente menor de torrents em relação ao que está disponível nas populares máquinas de busca do BitTorrent. Mas com essas novidades, é questão de tempo para aumentar a quantidade de arquivos disponíveis através da sua rede. ■

► iPad chinês vem com câmera e sistema Android

Os asiáticos são mesmo muito criativos. Depois de criar um MacBook que vinha com Windows de fábrica, cotado a menos de 300 dólares, agora eles atacam com um iPad que roda Android, sistema operacional da Google. A informação foi divulgada em sites de tecnologia como 9to5Mac e Shanzai.

O tablet, que é idêntico ao iPad por fora, mas que traz configuração bem diferente em seu sistema, custa apenas 277 dólares, tem tela de 9,7 polegadas, chip Cortex A8 de 800 MHz, 512 MB de memória e 4 GB de memória flash, conexão 3G, Wi-Fi e até câmera (recurso que só devemos ver no iPad 2). É bom os fabricantes de tecnologia ficarem de olho, pois os asiáticos estão com tudo! ■

► Google vai distribuir notebooks para testar sistema operacional na nuvem

O Google anunciou recentemente que testará seu sistema operacional baseado em Linux, o Chrome OS, em um projeto piloto que incluirá a distribuição de um notebook criado especificamente para o novo ecossistema.

Batizado de Cr-48, o notebook será distribuído gratuitamente pela gigante da Internet para alguns usuários da rede nos Estados Unidos, e será o primeiro de uma série de computadores adaptados para o Chrome OS. O sistema operacional, segundo o Google, será totalmente integrado à nuvem, ou seja: terá a capacidade de executar programas diretamente da Internet, sem a necessidade de instalação no computador do usuário.

O Cr-48 terá autonomia de 8 horas de funcionamento, e 7 dias em espera. Ao ser ligado,



Divulgação

entra em operação em apenas 10 segundos, de acordo com a empresa, que não informou quantos notebooks serão distribuídos no programa piloto.

Após os testes com o Cr-48, a primeira leva de PCs a usar o sistema operacional ChromeOS chegará às lojas em meados de 2011 nos Estados Unidos e contará com conexão sem fio gratuita da operadora Verizon por dois anos. Os novos notebooks Chrome terão 100 megabytes mensais de conexão sem fio gratuitas por dois anos.

O Google lançou também sua nova loja online de games, notícias e outros aplicativos, como parte da estratégia para conquistar uma participação maior na nova geração de mídia e entretenimento da Internet.

A produtora de games Electronic Arts fez uma demonstração de um jogo que estará disponível na “Chrome Store”, que será inaugurada em breve. A loja virtual também venderá aplicativos de notícias do jornal New York Times e da National Public Radio.

Executivos do Google disseram, em coletiva em San Francisco que o navegador Chrome já conta com 120 milhões de usuários. Em maio, o browser do Google contava com apenas 70 milhões de usuários.

A Apple afirmou em outubro que também iria abrir uma loja virtual de aplicativos para seus computadores Macintosh, em busca de replicar o sucesso da “app store” para o iPhone. O serviço, que será integrado ao sistema operacional Mac OS X, deve estar disponível até janeiro. ■

► Netbooks distribuídos à rede pública de ensino portarão o Mandriva Linux

O Ministério da Educação e Cultura (MEC) escolheu a distribuição Mandriva Linux para ser distribuída a alunos de rede pública de ensino, informou o blog da Mandriva Conectiva durante o mês de dezembro.

O sistema operacional será incluído nos netbooks ClassmatePC, que possuem processadores Intel, e são fabricados pela Positivo. Possui tela de 10 polegadas, chip Atom e conexão Wi-fi, além de ser resistente a quedas.

A decisão do governo brasileiro de escolher as soluções da Intel Learning Series (Linha de Aprendizagem da Intel) com o Mandriva Linux nos ClassmatePC consolida a posição do Linux como o sistema operacional preferido para o mercado global de educação, com o Mandriva sendo o líder no mercado Linux orientado à educação. E de acordo com o comunicado, essa será uma das “maiores implantações organizadas de Linux no mundo, com potencial para atingir 1,5 milhão de unidades”. ■

A edição brasileira do Mandriva é baseada na versão mais recente da distribuição franco-brasileira para mini notebooks, a versão 2010, e foi adaptada para os computadores com processadores Intel com um lançador de aplicações exclusivo, que torna mais fácil o acesso ao aplicativos de código aberto mais comuns. Os computadores serão usados por professores, pais e alunos nas escolas brasileiras. ■



Divulgação

► Oracle pede à Apache que volte ao comitê executivo do Java

A Oracle pediu à Fundação Apache (ASF – *Apache Software Foundation*) que reveja sua decisão de sair do comitê executivo do Java, por considerá-la de suma importância para o futuro da plataforma.

“A preocupação comercial de uma única entidade, a Oracle, continuará a interferir seriamente na ideia de uma direção transparente para o ecossistema”, afirmou a Apache, por meio de seu blog oficial, em alusão ao grande controle que a empresa fundada por Larry Elisson tem sobre a tecnologia.

Ela também mostrou irritação quanto às restrições da Oracle quanto ao Kit de Compatibilidade de Tecnologia Java (TCK), usado pela fundação nos testes de seu software de código aberto, o Harmony. Os obstáculos impostos impedem a adaptação do programa para dispositivos móveis.

Logo após o anúncio, o vice-presidente de desenvolvimento da Oracle, usou um tom conciliatório em seu discurso para reverter a situação:

“Nós renomeamos a Fundação Apache para o comitê executivo, porque valorizamos sua perspectiva e participação ativa”, escreveu em um comunicado. “A Oracle

tem a responsabilidade de levar o Java adiante e manter sua uniformidade, em razão dos milhões de desenvolvedores que o utilizam. A Fundação Apache, e seus muitos projetos de código aberto, são parte importante do ecossistema”.

De fato, são mais de 100 projetos relacionados ao Java patrocinados pela ASF, como as aplicações para servidores Tomcat e Geronimo. Aparentemente, a resposta da corporação americana leva em conta tal fator, ao considerar o prejuízo que a plataforma sofreria com a baixa.

A princípio, no entanto, a Fundação Apache não se mostra convencida. “Dê-nos um motivo para reconsiderarmos a decisão que não seja um simples pedido de por favor”, postou seu presidente, Jim Jagielski, no Twitter.

“O Java Community Process – processo que permite que as partes se envolvam nas definições de versões futuras da plataforma – está morto”, escreveu o executivo em seu blog. “Tudo o que resta é um zumbi, vagando pelas ruas do ecossistema, à procura de cérebros. Mas, quem sabe, a partir dessa morte, uma nova comunidade possa surgir, formada por pessoas diferentes; uma em que não existam membros mais iguais do que os outros. Isso é algo que a ASF adoraria ver”, concluiu. □

► BMC Software e Salesforce.com ampliam parceria para cloud computing

A *BMC Software* e a *Salesforce.com* ampliaram sua parceria na adoção de ferramentas baseadas na nuvem. As empresas acabam de anunciar o *RemedyForce*, uma ferramenta de cloud. “Os clientes da gestão de serviços de TI têm agora uma solução na nuvem para atender às suas necessidades”, afirma Marc Benioff, presidente e CEO da *Salesforce.com*. “Esperamos impulsionar o sucesso da computação em nuvem em todos os departamentos de TI, de empresas de todos os tamanhos”.

“O RemedyForce fornece às empresas a oportunidade de acessar recursos de TI por meio das soluções de gerenciamento de serviços da *BMC*, bem como reforça a base das ofertas disponíveis aos nossos próprios clientes. Como resultado, as empresas poderão extrair mais de seus investimentos de TI”, diz Bob Beauchamp, presidente e CEO da *BMC Software*. “Esse é o melhor dos dois mundos, a entrega de soluções comprovadamente de ponta, que irão acelerar o sucesso do cliente e a evolução da nuvem e da gestão de TI”.

Com base na parceria, o *RemedyForce* adiciona uma nova oferta da *Salesforce.com* nos serviços de nuvem atuais, que incluem vendas na nuvem, serviços, colaboração, plataforma *Force.com* e o *Database.com*. Da mesma forma, junta-se ao *RemedyForce* a família de soluções *BMC* de produtos de gerenciamento de serviços, incluindo o *BMC Remedy IT Service Management Suite* e o *OnDemand BMC Remedy*. A *BMC* adiciona ao *RemedyForce* recursos como o *Service Desk*, que reúne uma série de funções de gestão da plataforma de cloud computing *Force.com*. A solução resultante é de fácil utilização, com desempenho otimizada para os recursos da nuvem. ■

► VMware e Fujitsu firmam acordo de OEM para soluções de virtualização no Brasil

A VMware e a Fujitsu acabam de assumir no Brasil os termos do contrato mundial que estabelece a parceria na modalidade *Original Equipment Manufacturer* (OEM), na qual a Fujitsu se torna distribuidor das soluções de virtualização da VMware agregadas a seus servidores de missão crítica da série *Primequest*. A partir de agora, a Fujitsu terá como valor agregado aos servidores, soluções de virtualização e *cloud computing* para espelhamento das aplicações de missão crítica de seus clientes. O contrato OEM compreende consultoria, hardware, software, integração de sistemas e manutenção em todo o país.

De acordo com Edson Siqueira, diretor comercial da Fujitsu do Brasil, “a parceria entre VMware e Fujitsu será muito interessante para ambas as empresas, pois a estratégia de *cloud computing* vem ao encontro da Fujitsu para oferecer aos clientes soluções ininterruptas que assegurem a continuidade de seus negócios. A série de servidores Primequest é compatível com os principais softwares de virtualização do mercado e é o mais adequado, tanto para trabalhos em plataformas baseadas em *cloud computing* quanto em integração de servidores. Outra característica forte é a redução do custo total de propriedade dos sistemas de tecnologia da informação e da comunicação (TIC)”.

Para a VMware, o novo contrato é uma evolução do trabalho que a Fujitsu já vinha fazendo no Brasil, ao oferecer soluções de virtualização a seus clientes com as aplicações vSphere 4.1 e vCenter Server adquiridas via distribuidores locais. “É uma excelente parceria para ambientes de consolidação ou muito criteriosos como, por exemplo, plataformas de TI de empresas do mercado financeiro, de telecomunicações ou de e-commerce, que precisam de alto poder de processamento de dados em ambientes virtualizados. E a Fujitsu é especialista nesse segmento”, afirma Marco Fontenelle, diretor de Canais Brasil da VMware.

A série de servidores Primequest [1], da Fujitsu, é comercializada somente no Japão e no Brasil e é homologada pela VMware. Entre suas características estão a compatibilidade com plataforma Unix, menor consumo de energia, menor espaço ocupado, menores preços, monitoramento a distância, manutenção preventiva e aumento de desem-

penho. Além disso, os servidores se alinham à política de TI verde.

“A preocupação com o meio ambiente está no DNA da Fujitsu, desde a política de descarte, produção, manufatura até a relação com seus funcionários. É uma ideologia que se estende para nossa vida pessoal depois de aplicada no trabalho. Nesse sentido a VMware está em linha com o que pensamos. *Cloud computing* veio para minimizar o impacto na natureza”, declara Edson Siqueira, diretor comercial da Fujitsu do Brasil. A Fujitsu foi considerada a segunda empresa de tecnologia do mundo que mais se preocupa com o meio ambiente em um estudo do *Gartner Group* [2].

VMware vSphere [3] é a plataforma mais confiável do mercado para virtualização de //data centers/. A empresa usuária de vSphere reduz significativamente os custos operacionais e de capital, além de aumentar a eficiência da equipe de TI, com a liberdade de escolher qualquer aplicativo, sistema operacional ou hardware. O VMware vCenter Server [4] oferece uma plataforma de gerenciamento central, escalonável e extensível, que serve de base para a virtualização. Permite gerenciar o VMware vSphere para que os administradores de TI aperfeiçoem o controle sobre o ambiente virtual. ■

Mais informações

- [1] Primequest Fujitsu: <http://www.fujitsu.com.br/services/servers/primequest/>
- [2] Estudo do Gartner Group: <http://www.gartner.com/it/page.jsp?id=1458613>
- [3] Site do VMware vSphere: <http://www.vmware.com.br/products/vsphere/>
- [4] VMware vCenter Server <http://www.vmware.com/products/vcenter-server/>

Para notícias sempre atualizadas e com a opinião de quem vive o mercado do Linux e do Software Livre, acesse nosso site: www.linuxmagazine.com.br

► Red Hat adquire Makara e acelera estratégia de PaaS

A Red Hat anunciou a aquisição da Makara, uma fabricante de soluções de gerenciamento para aplicações em nuvem. As tecnologias da Makara vão acelerar o desenvolvimento da solução abrangente de plataforma-como-serviço (PaaS) da Red Hat, como parte de seu portfólio, o *Cloud Foundations*.

Sediada na cidade de Redwood, na Califórnia, a Makara oferece soluções que permitem às organizações implementar, gerenciar, monitorar e escalonar suas aplicações em nuvens públicas e privadas. Integrando a infraestrutura *JBoss Enterprise Middleware* com a *Cloud Application Platform* da Makara, a Red Hat oferece uma solução ainda mais completa de plataforma-como-serviço que permite às organizações realizarem uma transição rápida de suas aplicações para a nuvem com modificações mínimas.

“A proposta da *Cloud Foundations* é permitir que clientes e desenvolvedores tenham uma via de acesso fácil para a nuvem. Com a inclusão da Makara, visamos simplificar a implementação e gerenciamento de aplicações”, disse Paul Cormier, presidente de produtos e tecnologias da Red Hat. “Nós damos as boas vindas à equipe da Makara e buscamos acelerar nossa oferta de soluções em plataforma-como-serviço para o mercado”.

A Red Hat lançou o *Cloud Foundations* em junho de 2010, tornando-se a única fabricante com infraestrutura necessária para entregar uma oferta de cloud de código aberto completo e flexível, incorporando sistema operacional, middleware e virtualização. Baseada no *JBoss Enterprise Middleware*, a Red Hat PaaS busca ser a solução que irá permitir a empresas, provedores de serviço de cloud, ISVs e provedores de software-como-serviço, utilizar seus recursos para desenvolver novas aplicações e implementá-las em ambientes de cloud pública e privada, sem precisar reescrevê-las.

A Red Hat pretende lançar o Red Hat PaaS como software oferecido como serviço a clouds públicas e privadas para ajudar desenvolvedores e organizações a construir, implementar e administrar o ciclo de vida completo de suas aplicações. As ferramentas, tecnologias e soluções da Makara serão totalmente integradas à Red Hat PaaS, como parte do portfólio *Cloud Foundations*.

Hoje, as empresas podem começar a implementar *JBoss Enterprise Middleware* em clouds privadas através da consultoria da Red Hat em conjunto com produtos e serviços dos parceiros da Red Hat. A Red Hat oferece uma suíte completa de produtos e serviços para todo o ciclo de vida das aplicações ideais para a transição com eficiência de custos ou novas aplicações para nuvem pública e privada. ■

► Executivo confirma que Microsoft tentou comprar Facebook por US\$ 15 bilhões

Em uma conferência de tecnologia em Paris, na França, na primeira quinzena de dezembro, um executivo da Microsoft confirmou que a empresa deu um lance fracassado para comprar o Facebook há três anos atrás.

Mark Zuckerberg, CEO do Facebook, recusou uma oferta de 15 bilhões de dólares (cerca de 25,5 bilhões de reais, nos valores de hoje) feita pelo CEO Steve Ballmer, disse Fritz Lanman, diretor sênior de estratégia corporativa e aquisições da gigante de Redmond. O executivo deixou escapar a informação sobre a compra fracassada enquanto discursava na conferência *LeWeb*, realizada em Paris.

“Sim, nós tentamos comprar o Facebook”, disse Lanman durante uma entrevista no palco, de acordo com o *TechCrunch*. “Naquela época, o Facebook guardava muita semelhança com a Microsoft.”

Lanman acrescentou que, quando o Facebook rejeitou a oferta da Microsoft, a empresa investiu 240 milhões em uma pequena participação acionária na rede social.

Mesmo assim, a Microsoft e o Facebook continuam a trabalhar juntos. Em outubro de 2010, as empresas anunciaram uma parceria para levar mais elementos de rede social às buscas na web. Como parte do acordo, a busca do Facebook, que é equipada pelo Microsoft Bing, tem facilitado o encontro de pessoas no site da rede social.

Lanman disse que o Facebook poderá, um dia, valer tanto quanto a Microsoft.

“É fácil dizer que a Microsoft perdeu uma enorme oportunidade ao não comprar o Facebook quando Ballmer se encontrou com Zuckerberg”, disse Dan Olds, analista da *The Gabriel Consulting Firm*. “Mas a Microsoft ofereceu uma grande quantia em dinheiro e foi rechaçada mais de uma vez. Como se trata de uma empresa de capital fechado, o melhor que a Microsoft pôde fazer foi comprar uma parte dela por 240 milhões.”

E a decisão de Zuckerberg pode ter sido boa, no fim das contas. “Quem diria que o Facebook seria tão bem sucedido se tivesse sido comprado pela Microsoft?”, pergunta Olds. “Por tudo que conhecemos, a Microsoft bem que poderia ter estragado com tudo”, completa. ■

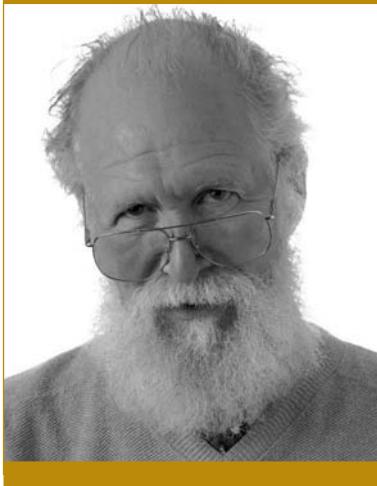
Livro Certificação LPI-1 3ª edição



A Linux Magazine está lançando a **3ª edição revisada e ampliada** do livro que te prepara para a **Certificação LPIC-1** com as seguintes novidades:

- Exercícios em todos os tópicos
- Todo conteúdo ampliado para a nova versão da prova, atualizada em abril/2009

Garanta já o seu pelo site da Linux Magazine
www.linuxmagazine.com.br



Coluna do maddog

Fotos antigas

O colunista fala sobre formatos de arquivos de imagens ultrapassados, e a solução para gerenciá-los.

por **Jon "maddog" Hall**

Costumo falar frequentemente sobre padrões de documentos e a importância dos formatos abertos, principalmente sobre formatos como o padrão *Open Document Format* (ODF) em comparação com a especificação OOXML, da Microsoft.

Recentemente, eu estava nostálgico e decidi dar uma olhada em algumas fotos antigas. Em determinado ponto da minha vida, tirei muitas fotos com uma câmera que utilizava filmes 35mm. Para diminuir o custo de revelação, preferi fazer *slides* em vez de fotos normais, impressas em papel. Claro que slides não são tão convenientes quanto fotos em papel, já que é preciso instalar um projetor e uma tela para ver as fotos.

Por volta de 1995, duas coisas aconteceram. Eu comecei a usar mais os computadores em casa, graças ao projeto Linux, e comecei a fazer PhotoCDs Kodak a partir dos meus slides. Um PhotoCD Kodak podia armazenar até 100 diferentes fotos em até seis tamanhos diferentes. Enviei o filme para ser processado na Kodak, pedindo que as imagens também fossem colocadas em um CD. O PhotoCD foi entregue em uma caixa com capa que incluía uma miniatura das fotos, que estavam

numeradas de forma a permitir que eu as encontrasse com facilidade. A Kodak criou também outros itens para o PhotoCD, como um reproduutor de CDs que podia ser acoplado à TV para que eu visse as fotos na tela.

O formato das imagens no PhotoCD era proprietário. A Kodak fornecia um programa que conseguia ler o PhotoCD, manipular as imagens e armazenar a foto em algum outro formato, normalmente usando algum tipo de compressão (por exemplo, JPEG). Claro que o programa só funcionava no Microsoft Windows. Felizmente, no Linux havia um ótimo programa chamado [xpcd \[1\]](#), criado para ler arquivos PhotoCD. Os autores haviam feito engenharia reversa no formato PhotoCD para ler o CD da Kodak (cujo sistema de arquivos era ISO 9660), extrair as imagens e exibi-las. O [xpcd](#) conseguia até realizar manipulações simples, como rotacionar as imagens, antes de armazená-las em um formato diferente.

Esqueci de dizer que o maior formato no PhotoCD era 4096x6144 pixels e (dependendo da imagem) um JPEG de 8 MB. Muitas pessoas (particularmente aquelas que possuem as atuais câmeras digitais profissionais) dirão que uma imagem de 8 MB não é tão grande. Mas era 1995 e a memória não custava US\$ 10 por gigabyte. Meu pequeno sistema Linux tinha somente 8 MB de memória principal, mas evidentemente tinha suporte a memória virtual. Eu pedia ao [xpcd](#) para ler uma foto do CD e ele o fazia relativamente rápido. Depois, eu pedia que ele rotacionasse a imagem, e o PC parecia estar tendo uma hemorragia interna. Felizmente, em pouco tempo consegui comprar mais 8 MB de memória e a minha manipulação de fotos ficou bem mais rápida.

No final dos anos 1990, comprei uma câmera digital e meus PhotoCDs foram relegados a uma mala. Recentemente, decidi olhar algumas fotos de 1995.

Descobri que a Kodak não produzia mais PhotoCDs, além de ter "abandonado" o formato, o que significava que havia terminado o suporte a seu programa.

Tirei os PhotoCDs da bolsa e procurei “PhotoCD” no repositório de softwares da minha distribuição. Nada.

Havia programas para JPEG, GIF, PNG e vários outros formatos, mas não PhotoCDs. Drogas... eu tinha milhares de fotos naqueles PhotoCDs!

Fui ao Google em busca de ajuda e descobri que a Kodak não produzia mais PhotoCDs, além de ter “abandonado” o formato, o que significava que havia terminado o suporte a seu programa e nem ao menos tinham antigos binários em seu site, para que os pobres usuários que tinham imagens neste formato pudessem abri-las algum dia. A Kodak possuía alguns documentos que descreviam os recursos de um PhotoCD, mas eram poucas informações.

Usando a busca do Google, encontrei alguns sites de usuários que falavam sobre PhotoCDs, incluindo um site do meu velho amigo [xpcd](#). Infelizmente, a última versão do [xpcd](#) foi atualizada em 2004, e um simples `configure` e `make` gerava um monte de erros que (naquele momento) eu realmente não queria investigar.

Felizmente, também encontrei o [pcdtojpeg](#) [2], um programa de linha de comando capaz de converter facilmente PhotoCDs para JPEGs. O programa foi compilado com relativa facilidade e eu estava salvo!

De agora em diante, sempre vou me assegurar de ter cópias dos códigos fonte tanto do [pcdtojpeg](#) quanto do [xpcd](#) em todos os meus computadores (isso é claro, se eu quiser continuar tendo acesso às fotos dos meus PhotoCDs). No futuro, posso gastar algum tempo no [xpcd](#) para fazê-lo funcionar no meu sistema e contribuir de volta. Também posso gastar algum tempo criando um programa [pcdtopnm](#) para converter todos os meus PhotoCDs Kodak. Claro, isso virá após o restante dos meus projetos em andamento... Carpe diem! ■

Mais informações

[1] XPCD:

<http://linux.bytesex.org/fbida/xpcd.html>

[2] pcdtojpeg:

<http://pcdtojpeg.sourceforge.net/Home.html>

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

Certificação Linux Número 1 no Mundo



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



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



LPIC-3: a primeira certificação 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



Coluna do Taurion

Situação atual do ODF e do OpenXML

Taurion aborda os padrões abertos e o andamento da adoção dos formatos de documento no mercado brasileiro atual.

O outro dia almoçava com um amigo que me perguntou como vão as coisas com o formato ODF no Brasil. Do ponto de vista dele, estão meio paradas. E do meu ponto de vista, também. Realmente, o assunto “padrão aberto de documentos” saiu do noticiário da mídia especializada, embora continue muito importante.

A cada dia, geramos mais e mais documentos eletrônicos. Provavelmente, nos próximos cinco anos geraremos tantos documentos digitais quantos foram gerados nos últimos 25 ou 30 anos. Sendo assim, adotar um padrão aberto para documentos é essencial, inclusive para os governos. Isso porque eles precisam compartilhar informações entre os seus diversos órgãos sem preocupar-se com incompatibilidades entre os formatos de documentos, além de ter que garantir a integridade e a perpetuidade dos seus documentos, que são a memória da nação, mesmo após o software que o criou ter desaparecido do mercado.

A adoção de um padrão aberto, independente de fornecedor, baseado em XML, garante que mesmo sem o software original, o documento continuará sendo acessado.

Um padrão aberto é fundamental para o nosso mundo globalizado e interligado. Por outro lado, padrões proprietários criam barreiras econômicas, pois a exigência de pagamento de *royalties* encarece os produtos e dificultam a competitividade.

Neste contexto, muitos governos já adotaram ou estão em vias de adotar o ODF (*Open Document Format*) como seu padrão aberto de documentos. Mas ainda vemos muita confusão e desinformação sobre essa questão, principalmente pelo surgimento de um padrão alternativo, o OpenXML, proposto pela Microsoft.

Ele foi proposto inicialmente como uma forma de preservar o espaço criado pelos formatos proprietários da suíte Office, diante das demandas dos governos por padrões abertos, que começavam a voltar sua atenção ao ODF. Para tornar o OpenXML aberto, seria fundamental que ele fosse aceito pela ISO (*Organização*

Internacional de Padrões). Depois de muitos debates e discussões, a Microsoft concordou em criar duas classes de conformidade: a *Transitional*, que incluía componentes que dependiam diretamente de recursos disponíveis exclusivamente no sistema Windows, e que seria adotada como meio de facilitar a transição dos documentos legados, em formato proprietário, para o padrão aberto.

Esta classe de conformidade deveria ser usada, portanto, apenas para a migração e não para a criação de novos documentos. A outra classe, *Strict*, satisfazia as demandas da ISO e o OpenXML foi então aprovado como padrão aberto pela entidade, como ISO/IEC 29500, em março de 2008.

Mas como estão as coisas agora, em 2010? O ODF está sendo adotado por governos de vários países do mundo, inclusive Brasil. O OpenXML, por sua vez, é implementado por um conjunto de versões diferentes, o que gera incompatibilidade e riscos à preservação de acessos futuros aos documentos. Por exemplo, a versão *Transitional* não deve ser usada para gerar novos documentos e é interessante que nem mesmo os produtos Office 2007 e 2010 da Microsoft conseguiram implementar todas as especificações dessa versão.

A classe *Strict* é a que deve ser usada para gerar novos documentos. Mas nem mesmo o Office 2010 consegue gravar arquivos nessa versão. Na prática, ao não implementar a classe e criar extensões proprietárias, a Microsoft mantém sua estratégia de padrão fechado, embora agora com uma camada de verniz para ser chamado de “aberto”.

Minha recomendação é que as empresas e governos continuem adotando o padrão ODF e fiquem alertas para não adotarem o OpenXML em uma versão que não seja a *Strict*. ■

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

Interoperabilidade

Convivência harmoniosa

Nos dias atuais, é possível manter sistemas operacionais distintos operando em sintonia. Bem-vindo ao mundo da interoperabilidade.

por Flávia Jobstraibizer

Feliz é o administrador de redes que pode se dar ao luxo de trabalhar com uma arquitetura homogênea, com apenas um tipo e modelo de sistema operacional. No entanto, são pouquíssimas as empresas que se enquadram nessa realidade – se é que existem. Se você tem interesse em solucionar problemas reais em redes de verdade, é impossível escapar das agruras da integração de recursos dos sistemas operacionais GNU/Linux e Windows.

Até pouco tempo atrás, eram comuns os graves e sérios problemas que a convivência entre sistemas operacionais diversos em uma mesma rede causavam. Hoje em dia a harmonia é possível, através de ferramentas e soluções cada vez mais modernas e transparentes aos usuários, minimizando os problemas que os diferentes sistemas antigamente causavam a administradores e, muitas vezes, até usuários.

É comum o administrador de redes encontrar problemas para acessar arquivos, diretórios ou recursos da rede, ou mesmo estar seguro de que um arquivo gravado a partir de um cliente Linux, não foi corrompido no momento de seu armazenamento em um diretório NTFS em uma máquina Windows. Para resolver este problema de acesso a partições NTFS, o artigo “Obstáculos superados” aborda o uso do Ntfs-3g, que permite acesso de leitura e es-

crita a partições NTFS com rapidez e agilidade.

No caso de servidores GNU/Linux, as tarefas na área da interoperabilidade começam com a configuração dos serviços Samba e OpenLDAP, com a devida integração entre si, tema que é abordado em um dos artigos desta edição.

Ainda na edição deste mês da **Linux Magazine** oferecemos diversos artigos úteis para que você possa integrar servidores e clientes Windows modernos à sua rede heterogênea já em funcionamento, como por exemplo, um artigo sobre a ferramenta GOsa, que fornece ao administrador de redes uma interface mais ágil e amigável para gerenciar grupos e usuários em sua base de dados LDAP.

Outro recurso interessante, é a integração da autenticação no Linux com múltiplos domínios Microsoft Active Directory por meio do Fedora 389 Directory Server, com encadeamento e autenticação de tráfego.

Esta edição traz conhecimentos imprescindíveis e aborda recursos necessários que todo bom administrador de redes deve ter sempre à mão. Boa leitura! ■

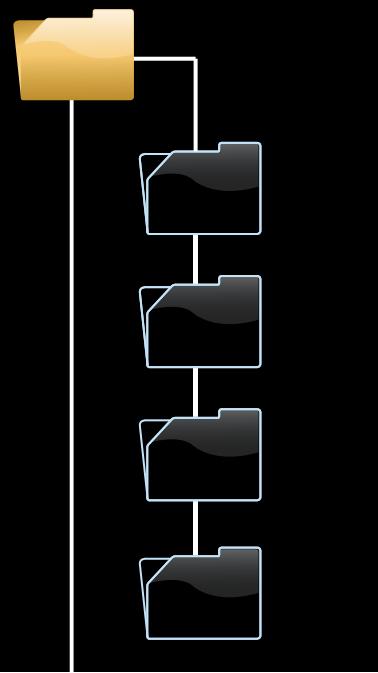
Matérias de capa

Diretórios virtuais	34
Obstáculos superados	40
União perfeita	38
Administração centralizada com OpenLDAP	44
Mais que uma interface bonita	48
Administração versátil	52



Diretórios virtuais

Aprenda a integrar a autenticação no Linux com múltiplos domínios Microsoft Active Directory por meio do Fedora 389 Directory Server, com encadeamento e autenticação de tráfego.
por **Alex Davies e Alessandro Orsaria**



É relativamente fácil configurar um sistema de gerenciamento de identidades em um ambiente com um único sistema operacional, mas a coisa fica mais complicada em uma configuração com múltiplos sistemas operacionais e diferentes sistemas de gerenciamento de identidades coexistentes. Este artigo explora a integração de clientes Linux em um ambiente com múltiplos domínios Microsoft Windows Active Directory (AD).

Embora esse problema tenha várias soluções ([quadro 1](#)), este artigo terá como foco o 389 Directory Server (389 DS) do Fedora, um servidor LDAP seguro e altamente escalonável com diversos recursos avançados, incluindo replicação multi-mestre, sincronização de usuários e grupos a partir do Active Directory e a capacidade de virtualizar outros diretórios LDAP.

Arquitetura

A [figura 1](#) mostra um panorama da arquitetura referida neste artigo. Há dois controladores de domínio Windows disponíveis, cada um pertencente a uma floresta diferente com os contextos `dc=foo`, `dc=example`, `dc=local` e `dc=bar`. O objetivo é autenticar usuários SSH que estejam

acessando clientes Linux por meio das credenciais de usuário e senha armazenadas nos servidores do AD. O servidor de diretório encaminha as buscas efetuadas no LDAP e associa requisições ao servidor LDAP/AD apropriado, sem necessidade de sincronizar qualquer dado.

Essa técnica possui algumas vantagens sobre o *Windows Sync* – por exemplo, quando há a necessidade de agregar rapidamente múltiplos controladores AD em uma única máquina LDAP ou em ambientes nos quais a sincronização de usuários e senhas do Active Directory possua muita complexidade. Para máxima flexibilidade, mantemos todas as informações de usuários (nomes de usuário, UID, shell etc.) no Active Directory, com os grupos de autorização no 389 DS. Testamos nossa configuração no RHEL5 e no Windows Server 2003 R2, mas ela também deve funcionar em outras distribuições Linux recentes, especialmente o CentOS, com pequenas modificações.

Se termos como *sufixo*, *distinguished name* e *atributo* soam pouco familiares, talvez seja interessante dedicar algum tempo ao aprendizado do funcionamento do LDAP. O [quadro 2](#) é um ponto inicial, mas se você precisar de uma explicação

mais aprofundada, o livro de Gerald Carter, *LDAP System Administration* [\[1\]](#) é uma ótima referência para começar.

AD e atributos Unix

A primeira etapa é permitir que os servidores AD armazenem informações do Unix como UIDs, GIDs, diretórios `home` etc. Em um servidor AD com Windows 2003 R2, é possível configurar o suporte a Unix por meio da instalação do *Identity Management for Unix*, também disponível no Windows 2008. A instalação deste pacote é simples, então não incluímos detalhes (supomos que você tenha intimidade com instaladores gráficos do tipo *Next → Next → Finish*). No *Painel de Controle* do Windows 2003 R2, apenas clique em *Adicionar ou Remover Programas*, em seguida em *Adicionar/Remover Componentes do Windows*, e selecione *Identity Management for Unix* como mostra a [figura 2](#). Mesmo que seja solicitado, não é preciso criar um domínio NIS.

Com a instalação completa, o schema LDAP que oferece a estrutura do AD está estendido. Para ver provas dessas novas configurações, edite a conta de um usuário que você deseja autenticar nas máquinas Linux, como você faria normal-

Quadro 1: Soluções de gerenciamento de identidades

Clientes Linux geralmente usam o módulo `nss-ldap` para recuperar informações de usuários e grupos a partir de servidores LDAP. Porém, esse módulo não possui meios para solicitar informações de acesso de usuários a múltiplos servidores LDAP e agregar as respostas de volta aos clientes.

Com múltiplas instâncias Active Directory, há três técnicas principais de gerenciamento de identidades que funcionam para clientes Linux e Windows: replicação, diretórios virtuais e clientes especializados.

Muitos servidores de diretório, como o *OpenLDAP*, 389 DS e *Oracle Internet Directory*, possuem recursos embutidos para sincronizar entradas do Active Directory. Embora a replicação de objetos de usuários e grupos funcione bem na maioria dos casos, ela tem algumas limitações.

Primeiramente, apenas uma pequena parcela dos atributos pode ser replicada. Além disso, sincronizar senhas do AD pode ser maçante de gerenciar, principalmente em grandes infraestruturas de Active Directory. Como alternativa, sempre é possível redirecionar requisições de autenticação ao AD via SASL ou LDAP, como descrito neste artigo.

Se a replicação do AD não for possível ou recomendável, os diretórios virtuais oferecem uma rápida alternativa para configurar repositórios centralizados atuando como proxy de requisições LDAP para outros servidores. O 389 DS oferece algumas capacidades de diretórios virtuais, embora faltem recursos mais avançados como mapeamentos de atributos.

Clientes especializados incluem o *Samba* ou o *Winbind* – que pode ser usado para realizar a conexão a um controlador Windows – e softwares como o *Likewise Enterprise*, também disponível em uma versão livre [8]. O Likewise ainda tem o benefício de integrar-se com as políticas de grupo do AD para controlar aspectos do gerenciamento de identidades do Linux assim como de Windows e Mac.

mente no Active Directory. Deverá ser exibida uma nova aba, chamada *Unix Attributes*. Selecione-a para fornecer os atributos de usuário do Unix (UID, GID, shell etc.), como mostra a [figura 3](#).

Instalação do 389 DS

Este artigo não vai a fundo em todas as opções de configuração do 389 DS – para isso há ótimos artigos na web – mas o melhor ponto de partida para mais estudos é a documentação do *Red Hat Directory Server* [2]. Na realidade, o 389 DS é simplesmente a base de código do *Red Hat Directory Server*. Se você não tiver tempo para percorrer o guia de administração do 389 DS, que, infelizmente, tem o tamanho da lista telefônica de São Paulo, há alguns manuais do tipo “como fazer” na página oficial de documentação do 389 DS no site do Projeto Fedora [3].

Instalar o OpenJDK 1.6.0 ou o Sun JDK 1.6.0 é um pré-requisito para o correto funcionamento do 389 DS. No caso do OpenJDK, isto é tão sim-

ples quanto executar o comando `yum install java-1.6.0-openjdk`. Se você tiver mais de uma versão do JDK em seu sistema, selecione a versão padrão com a alternativa `--config java`.

Em seguida, instale o pacote `RPM 389-ds` e todas as suas dependências por meio do `yum`. Se este pacote não estiver incluído na sua distribuição Linux, é possível encontrá-lo no

repositório `yum EPEL (Extra Packages for Enterprise Linux)` [4]; para adicionar o EPEL, baixe e instale o pacote `epel-release-5-3.noarch.rpm`.

Por último, execute o script `setup-admin.pl` para configurar o servidor de diretórios. Talvez seja exibido um aviso a respeito do número de descriptores de arquivos disponíveis, ou uma sugestão para reduzir o tem-

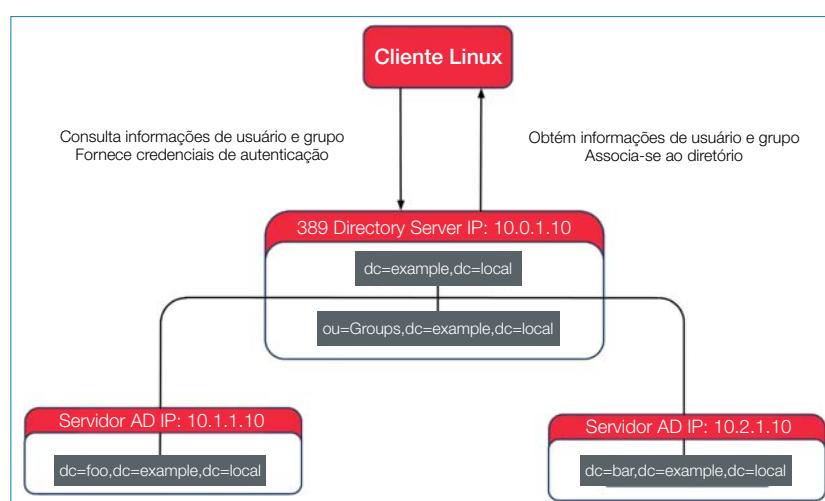


Figura 1 Este diagrama mostra a arquitetura de alto nível de um cliente Linux, uma máquina 389 DS e dois servidores AD.

Quadro 2: O básico sobre o LDAP

O *Lightweight Directory Access Protocol* (LDAP) é um protocolo aberto para armazenar, acessar e atualizar informações em um diretório. Um diretório é um tipo particular de banco de dados otimizado para operações de leitura; o LDAP define o formato das mensagens (busca, modificação, exclusão etc.) trocadas entre um cliente e um servidor de diretório.

Diretórios contêm entradas, que por sua vez contêm atributos, que podem ou não ser opcionais, dependendo das classes de objetos às quais essas entradas pertencem. Cada atributo possui um tipo, que possui uma sintaxe que define quais valores o atributo pode armazenar. Diretórios são organizados em uma estrutura semelhante a uma árvore, com base em seu *distinguished name* (DN), que é composto de uma sequência de DNs relativos (RDNs).

Por exemplo, `cn=Alex, ou=IT, dc=example, dc=com` é o DN de uma entrada, que representa o usuário com o nome (nome comum, ou *common name*, daí o `cn`), `Alex` na unidade organizacional `IT` do diretório com sufixo raiz `dc=example, dc=com`. Essa entrada poderia ser do tipo *person*, que possui campos obrigatórios e opcionais, como `sn` (sobrenome) e `telephoneNumber`. Também pode pertencer a mais classes de objetos, como `posixAccount`, que define outros atributos como `uidNumber`, `gidNumber` e `loginShell`.

Diretórios LDAP podem ser usados para gerenciar contas de usuários em um repositório central e, ao longo dos anos, substituíram outros sistemas centralizados de gerenciamento de usuários, como o NIS.

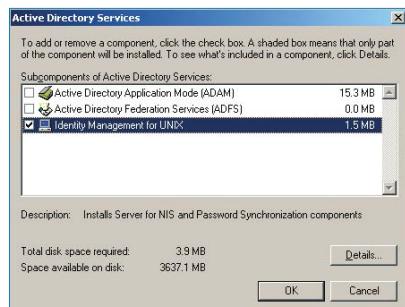


Figura 2 Instalação do Identity Management for Unix.

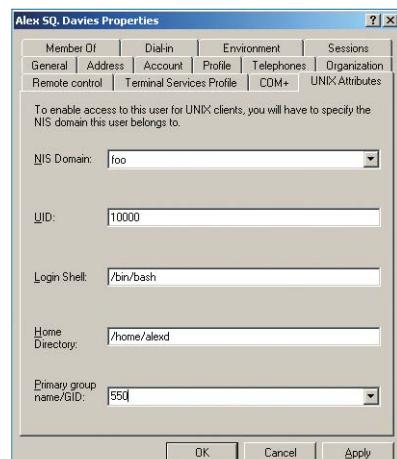


Figura 3 Configuração dos atributos do Unix para um usuário no AD.

```
chkconfig dirsrv on
chkconfig dirsrv-admin on
```

Para gerenciar seu novo servidor LDAP, há um console de gerenciamento em Java, que pode ser iniciado com o comando `389-console`. Este cliente também está disponível na forma de um instalador para Windows [\[6\]](#).

Configuração de encaminhamento

Agora que o `389 DS` está instalado, ele precisa ser configurado para encaminhar consultas LDAP destinadas a `dc=foo, dc=example, dc=local` e `dc=bar`, para os controladores de domínio Windows. Para configurar o encaminhamento, abra o cliente `389 DS` recém-instalado (que pode ser executado no servidor LDAP ou em qualquer outra máquina) e conecte-se com o nome de usuário `cn=Directory Manager` à porta `9830` do seu servidor `389 DS`, como mostra a **figura 4**. Se tudo acontecer como esperado, a janela principal do *Management Console* será exibida.

Em seguida, expanda o menu da esquerda para selecionar o servidor de diretórios e clique em *Open*, como mostra a **figura 5**. Dê um clique com o botão direito no sufixo raiz `dc=example, dc=local` sob a aba *Configuration* e selecione a opção *New Root Sub-Suffix*. Na janela que abrir, desmarque a caixa e crie um sufixo com o mesmo *distinguished name* do seu domínio AD, como ilustra a **figura 6**.

Depois disso, expanda o novo sufixo, clique nele com o botão direito e selecione *New Database Link*. Digite um nome para o link do banco de dados e o IP do controlador Windows remoto. O *Active Directory* normalmente não permite acesso de leitura anônimo, então é preciso fornecer o *distinguished name* e a senha de um usuário com permissões de efetuar



Figura 4 Login em um servidor 389 DS como *Directory Manager*.

pesquisas no AD. Em um ambiente de produção, é altamente recomendável usar TLS para proteger essas credenciais. Para manter a concisão, este artigo não cobre a configuração do TLS, então a saída completa apresentada na [figura 7](#) mostra a opção *Simple Bind* selecionada para fins de teste.

O próximo passo é modificar alguns poucos parâmetros de configuração para que o encaminhamento funcione corretamente. Vá até a aba *Directory*, expanda os itens *config/plugins/chaining* e dê um duplo clique no nome do banco de dados associado ao AD. Altere o valor do atributo *ns-ProxiedAuthorization* para *off*. Isto faz o 389 DS desativar a autorização via proxy e executar todas as requisições de operações encaminhadas como o usuário especificado na tela anterior.

Agora, pare o serviço do 389 DS com o comando `service dirsrv stop`. Edite o arquivo `/etc/dirsrv/slapd-*/dse.ldif` e procure por uma seção que começa com `dn:cn=chaining database, cn=plugins, cn=config`.

Apague todas as linhas desta seção que contenham a informação `nstransmitted-controls`. Isto desativa alguns controles que o sufixo encaminhado envia – o que pode causar problemas. Por último, salve o arquivo e inicie o serviço com o comando `service dirsrv start`. Neste ponto, já deve ser possível consultar o 389 DS local em busca de usuários adicionados ao Active Directory, por exemplo, usando a seguinte sintaxe:

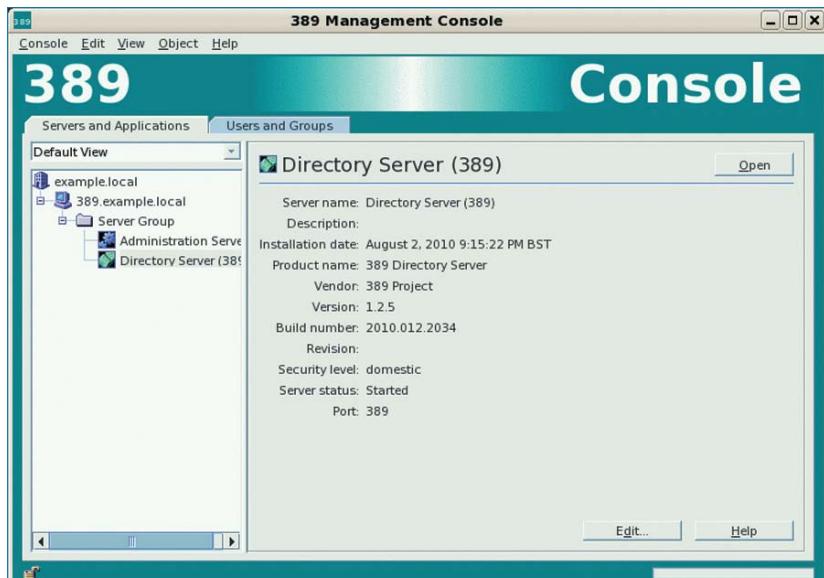


Figura 5 Conexão ao diretório real como *Directory Manager*.

`ldapsearch -x -b dc=example,dc=local "(uid=alex)"`

Para incluir os usuários armazenados dentro do controlador de domínio da segunda organização nos resultados retornados pelo novo diretório virtual, simplesmente repita boa parte deste processo: crie um novo subsufixo e uma nova conexão de banco de dados. Lembre-se que o controlador de domínio Windows para o qual você está apontando precisa possuir uma conta que possa ser usada para consultas, e ele também precisa ter instalado o *Identity Management for Unix*.

Um problema que pode ocorrer quando dois domínios AD forem unidos por um diretório virtual é que os atributos do Unix, como UID, podem gerar conflitos. Isto pode ser solucionado atribuindo-se diferentes faixas de UIDs a diferentes domínios AD. Embora existam métodos para configurar esse comportamento, eles não serão cobertos neste artigo.

Outra questão potencial é que o Active Directory retorna objetos em páginas com 1.000 entradas cada, enquanto que o plugin de encaminhamento do 389 DS não suporta resultados paginados. Isto significa

que se você possuir mais de 1.000 usuários com atributos Unix no Active Directory, somente receberá uma lista parcial dos usuários ao realizar buscas a partir do 389 DS. Para corrigir este problema, pode-se modificar o parâmetro padrão *MaxPageSize* do AD conforme descrito no artigo 315071 [\[7\]](#) da Microsoft Knowledge Base.

Autenticação pass-through

Até aqui, foi descrito como recuperar usuários e grupos a partir de múltiplos servidores Active Directory usando o 389 DS. A próxima etapa consiste em configurá-lo para encaminhar ao controlador de domínio Windows adequado as requisições de autenticação LDAP de entradas que

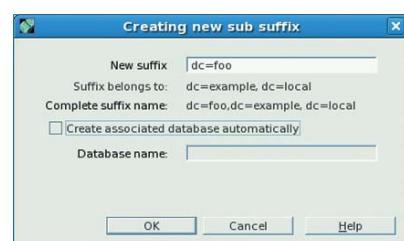


Figura 6 Criação de um novo subsufixo raiz.

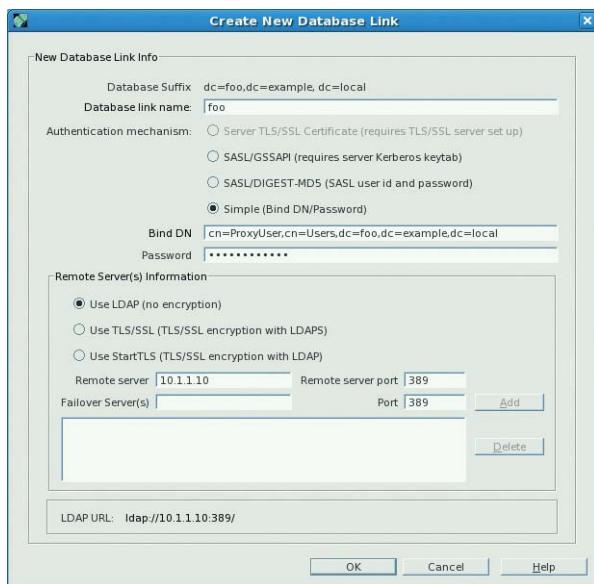


Figura 7 Configuração de um link de banco de dados para o Active Directory.

não estejam armazenadas no banco de dados local. O plugin de autenticação `pass-through` (PTA) pode ser

guração ao 389 DS.

Por último, reinicie o servidor de diretório com o comando `service dirsrv restart`. Isto permite

usado para isso, e é extremamente fácil de configurar.

Primeiramente, crie um arquivo **LDIF** com o mesmo conteúdo do `pta.ldif` mostrado na **listagem 1** (**LDIF** é o formato padrão usado para descrever entradas de diretório). Em seguida, execute o comando `ldapmodify -x -D "cn=Directory Manager" -W -f pta.ldif` para aplicar as alterações de configuração ao 389 DS.

Por último, reinicie o servidor de diretório com o comando `service dirsrv restart`. Isto permite que o 389 DS direcione requisições aos sufixos `foo` e `bar` para o servidor Windows Active Directory adequado, como especificado no arquivo `pta.ldif`. Novamente, neste exemplo foi omitida a criptografia TLS para manter a concisão, mas é altamente recomendável ativá-la em ambientes de produção.

Clientes Linux

Com esta infraestrutura criada, podemos configurar os clientes Linux. Primeiro, certifique-se de que os pacotes RPM `nss_ldap` e `pam_ldap` estejam instalados nos clientes. Em seguida, modifique o arquivo `/etc/ldap.conf` conforme exibido na **listagem 2**. Este arquivo especifica a URI da máquina 389 DS à qual se conectar, o *distinguished name* de base a ser usado em buscas e alguns outros parâmetros.

É preciso configurar os clientes Linux para usar o 389 DS para recuperar informações de usuários e grupos. Modifique as linhas `passwd:` e `group:` do arquivo `/etc/nsswitch.conf` como mostra a **listagem 3**. Se tudo correr bem, neste momento deve ser possível obter a lista com-

Listagem 1: Criação do arquivo `pta.ldif`

```
01 dn: cn=Pass Through Authentication,cn=plugins,cn=config
02 nsslapd-pluginEnabled: on
03 nsslapd-pluginarg0: ldap://10.1.1.10/dc=foo,dc=example,dc=local
04 nsslapd-pluginarg1: ldap://10.2.1.10/dc=bar,dc=example,dc=local
```

Listagem 2: Modificação do arquivo `/etc/ldap.conf`

```
01 scope sub
02 ldap_version 3
03
04 # Não seguir "referrals".
05 # Seguir referrals envia o cliente a todos os domínios de uma floresta AD, o que leva muito tempo e não tem vantagens
06 referrals no
07
08
09 # Filtrar somente usuários/grupos com atributos Unix
10 # (gera grande ganho de desempenho)
11 nss_base_passwd dc=example,dc=local?sub?&(uidNumber=*)
12 nss_base_group dc=example,dc=local?sub?&(gidNumber=*)
13 nss_initgroups_ignoreusers root,ldap,dbus,xfs,haldaemon,nscd,nopulse
14
15 # Se não for 'soft', a máquina pode paralisar na inicialização
16 # ou ter outros efeitos horríveis se não conseguir acesso ao servidor
17 bind_policy soft
18
19 uri ldap://10.0.1.10:389/
20
21 # DN base para iniciar a busca
22 base dc=example,dc=local
23
24 # Mapeamentos do Active Directory
25 nss_schema rfc2307bis
26 nss_map_objectclass posixAccount organizationalPerson
27 nss_map_attribute homeDirectory unixHomeDirectory
28 nss_initgroups backlink
29
30 # Com custo de repetição excessiva, use StartTLS ou
31 # LDAP sobre SSL em ambientes de produção
32 ssl no
```

pletea de usuários locais do AD com o comando `getent passwd`.

O próximo passo é configurar os clientes Linux para usarem o 389 DS para a autenticação de usuários. O módulo `pam_ldap` é responsável por isso, e na maioria das distribuições da família Red Hat ele usa o `system-auth-ac` para fornecer uma interface comum de configuração para `daemons` de serviço. A **listagem 4** mostra um exemplo em funcionamento do `system-auth-ac`, que também usa o módulo `pam_mkhomedir` para criar o diretório `home` de um usuário automaticamente caso ele não exista quando o usuário fizer login. Neste ponto, já deve ser possível fazer login no cliente Linux usando uma conta configurada em um dos controladores de domínio Windows.

Uma etapa de configuração opcional é ativar o daemon `nscd`. Ele pode aumentar o desempenho por meio do *cache* de requisições de usuários e grupos. É possível ativar e iniciar o `nscd` usando os seguintes comandos:

```
chkconfig nscd on
service nscd start
```

Da autenticação à autorização

Descrevemos como obter usuários a partir de múltiplos servidores Active Directory usando o 389 DS e como encaminhar requisições LDAP aos servidores AD. Essa configuração é útil caso todos os usuários tenham permissão de login em todos os servidores, mas raramente esse é o caso. Normalmente, diferentes usuários têm permissão de login em máquinas distintas, então é preciso um método para reconhecer quais usuários têm autorização de login em cada servidor. Para isso, o `pam_access` oferece uma forma fácil de configurar o gerenciamento de acesso. Em cada cliente Linux, é preciso estabelecer

quais usuários devem ter direitos de acesso e criar grupos de usuários no 389 DS, que depois serão referenciados na configuração do módulo do PAM.

Para criar um grupo no 389 DS, é possível usar tanto um console gráfico quanto a linha de comando. A **listagem 5** mostra um exemplo de arquivo LDIF que descreve um objeto de grupo, cujos membros são identificados pelo atributo `uniqueMember`. Após o arquivo `linuxadmins.ldif` ser criado (conforme a **listagem 5**), o seguinte comando cria o novo objeto de grupo no 389 DS: `ldapmodify -x -D "cn=Directory Manager" -W -f linuxadmins.ldif`.

Neste ponto, já é possível especificar quais combinações de usuários e grupos têm direito a login em cada máquina. Especifique esses usuários e grupos editando o arquivo `/etc/security/access.conf`. A **listagem 6** contém um trecho que mostra como o arquivo `access.conf` pode ser configurado.

As duas primeiras linhas permitem que os usuários `root` e `joe` façam login a partir da máquina local e em qualquer lugar, respectivamente. Depois, a terceira linha permite ao grupo `LinuxAdmins` acesso ao servidor `server1.example.local` a partir de qualquer máquina da rede `10.1.1.0/24`. Por último, a

Listagem 3: Configuração dos clientes Linux com /etc/nsswitch.conf

```
01 passwd: files ldap
02 group: files ldap
```

Listagem 4: Exemplo de funcionamento do /etc/pam.d/system-auth-ac

```
01 # Este arquivo é auto-gerado.
02 # Mas modificado pelo Alex
03 # Alterações manuais serão destruídas na próxima execução do authconfig.
04 # Então por favor não faça nada :p
05 auth required pam_env.so
06 auth sufficient pam_unix.so nullok try_first_pass
07 auth requisite pam_succeed_if.so uid >= 500 quiet
08 auth sufficient pam_ldap.so use_first_pass
09 auth required pam_deny.so
10
11 account required pam_unix.so broken_shadow
12 account sufficient pam_succeed_if.so uid < 500 quiet
13 account default=bad success=ok pam_ldap.so
14 account required pam_permit.so
15
16 password requisite pam_cracklib.so try_first_pass retry=3
17 password sufficient pam_unix.so md5 shadow nullok try_first_pass use_authtok
18 password required pam_deny.so
19
20 # Criar diretório home
21 session optional pam_mkhomedir.so skel=/etc/skel/ umask=0077
22 session optional pam_keyinit.so revoke
23 session required pam_limits.so
24 session success=1 pam_succeed_if.so service in crond quiet use_uid
25 session required pam_unix.so
26 session optional pam_ldap.so
```

Listagem 5: Objeto de grupo

```
01 dn: cn=LinuxAdmins,ou=Groups,dc=example,dc=local
02 gidNumber: 500
03 objectClass: top
04 objectClass: groupOfUniqueNames
05 objectClass: posixgroup
06 cn: LinuxAdmins
07 uniqueMember: CN=Alessandro Orsaria,CN=Users,DC=bar,DC=example,DC=local
08 uniqueMember: CN=Alex SQ. Davies,CN=Users,DC=foo,DC=example,DC=local
```

Listagem 6: Trecho de configuração do arquivo access.conf

```
01 + : root : LOCAL
02 + : joe : ALL
03 + : LinuxAdmins@server1.example.local : 10.1.1.0/24
04 - : ALL : ALL
```

última linha nega acesso a todos os demais.

A última etapa é configurar o PAM para usar as diretivas especificadas em `access.conf`. Esta etapa é fácil por meio da adição da seguinte linha ao arquivo `/etc/pam.d/system-auth-ac`: `account required pam_access.so`.

Falhas no controlador de domínio

Até agora não consideramos as consequências de uma falha no 389 DS de um controlador de domínio Windows.

Felizmente, tornar este sistema mais confiável é extremamente simples. Primeiramente, é preciso mais um 389 DS instalado e com a mesma configuração ilustrada anteriormente. Considere ativar a replicação para sincronizar todos os objetos locais.

Gostou do artigo?

Queremos ouvir sua opinião.
Fale conosco em
cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4605>

tiplos servidores de autenticação, inseridos em uma lista separada por espaços.

Por último, é possível configurar os clientes Linux para obterem usuários e grupos a partir de um servidor 389 DS alternativo caso o primário esteja inativo especificando uma URI alternativa em `/etc/ldap.conf`. Também pode valer a pena ajustar os tempos máximos de consulta de forma que, caso um servidor LDAP esteja indisponível, o cliente consulte outra máquina em um intervalo de tempo aceitável.

Conclusão

A integração do gerenciamento de identidades entre Linux e Windows certamente é uma tarefa desafiadora, já que o Active Directory não foi feito para interoperar bem com outros servidores LDAP. Este artigo oferece uma técnica útil para integrar clientes Linux a um ambiente Active Directory. O objetivo é que as técnicas descritas aqui ajudem a criar e manter sua infraestrutura de autenticação simples e facilmente integrada a servidores AD. ■

Mais informações

- [1] LDAP System Administration; de Gerald Carter; Editora O'Reilly, 2003
- [2] Documentação do Red Hat Directory Server:
<http://www.redhat.com/docs/manuals/dir-server/>
- [3] Documentação do 389 DS no Fedora:
<http://directory.fedoraproject.org/wiki/Documentation/>
- [4] Repositório de pacotes EPEL:
<http://download.fedoraproject.org/pub/epel/5/>
- [5] Ajuste de desempenho do 389 DS no Fedora:
http://directory.fedoraproject.org/wiki/Performance_Tuning/
- [6] Página de download do 389 DS no Fedora: <http://directory.fedoraproject.org/wiki/Download/>
- [7] Como visualizar e definir políticas LDAP no Active Directory:
<http://support.microsoft.com/kb/315071/>
- [8] Likewise Open: <http://www.likewiseopen.org/>

Livro Certificação LPI-2 2ª edição



A Linux Magazine está lançando a **2ª edição revisada e ampliada** do livro que te prepara para a Certificação LPI-2 com as seguintes novidades:

- Exercícios em todos os tópicos
- Todo conteúdo ampliado para a nova versão da prova, atualizada em abril/2009

Garanta já o seu pelo site da Linux Magazine
www.linuxmagazine.com.br

Acesso a partições NTFS

CAPA

Obstáculos superados

Se você precisa acessar partições NTFS do Windows XP, Vista ou 7 a partir de um sistema GNU/Linux, aprenda como utilizar o Ntfs-3g, que permite acesso de leitura e escrita a partições NTFS com rapidez e agilidade.

por Thomas Leichtenstern e Kristian Kissling

Ondejfranta - sxc.hu

Discos formatados com NTFS costumavam ser um pesadelo para usuários Linux. Com alguma sorte, era possível conseguir ler o conteúdo do disco, mas em operação de gravação sempre havia o risco de perda de dados. Os problemas com o NTFS significavam que o sistema de arquivos FAT32 era a forma mais comum de trocar dados entre Windows e Linux. Infelizmente, o FAT32 somente lida com arquivos de até 4 GB e não possui o recurso de *journal* (gravação de um *log* de todas as mudanças que serão feitas no sistema de arquivos antes da efetiva gravação dos dados), o que aumenta enormemente o risco de perda de dados. O

recurso de journal é importante, pois possibilita recuperar o estado anterior do disco após uma falha, sem perda de informações.

Esta situação mudou dramaticamente desde o lançamento do Ntfs-3g [1] [2] em 2007. O acesso de leitura e escrita a partições NTFS não é mais um problema. O programa maduro suplantou seus concorrentes, tanto o *Captive* quanto o módulo do kernel, e todas as distribuições mais recentes o utilizam. O **quadro 1** oferece um panorama dos utilitários disponíveis.

Como o Windows 7 usa o NTFS versão 3.1 – exatamente como seus antecessores XP e Vista – nada mudou em questões de acesso. Embora

o Ntfs-3g seja utilizado exclusivamente para montar partições NTFS, o pacote Ntfsprogs [3] inclui várias ferramentas para editar os dados de diversas formas.

Uso do Ntfs-3g

Várias das principais distribuições atualmente usam o Ntfs-3g como ferramenta padrão para montar partições NTFS. O gerenciador de arquivos *Nautilus* geralmente exibe nomes de partições ou seus UUIDs na coluna da esquerda (**quadro 2**). Para montar uma partição com total acesso de leitura e escrita, simplesmente clique na entrada correspondente. O caminho utilizado pelas

Quadro 1: Uma breve introdução às ferramentas do NTFS

O Ntfsprogs é uma coleção de ferramentas para manipular partições NTFS: o programa `ntfsresize`, por exemplo, permite alterar o tamanho de um volume NTFS, e o utilitário `mkntfs` cria um novo volume. Embora a coleção inclua o `ntfsmount`, uma ferramenta para montar partições NTFS, é uma boa ideia dar tratamento preferencial ao Ntfs-3g para isso. O desenvolvimento do Ntfs-3g ainda está a pleno vapor e oferece muito mais recursos. A última versão do Ntfsprogs, a 2.0, foi lançada em setembro de 2007. Porém, os repositórios do Ubuntu ainda incluem pacotes para elas, e a coleção Ntfsprogs é a base de programas como o GParted.

O Ntfs-3g é um *fork* da ferramenta `ntfsmount`, baseado no FUSE. Em março de 2010, os desenvolvedores lançaram a versão estável 2010.3.6, usada no Ubuntu 10.04. Segundo as notas de lançamento, a ferramenta agora melhorou seu suporte a UTF-8/UTF-16 e resolve datas

de arquivos mais rapidamente. Ela também oferece tratamento melhorado a partições criptografadas.

O módulo do kernel NTFS [4] é principalmente usado para acesso de leitura a volumes. Com a introdução do kernel 2.6.16, ele ganhou a capacidade de redimensionar arquivos. A última vez que seus desenvolvedores alteraram os planos futuros do projeto foi em maio de 2006, então é seguro supor que o projeto foi descontinuado. O código-fonte do módulo possui um *copyright* que data de 2005, o que novamente indica que nada mudou desde então.

A ferramenta *Captive* [5] utiliza os drivers originais do Windows para acessar o sistema de arquivos. O problema é que as operações de gravação são extremamente lentas. O desenvolvedor Jan Kratochvil não mantém maisativamente o *Captive*, segundo a lista de discussão.

distribuições Linux para montar a partição geralmente é `/media/UUID/`.

É possível montar partições NTFS manualmente ou permanentemente com um único parâmetro de montagem e por meio do arquivo `/etc/fstab`. Para começar, digite o comando `mount` em um console: `$ sudo mount -t ntfs -o rw,auto,user,nls=utf-8,umask=007,gid='id -g' /dev/sdaX /mnt`.

Este comando especifica o NTFS como sistema de arquivos (`-t ntfs`). O parâmetro `-o` permite acrescentar outros parâmetros ao comando de montagem. Por exemplo, `umask=0027` estipula que o usuário tem permissão de ler, gravar e executar arquivos e diretórios. Usuários que pertençam ao mesmo grupo (`gid='id -g'`) podem ler o diretório e executar programas, mas não têm permissão de escrita. Outros usuários não têm acesso ao sistema de arquivos. Se você fornecer um valor de `0000` aqui, qualquer usuário tem permissão de fazer qualquer coisa. Os fóruns de Linux possuem mais informações sobre permissões e também sobre o `umask` [6]. O arquivo de dispositivo que representa o disco é `/dev/sdaX`. O diretório `/mnt` é o local onde o disco será montado.

Para especificar o usuário a quem pertence o ponto de montagem, é possível utilizar também a opção `uid` seguida pelo ID do usuário. Para descobrir o ID de um usuário, execute o comando `id -u`. Isto explica por que a entrada de um único usuário é `uid='id -u'`. Se você utilizar múltiplas opções, separe-as com vírgulas como em `-o uid='id -u',umask=0027`.

Para montar partições NTFS que o Ubuntu não detecte automaticamente na inicialização, certifique-se de ter privilégios administrativos e adicione a seguinte linha ao arquivo `/etc/fstab`:

```
UUID=6CC40ABEC40A8A92 /media/
windows ntfs rw,auto,user,
nls=utf8, umask=007, gid=46 0 0
```

Quadro 2: UUID

O UUID – *Universally Unique Identifier* (Identificador Universalmente Único) atribui um número único a cada disco e partição. O Ubuntu usa esse número para se referir à mídia, a menos que você atribua um nome ao disco durante o particionamento. O arquivo `/etc/fstab` vem usando UUIDs para montar discos há algum tempo.

É preciso substituir o longo número após UUID pelo UUID da sua partição Windows. Use o comando `blkid` para descobri-lo. Crie a pasta `/media/windows` digitando o comando `sudo mkdir /media/windows` na linha de comando – este será o ponto de montagem do volume. Você já deve ter familiaridade com o restante dos parâmetros. Uma exceção é a entrada de ID de grupo, 46, que representa o grupo `plugdev` (o grupo que possui permissão para gerenciar mídias externas).

Desempenho e recursos especiais

O Ntfs-3g saiu-se muito bem em nossos testes. Por exemplo, não tivemos qualquer problema para criar

diretórios com 20 camadas de aninhamento – e nenhum problema para abri-los depois, no Windows. Os vários caracteres fora do padrão que o Windows usa para nomes de arquivos e diretórios foram tratados corretamente. E o Windows não teve problema para abrir pastas criadas no Ubuntu.

A maior restrição na versão do Ntfs-3g do Ubuntu é relacionada às permissões e à propriedade de usuário. Por exemplo, o Ubuntu inicialmente atribui as partições NTFS ao usuário que as monta e dá acesso para esse usuário – e somente para esse usuário – ler e escrever. Não é possível alterar posteriormente as permissões ou a propriedade de usuário para arquivos e pastas. ■

Mais informações

- [1] Ntfs-3g: <http://www.tuxera.com/>
- [2] Notas de lançamento: <http://www.tuxera.com/community/release-history/>
- [3] Ntfsprogs: <http://man-wiki.net/index.php/8:ntfsprogs/>
- [4] Módulo de kernel do NTFS: <http://sourceforge.net/projects/linux-ntfs/>
- [5] Captive: <http://www.jankratochvil.net/project/captive/>
- [6] Entenda permissões de arquivos: http://www.linuxforums.org/articles/file-permissions_94.html/

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4602>

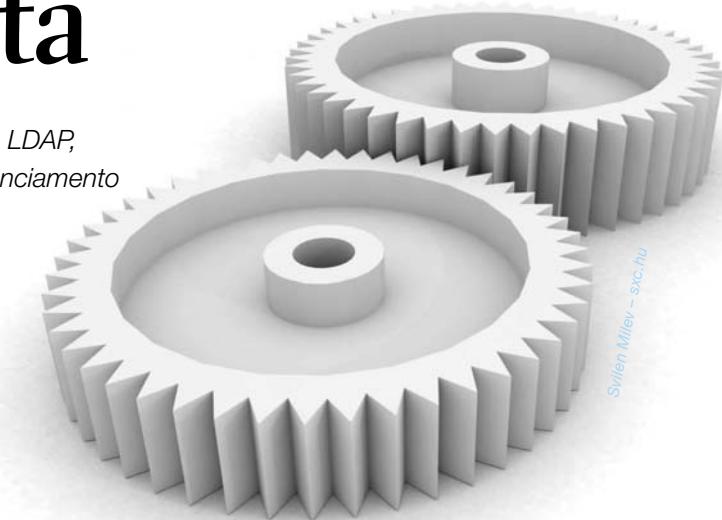


Samba e LDAP

União perfeita

A união das poderosas tecnologias Samba e LDAP, proporciona agilidade e simplicidade no gerenciamento de usuários de redes Linux e Windows.

por Marcos Amorim



Svetlin Mitev - sxc.hu

Que o Samba [1] é reconhecidamente uma das principais soluções para servidores de arquivos de rede, não temos dúvida. Porém, os ambientes onde a tecnologia costuma ser instalada

são maiores e para administrá-los são necessárias algumas ferramentas de auxílio. Neste artigo, vamos configurar um servidor Samba para autenticar-se em um servidor OpenLDAP. A configuração de um servidor

OpenLDAP pode ser encontrada entre os artigos desta edição.

Com o servidor OpenLDAP devidamente instalado e configurado, vamos prosseguir com a instalação do Samba e a integração dos dois serviços.

Listagem 1: Configuração do Samba

```

01 [global]
02 workgroup = LNMBR
03 server string = Servidor Samba na rede local
04 security = user
05 map to guest = Bad User
06 null passwords = Yes
07 passwd chat = *New*password* %n\n ↵
    *Retype*new*password* ↵
    %n\n*passwd:*all*authentication*tokens*updated*↵
    successfully*
08 log level = 1 vfs:0
09 syslog = 2
10 log file = /var/log/samba/%m.log
11 max log size = 10000
12 name resolve order = lmhosts wins bcast
13 socket options = TCP_NODELAY SO_RCVBUF=8192 ↵
    SO_SNDBUF=8192
14
15 # Informações de logon
16 logon script = netlogon.bat
17 logon path =
18 logon drive = H:
19 domain logons = Yes
20 os level = 200
21 preferred master = Yes
22 domain master = Yes
23 wins support = Yes
24 panic action = /usr/share/samba/panic-action %d
25
26 admin users = @domainadmin
27 create mask = 0640
28 directory mask = 0775
29 inherit permissions = Yes
30 inherit acls = Yes
31 nt acl support = No
32 map acl inherit = Yes
33
34 ## Integração ao OpenLDAP
35 ldap admin dn = cn=Admin,dc=linuxmagazine, ↵
    dc=com, dc=br
36 ldap group suffix = ou=Grupos
37 ldap idmap suffix = ou=Idmap
38 ldap machine suffix = ou=Computers
39 ldap passwd sync = Yes
40 ldap suffix = dc=linuxmagazine,dc=com,dc=br
41 ldap ssl = no
42 ldap user suffix = ou=Usuarios
43 passdb backend = ldapsam:ldap://127.0.0.1
44 passwd program = /usr/sbin/smbldap-passwd %u
45

```

LDAP com Samba

O uso do OpenLDAP é independente do Samba, mas o objetivo deste artigo é construir a solução completa, comumente utilizada em empresas. O cenário mais comum é integrar o servidor Samba à infraestrutura do OpenLDAP, que por sua vez se torna responsável por gerenciar os usuários e grupos de uma rede (tanto do Samba quanto do Unix) de forma centralizada.

Sem o OpenLDAP, cada usuário que precisar de uma pasta privada no servidor Samba precisará ser criado tanto no Samba quanto no sistema GNU/Linux do servidor, uma duplicação de tarefas pouco desejável. Com o OpenLDAP, os comandos `useradd` e `smbpasswd` podem ser esquecidos, pois ambos serão substituídos pelo comando `smbldap-useradd`.

Para os passos a seguir, é necessário que os pacotes dos servidores

Samba e OpenLDAP estejam instalados, assim como os utilitários e as ferramentas de integração do OpenLDAP ao restante do sistema GNU/Linux. Em sistemas derivados do Debian, o comando necessário para a instalação de tais pacotes é: `apt-get install samba smbldap-tools samba-doc libnss-ldap libpam-ldap smbclient`.

Algumas informações serão solicitadas durante a instalação, porém, mantenha as opções padrão, pois as configurações serão feitas manualmente.

A descrição dos campos do Samba para o OpenLDAP (que é a camada de “tradução” da configuração do Samba para o OpenLDAP), encontra-se no arquivo `samba3.schema` (ou `samba.schema`, dependendo da sua distribuição), que é geralmente instalado junto com o servidor Samba ou então através do pacote `samba-doc`. Esse arquivo

deve ser copiado para o diretório `/etc/ldap/schema/` (ou `/etc/openldap/schema/`) para ser utilizado de forma satisfatória pelo OpenLDAP:

```
# cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
# cd /etc/ldap/schema
# gunzip samba.schema.gz
```

Concluída essa tarefa, é preciso editar o arquivo de configuração do servidor OpenLDAP (`/etc/ldap/slapd.conf`) – este e outros arquivos de configuração, podem ser encontrados para download no site da **Linux Magazine**, em [2]) para fazer com que o OpenLDAP utilize o novo arquivo `.schema`.

Edito o arquivo `/etc/ldap/slapd.conf` e adicione o schema `include /etc/ldap/schema/samba.schema` abaixo na linha 9 do arquivo `slapd.conf`

```
46 ## Scripts das Smbldaptools
47
48 add machine script = /usr/sbin/smbldap-useradd -w "%u"
49 add user script = /usr/sbin/smbldap-useradd -a -m "%u"
50 delete user script = /usr/sbin/smbldap-userdel "%u"
51 add group script = /usr/sbin/smbldap-groupadd -o "%g"
52 delete group script = /usr/sbin/smbldap-groupdel "%g"
53 add user to group script = /usr/sbin/smbldap-groupmod -m "%g" "%u"
54 delete user from group script = /usr/sbin/smbldap-groupmod -x "%g" "%u"
55
56 # Compartilhamento de impressoras via Samba.
57 # somente as impressoras instaladas no servidor serão compartilhadas
58 # Compartilhamento de impressoras via Samba.
59 # somente as impressoras instaladas no servidor serão compartilhadas
60 [printers]
61 comment = All Printers
62 browseable = yes
63 path = /tmp
64 printable = yes
65 public = yes
66 writable = no
67 create mode = 0700
68
69 # Compartilhamento dos drivers de impressoras Windows.
70 # Por padrão, as estações buscam os drivers neste compartilhamento
71 [print$]
72 comment = Printer Drivers
73 path = /var/lib/samba/printers
74 browseable = yes
75 read only = yes
76 guest ok = no
77
78 # Compartilhamento do CD-ROM
79 [cdrom]
80 comment = Samba server's CD-ROM
81 writable = no
82 locking = no
83 path = /media/cdrom0
84 public = yes
```

Será necessário reiniciar os serviços do OpenLDAP para que este reconheça o novo schema adicionado. O reinício do OpenLDAP pode ser feito através do comando `/etc/init.d/slapd restart`.

Configuração do Samba

Neste momento estamos com tudo pronto para começar a configuração do Samba, então vamos editar os diversos arquivos de configurações de ambas as tecnologias. Vamos começar pelo arquivo `/etc/samba/smb.conf`, e as alterações necessárias estão presentes na [listagem 1](#).

Informe ao samba qual a senha do `ldap admin dn`, executando o comando `smbpasswd -w linux` e informando a senha.

PAM e nsswitch

É necessário configurar o PAM (*Pluggable Authentication Modules*) e o `nsswitch`, pois eles são necessários para reconhecer os usuários da base LDAP e autenticá-los no servidor. Com essas configurações feitas, os usuários poderão até mesmo fazer login via terminal usando `ssh`.

Configure o arquivo `/etc/libnss-ldap.conf`, desta forma:

```
base dc=linuxmagazine,dc=com,dc=br
uri ldap://localhost/
ldap_version 3
rootbinddn cn=admin,dc=linuxmagazine,dc=com,dc=br
```

Em seguida, configure a senha do administrador para a `libnss-ldap` e certifique-se de que o arquivo possui as permissões `600`: `/etc/libnss-ldap.secret`.

Estamos utilizando a senha `linux` como senha do administrador, mas você pode utilizar a senha que desejar. Configure o arquivo `/etc/pam_ldap.conf`, com as opções:

```
base dc=linuxmagazine,dc=com,dc=br
uri ldap://localhost/
ldap_version 3
rootbinddn cn=admin,dc=linuxmagazine,dc=com,dc=br
pam_password crypt
```

O que fizemos até o momento foi configurar o PAM e o `nsswitch` para conectar ao servidor LDAP. A

Listagem 2: Configuração do arquivo `/etc/smbldap-tools/smbldap.conf`

```
01 SID="S-1-5-21-2558116235-1446679944-621314221"
02 sambaDomain="LNM"
03 slaveLDAP="127.0.0.1"
04 slavePort="389"
05 masterLDAP="127.0.0.1"
06 masterPort="389"
07
08 ldapTLS="0"
09 verify="require"
10 cafile="/etc/smbldap-tools/ca.pem"
11 clientcert="/etc/smbldap-tools/smbldap-tools.pem"
12 clientkey="/etc/smbldap-tools/smbldap-tools.key"
13 suffix="dc=linuxmagazine,dc=com,dc=br"
14 usersdn="ou=Usuarios,${suffix}"
15 computersdn="ou=Computers,${suffix}"
16 groupsdn="ou=Grupos,${suffix}"
17 idmapdn="ou=Idmap,${suffix}"
18 sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
19
20 scope="sub"
21 hash_encrypt="SSHA"
22 crypt_salt_format="%s"
23
24 userLoginShell="/bin/bash"
25 userHome="/home/%U"
26 userHomeDirectoryMode="700"
27 userGecos="System User"
28
29 defaultUserGid="513"
30 defaultComputerGid="515"
31
32 skeletonDir="/etc/skel"
33 defaultMaxPasswordAge="45"
34
35 userSmbHome="\SERVSAMBA\%U"
36 userProfile="\SERVSAMBA\profiles\%U"
37 userHomeDrive="H:"
38 userScript="logon.bat"
39
40 mailDomain="linuxmagazine.com.br"
41 with_smbpasswd="0"
42 smbpasswd="/usr/bin/smbpasswd"
43 with_slappasswd="0"
44 slappasswd="/usr/sbin/slappasswd"
```

partir de agora vamos colocar essas alterações em produção e, para isso, será necessário editar alguns arquivos. No arquivo `/etc/nsswitch.conf`, crie a seguinte configuração:

```
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap
```

Já no arquivo `etc/pam.d/common-password`, basta informar o parâmetro `password sufficient pam_ldap.so`. Inclua o valor `auth sufficient pam_ldap.so` no arquivo `/etc/pam.d/common-auth` e por último, no arquivo `/etc/pam.d/common-account` defina: `account sufficient pam_ldap.so`.

Deste modo, finalizamos a configuração do PAM e do `nsswitch.conf`. Neste momento o servidor deverá estar configurado para ler as configurações de usuários e grupos que estão na base do LDAP.

Configurar o smb-ldap-tools

O `smbldap-tools` é um conjunto de scripts confeccionados em PERL que facilita muito a vida do administrador de redes. Uma de suas principais vantagens é que, através de comandos simples, podemos adicionar, remover e alterar informações dos usuários e grupos que estão na base LDAP, sem a necessidade de entender ou criar arquivos LDIF.

Antes de iniciar a configuração do `smbldap-tools`, é necessário saber qual é o SID do servidor samba. Para isso basta executar o comando: `# net getlocalsid`.

A saída desse comando deve ser algo como `SID for domain SERVSAMBA is: S-1-5-21-2558116235-1446679944-621314221`. Vamos utilizar esses valores na configuração do arquivo `/etc/smbldap-tools/smbldap.conf`, conforme a **listagem 2**.

Após a configuração do `smbldap.conf` é necessário informar qual é o usuário e a senha que possui direitos para adicionar, remover e alterar a base LDAP. No `smbldap-tools` esse arquivo é o `/etc/smbldap-tools/smbldap_bind.conf`. Ao criá-lo, certifique-se de que as permissões desses arquivos sejam `600`, para que somente o usuário `root` possa lê-los.

```
slaveDN="cn=Admin,dc=linux➡
magazine,dc=com,dc=br"
slavePw="linux"
masterDN="cn=Admin,dc=linux➡
magazine,dc=com,dc=br"
masterPw="linux"
```

Finalizando a configuração do servidor, é necessário popular a base de dados com as informações de grupos e usuários. Para isso, o script `smbldap-populate` pode nos ajudar a configurar a maioria dos grupos e outras informações. Use esse script com cuidado, caso a sua base já possua alguns obje-

tos, pois o `smbldap-tools` irá tentar recriá-los, o que pode gerar algum tipo de erro; por esse motivo, recomendo a utilização do seguinte comando: `smbldap-populate -e smbldap-populate.ldiff`.

Em seguida, execute: `ldapadd -c -x -W -D cn=admin,dc=linux magazine,dc=com,dc=br -f smbldap-populate.ldiff`.

Agora podemos adicionar um usuário de teste: `smbldap-useradd teste`. Confirme a adição do usuário executando o comando: `getent passwd e` o usuário deverá ser exibido na lista de usuários.

Finalizamos a configuração do servidor Samba integrado ao LDAP. Agora é a hora de se divertir criando os usuários com a ferramenta do `smbldap-tools`. Caso o leitor prefira utilizar uma interface web amigável para este fim, leia o artigo sobre Gosa, uma poderosa ferramenta para administração do LDAP que faz total integração com o domínio do Samba. ■

Mais informações

- [1] Página oficial do Samba: <http://www.samba.org/>
- [2] Download dos arquivos deste artigo: http://www.linuxmagazine.com.br/issues/74/LM74_samba_ldap.tar.gz

Sobre o autor

Marcos Amorim é mantenedor do projeto de sistema operacional embarcado para terminais leves chamado Thinstation, certificado LPIC-2, usuário de Linux há mais de 10 anos e consultor do UOL no desenvolvimento do projeto Cloud Computing.

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4592>



LDAP livre

Administração centralizada com OpenLDAP

Entenda como funciona o LDAP e aprenda como montar seu próprio servidor, com o propósito de usufruir deste serviço.

por Marcos Amorim



Este artigo tem a intenção de fazer com que o leitor conheça a origem do LDAP e entenda como o OpenLDAP pode, através da centralização, facilitar o trabalho do administrador da rede, facilitando assim o cadastros de usuários, o controle de acesso em geral e a auditoria de informações.

O LDAP (*Lightweight Directory Access Protocol* ou Protocolo Leve de Acesso a Diretórios), é um pro-

tocolo que rege a forma de acesso aos serviços de diretórios e seus respectivos clientes; em outras palavras, ele fornece a comunicação entre os usuários de uma rede, e os serviços de diretórios nela presentes.

Como sua implementação prática, temos o OpenLDAP [1], que é o LDAP melhorado e acrescido de vários recursos (**quadro 1**). Ele oferece a integração com os protocolos de comunicação IPV4 e IPV6, além

da integração do banco de dados de usuários, chaves criptográficas, e outras ferramentas, fazendo com que o LDAP possa ser implementado de forma segura e funcional. O OpenLDAP possui também a capacidade de armazenamento de dados dos usuários da rede de forma prática e segura, o que é importante. Logins, senhas, repositórios de dados do DHCP, informações de rede, sistemas operacionais e muito mais.

Quadro 1: Um pouco da história sobre a origem do LDAP

O X.500 é um padrão de protocolos de serviços de diretórios utilizados em redes de computadores que foi elaborado para trabalhar sobre o modelo OSI e incorporado ao pacote de protocolos deste, o ISO/IEC 9594. Foi designado para dar suporte ao padrão X.400, que define a troca de mensagens eletrônicas entre os usuários da rede local, onde a função do X.500 é prover serviços de diretórios para rede, centralizando a base de dados dos usuários da rede em um servidor X.500.

O protocolo de acesso a diretórios – DAP (*Directory Access Protocol*) faz parte das especificações do padrão X.500 e foi feito para trabalhar junto a todas as camadas do modelo OSI, tendo por objetivo definir o acesso de usuários aos serviços de diretórios que seu padrão provia.

O LDAP foi criado como uma alternativa ao DAP, para prover acesso aos serviços de diretórios do X.500 pelos protocolos da pilha TCP/IP. O LDAP é mais fácil de ser implementado

do que o DAP além de exigir menos os recursos da rede e memória. Ele foi desenvolvido e não adaptado como o DAP para aplicações TCP/IP; sendo assim, o LDAP obteve um melhor desempenho. Por esses motivos recebeu o nome de *Lightweight Directory Access Protocol* ou Protocolo Leve de Acesso a Diretórios, que é o nome de seu antecessor acrescentado de *Lightweight* (literalmente, peso leve).

O LDAP passou a ser a melhor forma de obter o acesso a serviços de diretórios e foi padronizado em julho de 1993 pela RFC 1487 da IETF (*Internet Engineering Task Force* – Força Tarefa de Engenharia da Internet).

Com o objetivo de facilitar o uso do LDAP, a Universidade de Michigan nos Estados Unidos, desenvolveu inicialmente o OpenLDAP, que por ser um software livre traz consigo todas as vantagens que programas de código aberto possuem, como a rápida ampliação de recursos e a correção de bugs. O OpenLDAP é a implementação do LDAP acrescido de recursos adicionais.

O recurso de principal destaque da ferramenta é a capacidade de oferecer a autenticação de usuários usando sua árvore em forma de diretório como base de dados. Com ela é possível acessar as referências de todas as informações dos usuários da rede em um único lugar. Assim, todos os protocolos e serviços de diretórios vinculados a um determinado usuário podem utilizar seus dados para a autenticação na rede. Através dessa centralização, a autenticação de todos os serviços de rede vai se concentrar em uma única árvore de informações, facilitando o trabalho do administrador de redes.

O OpenLDAP poderá ajudar não só os administradores de redes, mas também os estudantes de informática e futuros administradores de redes, que ao dominar o aplicativo, terão em suas mãos mais um diferencial – extremamente requisitado – de mercado, algo muito desejável quando o assunto é administração de redes, seja ela de pequeno, médio ou grande porte.

Conceito de diretórios

Antes de continuar, é importante entender realmente o conceito de diretórios (**figura 1**), o que por si só não é difícil de ser entendido. Uma estrutura organizada em diretórios tem por finalidade facilitar a busca das informações nele armazenadas.

Ela possui o mesmo princípio de orientação de um dicionário e é organizada de forma hierárquica, na qual um diretório principal, chamado de raiz, é a base para todos os demais. Os diretórios pertencentes a ela podem conter outros, que por sua vez podem conter outros e assim sucessivamente. Este processo recebe o nome de árvore de diretórios.

Todo tipo de informação pode ser armazenada nos atributos da base de dados do OpenLDAP, como nomes, identidades (IDs) de usuário, fotos, locais de trabalho,

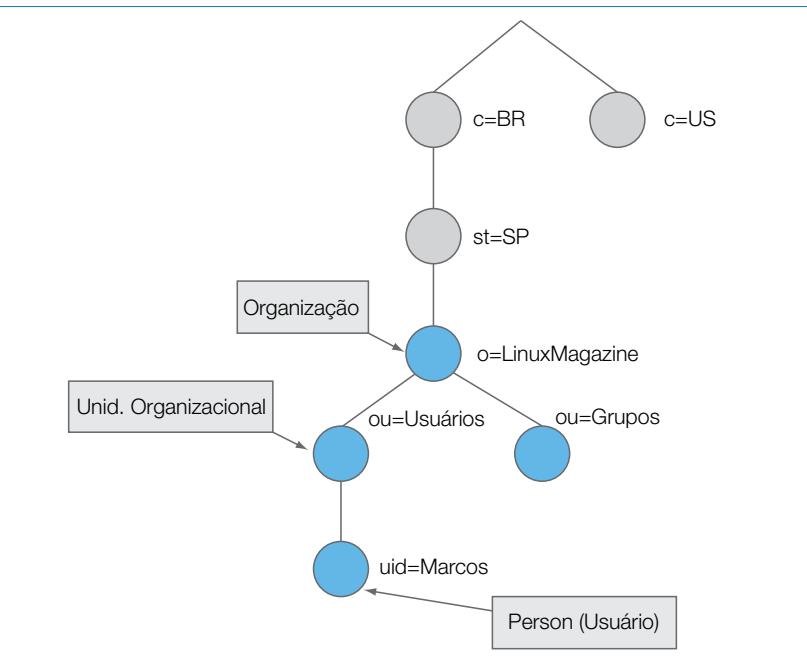


Figura 1 Árvore de diretórios LDAP.

senhas, e-mails, entre outros. Os responsáveis por determinar quais tipos de entradas de informações são válidas na base do OpenLDAP são os arquivos chamados *schema*. O schema é como uma planta-baixa, uma definição da estrutura das entradas e dos atributos que podem ser inseridos nelas.

Qualquer software que venha a necessitar da consulta de informações para seu funcionamento, é um forte candidato para a utilização do OpenLDAP. Para isso, basta que o software tenha um arquivo schema.

Criar arquivos de schema é possível, entretanto, não é necessariamente fácil; por isso o OpenLDAP traz consigo os schemas necessários para a configuração de seus principais recursos. Serviços conhecidos como o Samba [2], FTP, o servidor web Apache e uma boa parte dos sistemas baseados em softwares open source disponíveis no mercado já possuem schemas prontos e disponíveis em repositórios na Internet. Se o software que o usuário pretende usar não tiver nenhum schema existente, ele terá que criá-lo.

Com o OpenLDAP instalado e configurado, qualquer nome de usuário e senha poderá ser pesquisado na base LDAP em qualquer ponto da rede. O usuário terá acesso normal a todos os serviços que lhe forem permitidos.

Isso também acontece com a busca de qualquer tipo de informação, sendo necessário apenas que o usuário que estiver pesquisando tenha permissão para isso, por exemplo, o catálogo de endereços, listas de telefones ou informações de funcionários para uma rede local ou intranet.

Aplicações para o OpenLDAP

O OpenLDAP pode ser utilizado em todo tipo de rede, desde as pequenas até as grandes redes corporativas, pois consegue atender múltiplas chamadas ao mesmo tempo. Em outras palavras, ele conseguirá atender a vários usuários e requisições de software sem perda de desempenho. O OpenLDAP irá apenas até onde o hardware permitir, no que tange ao tráfego da rede e ao processamento

Listagem 1: Instalação do OpenLDAP

```

01 # Clientes não autenticados podem ler a base ldap
02 allow bind_v2
03
04
05 # Schemas utilizados pela nossa base ldap
06 include      /etc/ldap/schema/core.schema
07 include      /etc/ldap/schema/cosine.schema
08 include      /etc/ldap/schema/nis.schema
09 include      /etc/ldap/schema/inetorgperson.schema
10
11 pidfile     /var/run/slapd/slapd.pid
12 argsfile    /var/run/slapd/slapd.args
13
14 loglevel    none
15
16 modulepath/usr/lib/ldap
17 moduleloadback_hdb
18
19 sizelimit 500
20 tool-threads 1
21
22 backendhdb
23
24 # Definição da nossa base
25 database     hdb
26 suffix       "dc=linuxmagazine,dc=com,dc=br"
27 directory   "/var/lib/ldap"
28
29 # Usuário administrador da Base
30 rootdn"cn=admin,dc=linuxmagazine,dc=com,dc=br"
31
32 # Senha do administrador (aqui esta "linux")
33 rootpw{SSHA}qWPKzooDkgPW2rtjds9BxgP7bTiZen82
34
35 dbconfig set_cachesize 0 2097152 0
36 dbconfig set_lk_max_objects 1500
37 dbconfig set_lk_max_locks 1500
38 dbconfig set_lk_max_lockers 1500
39
40 # Indexação da base
41 index        objectClass eq
42
43 lastmod     on
44 checkpoint  512 30
45
46 # Controle de acesso aos dados armazenadas
47 access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=linuxmagazine,dc=com,dc=br" write
        by anonymous auth
        by self write
        by * none
48
49 access to dn.base="" by * read
50
51 access to *
        by dn="cn=admin,dc=linuxmagazine,dc=com,dc=br" write
        by * read

```

do servidor. Um serviço LDAP é muito mais rápido e eficiente para operações de leitura do que de escrita, ou seja, é mais rápido que um banco de dados transacional quando utilizado para operações de consulta.

Pensando nisso, vamos abordar neste artigo informações que ajudarão a desmistificar o OpenLDAP e a sua aplicação na prática, além de mostrar as diversas possibilidades de sua aplicação. Vamos montar um servidor OpenLDAP em um servidor Debian GNU/Linux e adicionar o serviço do Samba. Ao final vamos apresentar uma interface de administração do LDAP chamada Gosa [\[3\]](#).

Instalação

Para iniciar a instalação do OpenLDAP, vamos definir as informações mais importantes para a nova base LDAP. A base raiz será chamada `dc=linuxmagazine,dc=com,dc=br`. Logo abaixo dessa estrutura, teremos as `OU` (*Unidade Organizacional*) para os grupos e usuários. Na `OU` de usuários vamos adicionar um exemplo para o catálogo de endereços.

O sistema operacional para a instalação dessa base OpenLDAP será o Debian GNU/Linux 5.0, mas as configurações serão iguais em qualquer servidor que suporte a execução do OpenLDAP.

Para instalar os pacotes necessários à instalação, digite: `# apt-get install slapd ldap-utils`. Serão solicitadas algumas informações, conforme a **figura 2**. Configurar o arquivo `/etc/ldap/slapd.conf` conforme a **Listagem 1** (um exemplo do arquivo também pode ser baixado em [\[4\]](#)).

Para gerar a senha utilizada no parâmetro `rootpw` execute o comando `slappasswd -h {SSHA}`, copie o resultado e cole no local correto na linha 33 da **Listagem 1**.

Reinic peace o `slapd`, através do comando: `/etc/init.d/slapd restart`.

Neste momento é necessário iniciar o processo de população da base LDAP, e para isso, adicione as Unidade Organizacionais de usuários, grupos e também uma entrada de exemplo que pode ser utilizada no catálogo de endereços. Crie o arquivo `ou-grupos.ldif` com o comando abaixo:

```
dn: ou=Grupos,dc=linuxmagazine,dc=com,dc=br
objectClass: top
objectClass: organizationalunit
objectClass: dcObject
dc: LinuxMagazine
ou: Grupos
```

Adicione o `ldif` na base com o comando: `ldapadd -x -W -D cn=admin,dc=linuxmagazine,dc=com,dc=br -f ou-grupos.ldif`. Crie o arquivo `ou-usuario.ldif` com o conteúdo abaixo:

```
dn: ou=Usuarios,dc=linuxmagazine,dc=com,dc=br
objectClass: top
objectClass: organizationalunit
objectClass: dcObject
dc: LinuxMagazine
ou: Usuarios
```

Adicione o `ldif` na base com o comando: `ldapadd -x -W -D cn=admin,dc=linuxmagazine,dc=com,dc=br -f ou-usuario.ldif`.

Agora que a base já tem duas OU vamos adicionar uma entrada de exemplo, criando o arquivo `usuario.ldif` com o conteúdo abaixo:

```
dn: uid=marcos,ou=Usuarios,dc=linuxmagazine,dc=com,dc=br
sn: Teste
givenName: Marcos Amorim
uid: marcos
homePostalAddress: Rua GNU, 1000
homePhone: (11) 8232-1234
labeledURI: http://www.thinstation-br.org
ou: Virtualizacao
o: UOL Host
l: Centro SP
```



Figura 2 Senha do administrador da base.

```
st: SP
roomNumber: 1
telephoneNumber: (11) 1234-5678
cn: Marcos Amorim Teste
postalAddress: Rua Barao de Limeira, 100
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

Em seguida adicione o usuário na base: `ldapadd -x -W -D cn=admin,dc=linuxmagazine,dc=com,dc=br -f usuario.ldif`.

Finalizando a configuração do servidor LDAP, veja também entre as matérias desta edição como configurar o servidor Samba para autenticar-se no LDAP e também como configurar uma interface web para LDAP (GOsa). Isso vai evitar a criação de muitos arquivos LDIF, o que tornaria a administração do sistema muito trabalhosa. Nossa intenção é facilitar a vida do administrador de redes.

Gostaria de agradecer ao Professor Jaime Ribeiro Junior [5] pela fantástica referência. ■

Mais informações

- [1] Página oficial do OpenLDAP: <http://www.openldap.org/>
- [2] Página Oficial do Samba: <http://www.samba.org/>
- [3] Página Oficial do projeto GOsa: <http://www.gosa-project.org/>
- [4] Download dos arquivos deste artigo: http://www.linuxmagazine.com.br/issues/74/LM74_openldap.tar.gz
- [5] Artigo do Professor Jaime Ribeiro Junior <http://www.vivaolinux.com.br/artigo/OpenLDAP-a-chave-e-a-centralizacao/>

Sobre o autor

Marcos Amorim é mantenedor do projeto de sistema operacional embarcado para terminais leves chamado Thinstation, certificado LPIC-2, usuário de Linux há mais de 10 anos e consultor do UOL no desenvolvimento do projeto Cloud Computing.

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4587>



Mais que uma interface bonita

Poderosa ferramenta para gerenciamento de contas e sistemas de bancos de dados LDAP.

por Marcos Amorim

Dimitri Castrique - sxc.hu

GOsa [1], é uma poderosa ferramenta para gerenciamento centralizado de usuários em redes. Através dela, administradores de sistema podem gerenciar facilmente usuários, grupos, estações e *Thin Clients*, aplicativos, telefones e aparelhos de fax, listas de distribuição de correio eletrônico e muitos outros serviços.

Concebido inicialmente por Caius Pollmeier, o projeto foi premiado em 2009 com o prestigiado “Trophées du Libre” na categoria de software profissional, em Soisson, na França. Escrito em PHP e licenciado sob a GPL, o GOsa é parte integrante do projeto LiMux, da prefeitura da cidade de Munique, na Alemanha, maior iniciativa de migração para Linux da Europa, e que

utiliza a ferramenta para gerenciar sua rede de 14.000 computadores.

Em conjunto com a FAI (*Fully Automatic Installation* [2]), o GOsa permite a instalação altamente automatizada de sistemas pré-configurados e fornece portanto, um ponto único de gestão para ambientes grandes e pequenos baseado em LDAP, tornando mais simples, fácil e gerenciável a administração de usuários, sistemas e todos os parâmetros relacionados.

Pensando nisso, iremos ao longo deste artigo, instalar, configurar e testar o GOsa de modo a permitir a autenticação no servidor Samba [3] com OpenLDAP [4] e cujas respectivas instalações e configurações podem ser encontradas entre os artigos de capa desta edição. A partir daí, fica a critério da sua imaginação utilizar e configurar outros serviços que podem utilizar o LDAP em conjunto com o GOsa. Alguns exemplos são os servidores FTP, Proxy, e-mail, entre outros.

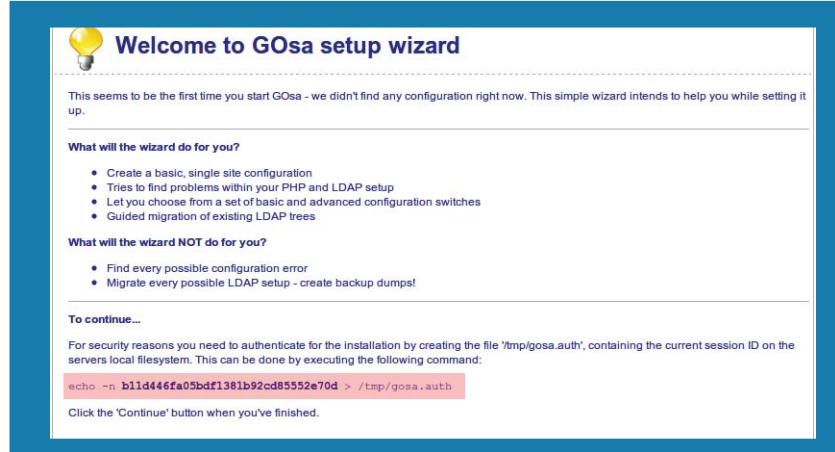


Figura 1 Tela de boas vindas do assistente do GOsa.

Instalação do GOsa

Vamos iniciar a instalação do GOsa, partindo do princípio de que este é dividido em dois pacotes principais: `gosa` que é o pacote principal, com todos os plugins e a interface web para administração e o `gosa-schema` que contém os *schemas* utilizados por ele para gerenciar os usuários.

No console, instale os dois pacotes com o comando `apt-get install gosa gosa-schema`.

Agora que o GOsa e os schemas estão instalados vamos configurar o servidor LDAP. Edite o arquivo `/etc/ldap/slappd.conf` (cuja cópia você pode baixar no site da **Linux Magazine** [5]) e adicione os schemas mostrados na **Listagem 1**, logo após os schemas do Samba.

Em seguida reinicie o serviço do `slapd`, através do comando `/etc/init.d/slappd restart`.

Finalizada a primeira parte da instalação do GOsa, vamos configurá-lo já em sua interface web. Para isso, acesse o endereço `http://IP_SERVIDOR/gosa`.

Na **figura 1** podemos ver o assistente de configuração do GOsa, que solicita que seja criado um arquivo com o ID da sessão no diretório `/tmp` do servidor.

Crie o arquivo conforme solicitado e em seguida pressione o botão *Continue*.

A próxima tela é a de seleção do idioma. Se você deixar o idioma configurado no modo automático o aplicativo irá selecionar o idioma correto de acordo com o navegador utilizado no momento do acesso. Infelizmente não temos a interface em Português nessa versão do GOsa, mas como já colaborei com o projeto, enviando os arquivos com as principais telas já traduzidas, esperamos que essa melhoria esteja disponível em breve.

Seguindo com o assistente, a próxima tela, ilustrada na **figura 2**, mostra a verificação de alguns módulos

Listagem 1: Inclusão de schemas

```
01 include      /etc/ldap/schema/gofon.schema
02 include      /etc/ldap/schema/gosystem.schema
03 include      /etc/ldap/schema/goto.schema
04 include      /etc/ldap/schema/gosa+samba3.schema
05 include      /etc/ldap/schema/gifax.schema
06 include      /etc/ldap/schema/goserver.schema
07 include      /etc/ldap/schema/goto-mime.schema
```

do PHP que podem estar faltando. Os módulos que são exibidos com a mensagem *Warning* não são obrigatórios para o correto funcionamento do GOsa, portanto trata-se apenas de um aviso.

O próximo passo será aceitar os termos de uso da licença GPL. Clique em *Accept* e em seguida em *Continue*. O seguinte passo, ilustrado na **figura 3**, mostra as configurações da base `ldap` e que devem ser pre-

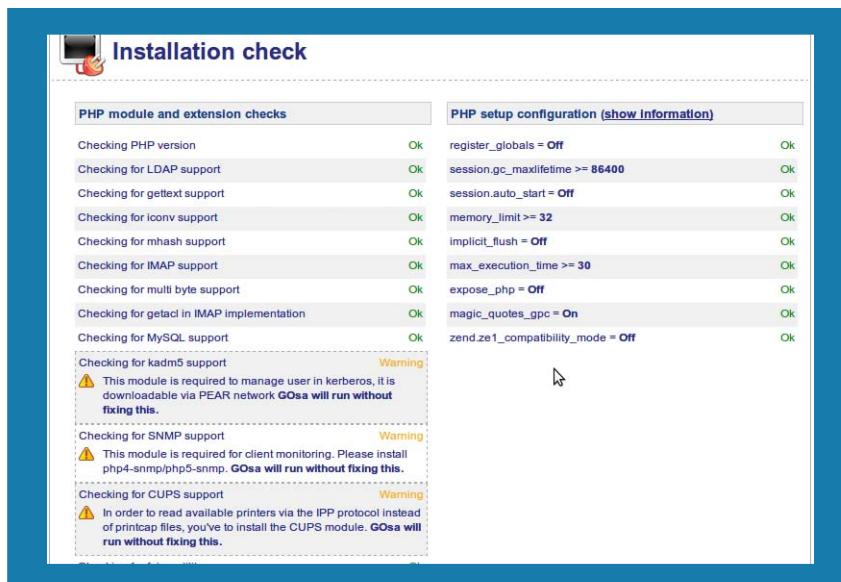


Figura 2 Verificação de módulos do PHP.

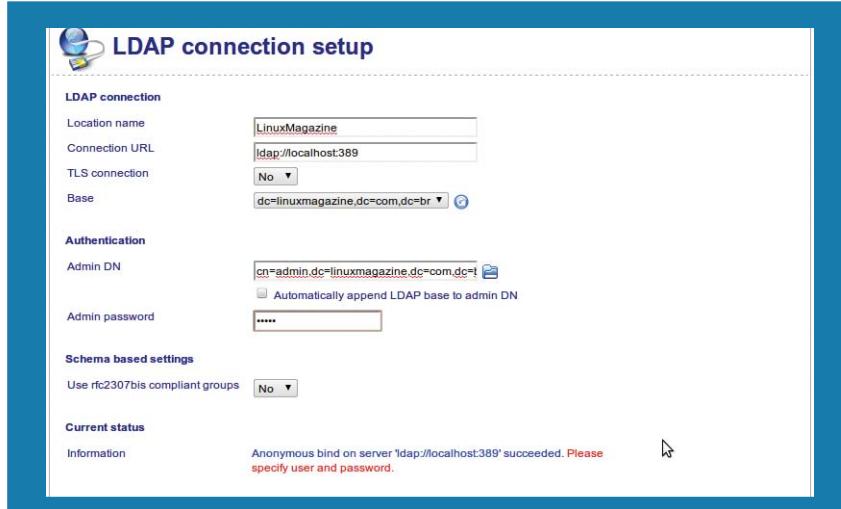


Figura 3 Configurações de conexão com o OpenLDAP.

enchidas corretamente para que a integração funcione perfeitamente.

Pressione *Continue*, e na próxima tela você verá que o GOsa executou

uma verificação no OpenLDAP para saber se todos os schemas estão ativos no servidor; caso ocorra algum erro, verifique o seu arquivo `slapd.conf`.

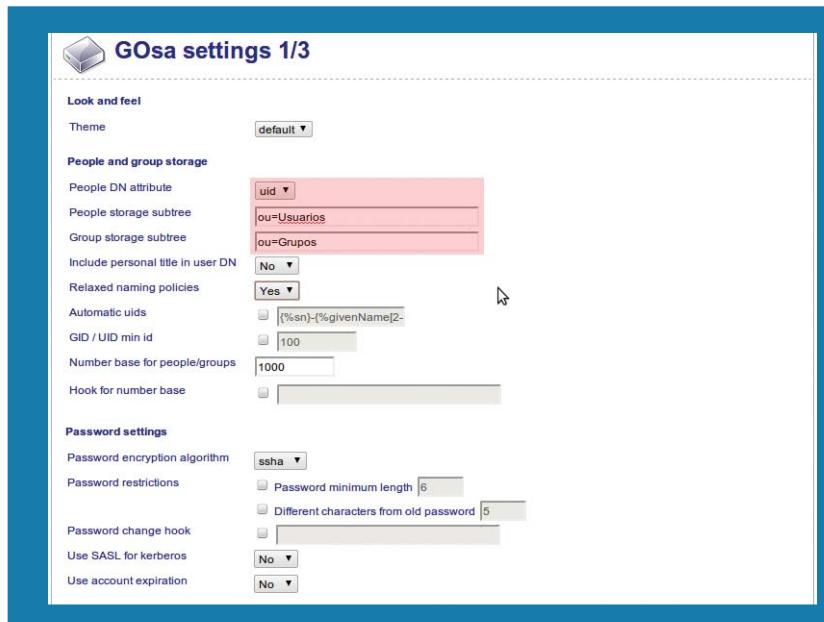


Figura 4 Contas de usuários e grupos.

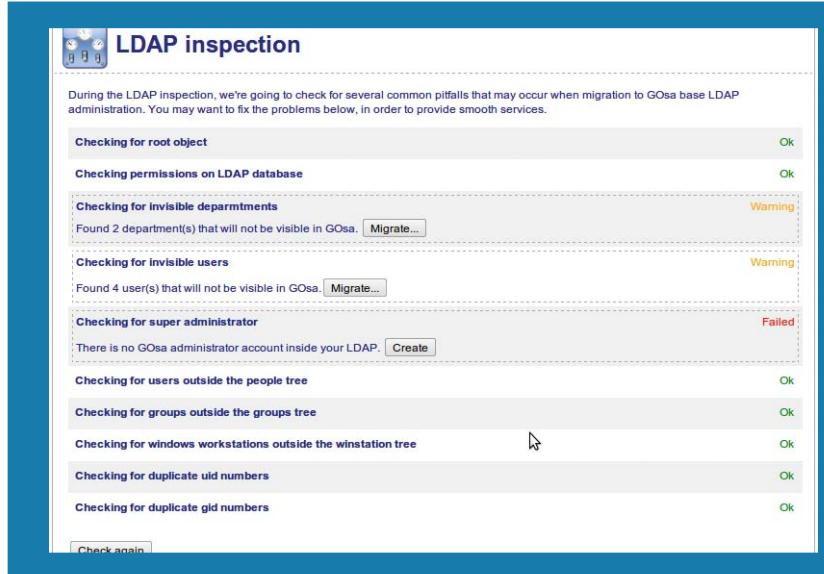


Figura 5 Verificação dos usuários para importação.

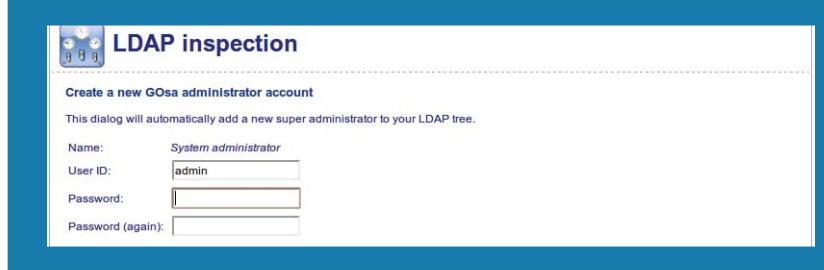


Figura 6 Criação do primeiro usuário administrador do sistema.

Pressione *Continue* para prosseguir na configuração.

Agora é o momento de informar ao GOsa onde serão armazenadas as contas de usuários e grupos, além da forma como serão armazenados conforme você pode conferir na **figura 4**. Configure de acordo com a sua necessidade e clique em *Continue* para prosseguir.

Confira os valores da próxima tela e pressione *Continue*. As duas telas seguintes, não exigem qualquer tipo de alteração, então apenas pressione *Continue*.

O instalador do GOsa pode fazer a importação dos usuários existentes na base LDAP adicionando algumas informações fornecidas por seus schemas, caso contrário, não serão exibidos na interface do GOsa.

Podemos observar na **figura 5** que foram encontrados quatro usuários e dois departamentos. Também é informado que a conta do administrador não existe, e por esse motivo, o aplicativo irá fazer a importação apenas dos usuários existente e criar a conta do administrador. Não precisamos importar os departamentos.

Usuários

Para realizar a importação de usuários, clique em *migrate* e em seguida selecione quais os usuários a serem importados, em seguida clicando em *Apply*.

O GOsa adiciona algumas classes de objetos para usuários que podem administrar a base LDAP; porém como na base atual ainda não existe um usuário com esses atributos, é necessário criar o usuário administrativo, clicando em *Create* e em seguida informando o nome e sua respectiva senha, confirmado de acordo com a **figura 6**.

Após a criação do usuário administrador, e da importação dos usuários existentes, clique em *Continue* e você poderá, na próxima tela, enviar

Finish - write the configuration file

Create your configuration file

After downloading and placing the file under /etc/gosa, please make sure that the user the webserver is running with is able to read gosa.conf, while other users shouldn't. You may want to execute these commands to achieve this requirement:

```
chown root.www-data /etc/gosa/gosa.conf
chmod 640 /etc/gosa/gosa.conf
```

[Download configuration](#)

Status: The configuration is currently not readable or it does not exists.

Figura 7 Arquivo de configuração do GOsa.

uma notificação para a equipe do GOsa sobre a sua instalação, mas essa notificação fica a seu critério. Pressione *Continue* para finalizar a instalação.

Neste ponto, chegamos ao final da configuração, embora ainda seja necessário baixar o arquivo de configuração gerado pelo assistente, e enviá-lo para o servidor. Esse arquivo deve ser baixado em sua máquina local e posteriormente copiado para o servidor no diretório `/etc/gosa`. Siga agora as informações contidas na [figura 7](#) para configurar as permissões do arquivo `gosa.conf` (baixe o arquivo de exemplo no link [\[5\]](#)).

Após configurar as permissões do arquivo, pressione *Continue* e você será redirecionado para a tela de login; logue-se com algum dos usuários criados.

Conclusão

Devido ao seu poderoso conjunto de recursos e à sua robustez enquanto plataforma de gerenciamento, o GOsa figura atualmente como uma das melhores soluções de código aberto para integração com o OpenLDAP – na opinião do autor deste artigo. Sua adoção por administradores de redes e sistemas em projetos profissionais é, assim, fortemente recomendada. ■

Mais informações

- [1] Página oficial do projeto GOsa: <http://www.gosa-project.org/>
- [2] Página oficial do projeto FAI: <http://fai-project.org/>
- [3] Página oficial do Samba: <http://www.samba.org/>
- [4] Página oficial do Openldap: <http://www.openldap.org/>
- [5] Download dos arquivos deste artigo:
http://www.linuxmagazine.com.br/issues/74/LM74_arquivos_gosa.tar.gz

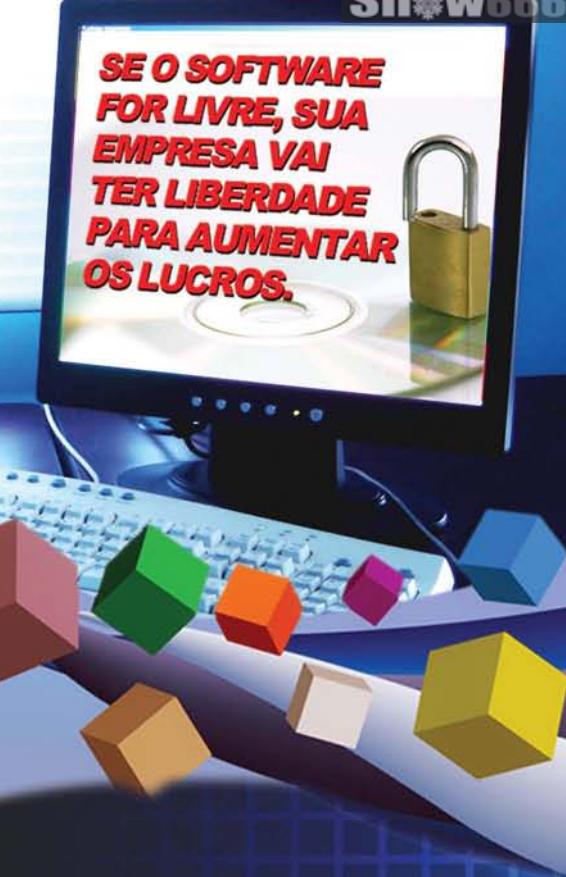
Sobre o autor

Marcos Amorim é mantenedor do projeto de sistema operacional embarcado para terminais leves chamado Thinstation, certificado LPIC-2, usuário de Linux há mais de 10 anos e consultor do UOL no desenvolvimento do projeto Cloud Computing.

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4586>



A F13 Tecnologia, é uma empresa dinâmica e criativa em soluções de tecnologia da informação.

Nosso objetivo é fazer serviços com foco no atendimento personalizado com qualidade, eficiência e segurança.

Sempre embasados nas melhores práticas dos principais frameworks de gestão de TI.

O trabalho da F13 é baseado em Software Livre, o que representa para o nosso cliente: redução de custos, ambientes computacionais mais seguros e amplas possibilidades de customização e adequação de softwares para a sua realidade.

Tudo isto administrado por profissionais com certificados LPI.

Escolha um parceiro de confiança.

Ligue agora mesmo

(85) 3252.3836

ou acesse www.f13.com.br



Samba + OpenLDAP + GOsa

CAPA

Administração versátil

Você já aprendeu como instalar e configurar os aplicativos Samba, OpenLDAP e a interface web GOsa. Agora aprenda a integrar todos eles de uma só vez, com a finalidade de obter um sistema completo e versátil.

por Marcos Amorim

Margarit Ralev - sxc.hu

Costumo seguir a lógica de instalação e configuração do OpenLDAP, autenticação com PAM, Samba, configuração do `smbldap-tools` e finalmente a configuração do GOsa. Sendo assim, neste artigo final de integração das tecnologias abordadas nos artigos anteriores, vamos tornar nosso ambiente completo e unificado.

Instalação dos pacotes

Todas as informações solicitadas serão configuradas manualmente após o processo de instalação; por isso, preencha quaisquer questionamentos sobre configurações com as opções padrão.

```
apt-get install slapd ldap-utils →
samba smbldap-tools samba-doc
libnss-ldap libpam-ldap smbclient →
gosa gosa-schema
```

É necessário copiar o *schema* do Samba para a pasta de schema do OpenLDAP:

```
cp /usr/share/doc/samba-doc/ →
examples/LDAP/samba.schema.gz →
etc/ldap/schema/
cd /etc/ldap/schema/ →
gunzip samba.schema.gz
```

OpenLDAP

Após a instalação de todos os pacotes necessários, vamos começar a configuração, iniciando pelo OpenLDAP. Apague o arquivo de configuração `/etc/ldap/slapd.conf` e crie o seu próprio conforme mostra a [listagem 1 \[1\]](#).

Após a configuração do `slapd.conf`, é possível reiniciar os serviços, através do comando: `/etc/init.d/slapd restart`.

Nsswitch

O NSSwitch é necessário para o reconhecimento das informações dos usuários e grupos que estão cadastrados no LDAP e por isso é necessário configurar o arquivo `/etc/`

`libnss-ldap.conf` para que possua as opções a seguir:

```
base dc=linuxmagazine,dc=com,dc=br
uri ldap://localhost/
ldap_version 3
rootbinddn cn=admin,dc= →
linuxmagazine,dc=com,dc=br
```

Configure a senha do administrador editando o arquivo `/etc/libnss-ldap.secret`. Para melhor organização, mantenha apenas uma linha neste arquivo, contendo apenas a senha, e certifique-se de que as permissões desse arquivo estejam habilitadas para leitura pelo *root* (`chmod 600`). A senha de administrador utilizada é a senha `linux`.

Ative a configuração editando o arquivo `/etc/nsswitch.conf` de acordo essas informações:

passwd:	compat ldap
group:	compat ldap
shadow:	compat ldap

PAM

O PAM é responsável pelo reconhecimento dos usuários e senhas no Linux. Sua configuração é necessária para que o PAM reconheça os usuários que estão também presentes no OpenLDAP. Portanto, edite o arquivo `/etc/pam_ldap.conf` e modifique as seguintes informações:

```
base dc=linuxmagazine,dc=com,dc=br
uri ldap://localhost/
ldap_version 3
rootbinddn cn=cn=manager,dc=linuxmagazine,dc=com,dc=br
pam_password crypt
```

Assim como o `libnss-ldap`, o PAM precisa da senha para conseguir ler o atributo de senha dos usuários, e por isso, é necessário configurar a senha no arquivo `/etc/pam_ldap.secret`. Novamente, confira as permissões do arquivo, que devem estar configuradas para `600`.

Comece ativando o reconhecimento dos usuários que estão na base LDAP editando o arquivo `/etc/pam.d/common-auth`, com as seguintes informações:

```
auth sufficient pam_ldap.so
auth required pam_unix.so nullok_
secure use_first_pass
```

No arquivo `/etc/pam.d/common-password`, configure a opção `password sufficient pam_ldap.so`. E por fim, no arquivo `/etc/pam.d/common-account`, configure os valores `account sufficient pam_ldap.so`.

Estes passos finalizam a configuração do PAM. Com isso, podemos prosseguir com a configuração do servidor.

Samba

Edito o arquivo `/etc/samba/smb.conf` e configure-o, de acordo com a [listagem 2](#) [1].

O Samba precisa saber qual é a senha do administrador, para que algu-

mas informações adicionais possam ser criadas. Para isso, temos de executar o comando: `smbpasswd -w linux`. A palavra `linux` é a senha do administrador da nossa base; você deve substituir pela senha de sua preferência.

Reinic peace os serviços do samba através do comando `/etc/init.d/samba restart`.

SMBLdap Tools

É chegada a hora de configurar o `smbldap-tools`, que será o responsável por popular a base LDAP com as informações necessárias para o funcionamento do Samba. Existem outras maneiras, mas nosso objetivo neste artigo é a facilitar a instalação e a administração. Assim, configure o arquivo `/etc/smbldap-tools/smbldap.conf` de acordo com as informações a seguir:

- 1 Antes de iniciar a configuração, precisamos obter o SID do servidor Samba. Execute o conteúdo da [listagem 3](#) [1] e ignore possíveis mensagens de erro. O SID será algo como: `SID for domain PDC-SRV is`.
- 2 Comece a popular a base LDAP, utilizando como base inicial o arquivo da [listagem 4](#) [1], que foi gerado com o `smbldap-populate -e smbldap-populate.ldif`.

- 3 Após a criação desse arquivo, vamos popular de fato a base de dados com o comando: `ldapadd -c -x -W -D cn=admin,dc=linuxmagazine,dc=com,dc=br -f smbldap-populate.ldif`.

Será solicitada a senha do administrador e assim a base estará completa e finalizada.

GOsa

O processo de configuração do GOsa, descrito no artigo “Mais que uma interface bonita”, não sofre nenhuma alteração. Apenas crie o arquivo `/etc/gosa/gosa.conf`, para que todas as configurações sejam compreendidas pela ferramenta.

Conclusão

Finalizamos assim, uma série de artigos que se complementam e que são de extrema utilidade para os administradores de rede. Espero que o leitor aprecie. Fique à vontade para enviar suas críticas, dúvidas ou sugestões.

Para facilitar a configuração e integração do seu ambiente, as listagens citadas neste artigo, estão disponíveis para download no site da [Linux Magazine](#), em [1]. ■

Mais informações

[1] Download das listagens deste artigo:

http://www.linuxmagazine.com.br/issues/74/LM74_listagens.tar.gz

Sobre o autor

Marcos Amorim é mantenedor do projeto de sistema operacional embarcado para terminais leves chamado Thinstation, certificado LPIC-2, usuário de Linux há mais de 10 anos e consultor do UOL no desenvolvimento do projeto Cloud Computing.

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4593>



Asterisk descomplicado



VoIP com Asterisk – parte III

O sistema telefônico ultrapassado, presente até pouco tempo, em cobranças: cada novo recurso ativado requer uma nova ativação de serviço, adicionado ao pagamento mensal. É hora de mudar. É hora de criar sua própria central VoIP.

por Stefan Wintermeyer

Na edição 73 da *Linux Magazine*, apresentamos a economia com padrões, o conceitos de contextos, caller-IDs e telefonemas via provedor. Nesta terceira parte do tutorial, vamos abordar secretárias eletrônicas e sistema interativo de resposta de voz (*Interactive Voice Response System*, ou IVR) no Brasil conhecido como URA (Unidade de Resposta Audível). Mão à obra!

Secretária eletrônica

O Asterisk traz um sistema de mensagens de voz muito poderoso e fácil de usar. A configuração é feita no arquivo `voicemail.conf`. Apague o arquivo de exemplo com um `rm /etc/asterisk/voicemail.conf` e crie um novo igual ao apresentado na **listagem 1**.

Listagem 1: Arquivo `voicemail.conf`

```
01 [general]
02 format=wav
03
04 [default]
05 ;Voicemailbox => senha, nome, e-mail
06 2000 => 1234, Hans Meier, hans.meier@exemplo.br
07 2001 => 1234, Uwe Klein, uwe.klein@exemplo.br
```

Para ativar a secretária eletrônica para todas as chamadas recebidas, expanda seu plano de discagem como na **listagem 2**. Se for usado um comando `Dial()`, o dispositivo chamado tocará para sempre. Porém, se você utilizar um segundo parâmetro para o comando `Dial()`, o Asterisk insistirá somente durante esse número de segundos – no caso, 30 (**linha 8** da **listagem 2**).

Fique à vontade para medir os segundos, mas não com um relógio atômico; o Asterisk usará alguma medida particular que resultará em cerca de 30 segundos. Se o telefone em questão não atender, o plano de discagem passará para a próxima prioridade (2, neste caso). Isto está na **linha 9**, ou na **linha 16** da **lista-**

gem 2 no caso de telefonemas que venham de fora. A extensão inicia a aplicação com a segunda prioridade, `VoiceMail()`, que age como uma secretária eletrônica. Ela precisa ser configurada no arquivo `voicemail.conf`.

Consulta aos recados

Uma secretária eletrônica também precisa ser consultada por seu proprietário. Para isso, criamos a extensão 3000 em nosso plano de discagem. Se você telefonar para o número 3000 a partir de um telefone interno (ou seja, de qualquer número no contexto `[meus-telefones]`), o sistema irá solicitar a sua senha – no nosso exemplo, esta é 1234. Digite-a e aguarde alguns instantes. Em seguida, o sistema de mensagens de voz vai informar que você pode ouvir as mensagens. Como está configurado em nosso `voicemail.conf`, o Asterisk ainda enviará uma cópia de cada recado, no formato WAV, para o e-mail especificado.

Na **listagem 2**, a extensão 3000 utiliza o parâmetro `$(CALLERID(num))` na **linha 11**. Esta é uma função do Asterisk para retornar o número de

quem originou a chamada. Não confunda com a variável `$_[EXTEN]` das outras linhas, que contém o número de destino.

URA

Vamos conhecer agora, o sistema interativo de resposta de voz (*Unidade de Resposta Audível*, ou URA). A URA oferece uma maneira automatizada de encaminhar chamadas e oferecer menus de voz com mais competência do que uma secretária eletrônica. Para criar uma URA, é preciso, primeiramente, usar arquivos de voz. No tocante ao Asterisk, isso significa usar a aplicação `Record()`. Ao contrário de `Playback()`, `Record()` requer que o final do arquivo passado esteja de acordo com o `codec` usado. Com o plano de discagem da **listagem 3**, é possível chamar qualquer extensão de **9900** a **9999** e pedir que o usuário grave sua mensagem de saudação (também chamada de *prompt* de voz). Eles terminam a mensagem pressionando a tecla **#** ou então aguardando. No entanto, uma longa pausa no final de um prompt de voz pode prejudicar o uso de uma série de componentes de voz de uma só vez.

Para implementar uma URA em conjunto com prompts de voz, utilize a aplicação `Background(arquivo)`. Ela reproduz o menu de voz do arquivo e escuta tons DTMF para prosseguir no plano de discagem. O processamento dos tons do teclado ocorre normalmente, como seria feito em uma ligação comum. Se, durante o uso da aplicação `Background()`, você pressionar as teclas **[8][8]**, o Asterisk buscará no contexto atual o que fazer com a extensão **88**, iniciando a partir da prioridade **1** desta extensão.

Um exercício simples: crie os seguintes prompts de voz e armazene-os no diretório `/var/lib/asterisk/sounds/`:

- ▶ **Entrada:** “Por favor disque um número no seu telefone.”

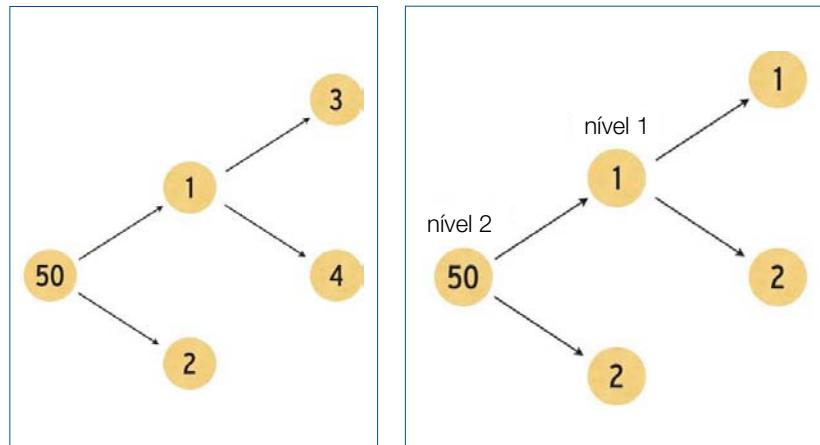


Figura 1 O conceito de URA do Asterisk funciona somente dentro de um contexto.

Figura 2 Graças ao `Goto`, um único dígito em um menu permite encaminhar o usuário a outro contexto.

Listagem 2: Arquivo extensions.conf

```

01 [outros]
02
03 [meus-telefones]
04 exten => 1234,1,Answer()
05 exten => 1234,2,Playback(hello-world)
06 exten => 1234,3,Hangup()
07
08 exten => _200[1-2],1,Dial(SIP/${EXTEN},30)
09 exten => _200[1-2],2,VoiceMail(${EXTEN},u)
10
11 exten => 3000,1,VoiceMailMain(${CALLERID(num)})
12 exten => _0X.,1,Dial(SIP/${EXTEN}:1)@axxes0_out)
13
14 [do-provedor-sip]
15 exten => _X.,1,Dial(SIP/2000,30)
16 exten => _X.,2,VoiceMail(2000,u)

```

Listagem 3: Plano de discagem para URA

```

01 exten => _99XX,1,Answer()
02 exten => _99XX,2,Wait(1)
03 exten => _99XX,3,Record(/tmp/promptvoz${EXTEN:2}.wav)
04 exten => _99XX,4,Wait(1)
05 exten => _99XX,5,Playback(/tmp/promptvoz${EXTEN:2})
06 exten => _99XX,6,Hangup()

```

Listagem 4: Plano de discagem

```

01 exten => 30,1,Answer()
02 exten => 30,n,Background(entrada)
03 exten => 30,n,Hangup()
04
05 exten => _[13579],1,Playback(impar)
06 exten => _[13579],n,Hangup()
07
08 exten => _[2468],1,Playback(par)
09 exten => _[2468],n,Hangup()

```

- ▶ **par.wav**: “Este número é par.”
- ▶ **ímpar.wav**: “Este número é ímpar.”

Com o plano de discagem da **listagem 4**, é possível experimentar a função URA. Mas atenção: a entra-

da precisa ser fornecida enquanto a mensagem da aplicação `Background()` é emitida. Se você quiser oferecer a possibilidade de o usuário esperar mais um pouco, use os prompts pré-fabricados `silence/1` até `silence/9`:

```
exten => 30,1,Answer()
exten => 30,n,Background(entrada)
exten => 30,n,Background(silence/5)
exten => 30,n,Hangup()
```

Onde os números representam o número de segundos que o Asterisk aguardará em silêncio.

Listagem 5: Mais opções

```
01 [ivr]
02 exten => 50,1,Answer()
03 exten => 50,n,Background(menuexemplo)
04 exten => 50,n,Background(silence/5)
05 exten => 50,n,Hangup()
06
07 ; Como um contexto só pode representar
08 ; uma extensão, o exemplo de menu
09 ; precisará de uma opção para cada
10 ; ação (até as de dois dígitos)
11
12 exten => 1,1,Background(dummy1)
13 exten => 1,n,Background(silence/5)
14 exten => 1,n,Hangup()
15
16 exten => 2,1,Playback(dummy2)
17 exten => 2,n,Hangup()
18
19 exten => 3,1,Playback(dummy3)
20 exten => 3,n,Hangup()
21
22 exten => 4,1,Playback(dummy4)
23 exten => 4,n,Hangup()
```

Listagem 6: Truques de menus e contextos

```
01 [nível0]
02 exten => 50,1,Answer()
03 exten => 50,n,Background(menuexemplo)
04 exten => 50,n,Background(silence/5)
05 exten => 50,n,Hangup()
06
07 ; No próximo nível, liberar os números para
08 ; outras possibilidades de forma a permitir
09 ; o uso de extensões que já tenham sido
10 ; usadas em menus anteriores.
11
12 exten => 1,1,Goto(nível1,99,1)
13
14 exten => 2,1,Playback(dummy2)
15 exten => 2,n,Hangup()
16
17 [nível1]
18 exten => 99,1,Background(dummy1)
19 exten => 99,n,Background(silence/5)
20 exten => 99,n,Hangup()
21
22 exten => 1,1,Playback(dummy3)
23 exten => 1,n,Hangup()
24
25 exten => 2,1,Playback(dummy4)
26 exten => 2,n,Hangup()
```

URAs com vários níveis

O problema no conceito de URA demonstrado é que ele sempre opera dentro de um contexto e, por isso, só pode oferecer mais opções por meio de mais números (**figura 1** e **listagem 5**). Isto é, obviamente, insatisfatório, mas uma instrução de `Goto()` pode resolver esse problema. Ela permite pular a outro ponto do plano de discagem.

Com `Goto(10)`, o Asterisk pula para a prioridade **10** na extensão atual. Com `Goto(555,1)`, ele vai para a extensão **555**, prioridade **1**. Ainda mais interessante é `Goto(produção,20,5)`, que pula para o contexto **produção**, extensão **20** e prioridade **5**. Com esses truques, é possível entrar, com um único dígito de um menu nível **1**, em uma extensão de dois dígitos em outro contexto, e novamente ter à disposição outras opções de um dígito (**listagem 6** e **figura 2**).

Na próxima edição da **Linux Magazine**, vamos falar sobre ramificações no plano de discagem, cálculos e operações sobre texto. Até lá! ■

Sobre o autor

Stefan Wintermeyer é o autor do Livro do Asterisk, da editora Addison Wesley e primeiro DCAP (Digium Certified Asterisk Professional) alemão. Ele auxilia clientes, por meio da Amooma GmbH (<http://www.amooma.de>), a implementar soluções com Asterisk.

Gostou do artigo?

Queremos ouvir sua opinião.
Fale conosco em
cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4578>

QUER FALAR COM OS 30.000 PROFISSIONAIS DE TI COM MAIOR NÍVEL DE CONHECIMENTO TÉCNICO DO MERCADO NACIONAL? ENTÃO ANUNCIE NA LINUX MAGAZINE!

Segundo dados do Instituto Verificador de Circulação*, a Linux Magazine é atualmente a segunda revista mais vendida para profissionais de TI do mercado editorial brasileiro. Além disso, é a revista que tem o público mais qualificado no quesito técnico. Nossa combinação exclusiva de conteúdo avançado com uma abordagem prática faz da Linux Magazine a publicação preferida de quem toma decisões e faz recomendações para compra de produtos e contratação de serviços. Anuncie conosco e fale com esse público.

Para anunciar, entre em contato:

anuncios@linuxmagazine.com.br

11 3675-2600

*Comparação de circulação para os últimos três meses de publicações nacionais voltadas ao segmento de TI.

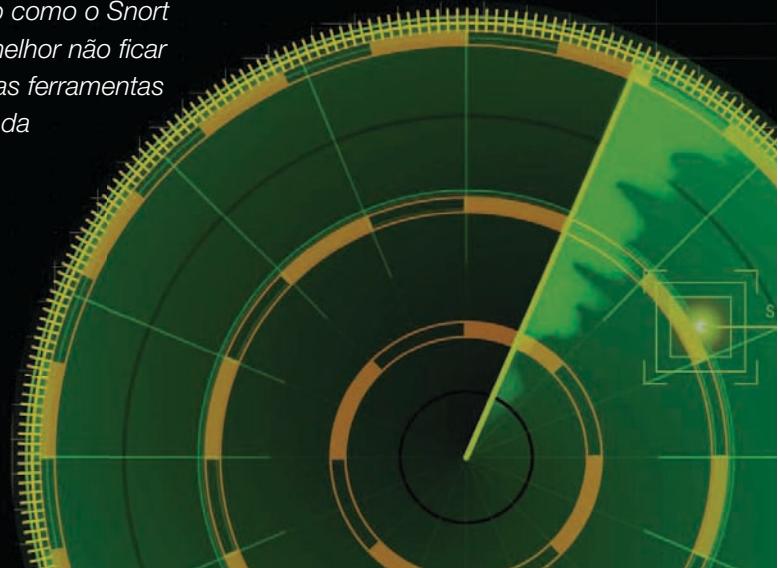


Detecção de intrusão

Sob o radar

Ferramentas de detecção de intrusão como o Snort ajudam a rastrear invasores, mas é melhor não ficar confortável demais. Conheça algumas ferramentas que os agressores utilizam para fugir da detecção de intrusão.

por Kurt Seifried



Você provavelmente já instalou e configurou sistema de detecção de intrusão para proteger sua rede contra ataques e ficou aguardando para receber um alerta assim que surgisse qualquer vestígio de comportamento suspeito. Mas você tem certeza de que está seguro? Tente novamente. Especialistas em segurança gastam muito tempo e dinheiro estudando técnicas para contornar sistemas de detecção de intrusão (IDS, na sigla em inglês) porque conhecem os agressores que estão lá fora fazendo o mesmo.

Ferramentas IDS e IPS (sistemas de prevenção de intrusão) não são livres de falhas. A detecção de intrusão baseada em *hosts* (HIDS) precisa, por definição, ser carregada no *host*, o que é ótimo se você tiver o total controle sobre este e realmente puder carregar seu software HIDS no sistema (boa sorte ao tentar fazer isso com todas as suas impressoras de rede, scanners, copiadoras, sistemas de ponto de venda etc.).

Em uma escala maior, os administradores implantam ferramentas IDS baseadas em rede, incluindo sofisticadas ferramentas IPS que de fato param ataques, por exemplo, enviando um pacote TCP *reset* para finalizar a conexão.

Mas até essas aplicações corporativas têm algumas complicações. Por exemplo, o bloqueio ao ataque pode acontecer tarde demais para ser eficaz; sistemas IPS geralmente precisam ser *in-line* (para conseguirem bloquear ataques antes que estes de fato comprometam no sistema) ou devem ser algo agressivos no bloqueio do tráfego “ruim” de dados.

Estas duas soluções podem causar outros problemas – a primeira é que introduz maior latência e pontos de falha em sua rede, e a segunda é que leva a falsos positivos de ataques e bloqueio de tráfego de rede legítimo.

Invasores experientes podem explorar esses problemas para se esgueirar para dentro da sua rede de segurança. Este artigo apresenta algumas das fer-

mentas e técnicas que os agressores usam para passar despercebidos até pelos melhores IDSs.

Fugir ou atacar

Invasores têm basicamente duas escolhas ao tentar passar despercebidos: eles podem tanto se esconder para não despertar interesse quanto mascarar suas atividades por meio de despeites (como o rapaz que contratou um monte de disfarces pela Craigslist [1] para roubar um carro-blindado).

De forma geral, esconder-se funciona melhor do que disfarçar-se, principalmente contra sistemas IPS que bloqueiam ataques – isto é, a menos que você deseje atacar diretamente o seu próprio IDS por meio de uma enchente de informações enviadas ao administrador (não há nada como ir de 100 alertas por dia para 100 alertas por minuto).

Basicamente, essas técnicas resumem-se a esgueirar-se pela cidade sob a proteção da escuridão ou provocar o estouro de uma manada e segui-la

até a cidade enquanto ela faz muito barulho e causa desordem.

Alteração de pacotes

A alteração de pacotes (*packet mangling*) é um método clássico de fugir de sistemas IDS e IPS, e com “clássico”, quero dizer que existe desde 1998. O utilitário Fragrouter [2] foi originalmente lançado para este fim e depois foi seguido pelo Fragroute [3] (note a falta do “r”). O Fragrouter original tinha um número limitado de opções – primariamente envolvia dividir os dados em fragmentos de 8, 16 ou 24 bytes com opções de duplicar pacotes e enviá-los fora de ordem (o que, em 1999, era mais do que suficiente para fugir de sistemas IDS). Claro que a maioria dos fabricantes desse tipo de sistema corrigiram seus produtos; então os autores do Fragrouter o melhoraram, chegando até o Fragroute. O Fragroute atua como um proxy em nível da rede; recebendo um influxo bem formado de pacotes TCP e o transformando em uma desordem que ainda faz alguns sistemas IDS e hosts se complicarem.

O Fragroute pode atrasar, descartar e duplicar pacotes (seja o primeiro, o último ou algum aleatório), criando lixo com diferentes *payloads* (cabeçalhos e dados de intrusão como scripts shell), opções IP inválidas e valores TTL modificados. Alternativamente, o Fragroute pode fragmentar pacotes em tamanhos arbitrários, adicionar opções IP e modificar valores TOS (tipo de serviço). Se você realmente deseja acabar com a vida de sistemas IDS frágeis, pode reordenar os pacotes de forma aleatória ou em ordem inversa (o que pode exaurir os buffers do IDS para armazenar e reorganizar os dados). Basicamente, qualquer coisa ruim que ainda resulte em dados que um host possa reorganizar e processar é possível com o Fragroute.

Invasores também usam o *Nmap* (figura 1) para fragmentar pacotes. O Nmap permite especificar uma

MTU (unidade máxima de transmissão) pequena. Por diversão, sugiro experimentar uma MTU de 1byte (um byte de dados por pacote TCP); embora isso seja lento e use muita banda, você se surpreenderá com a frequência com que essa técnica derruba (ou deixa em estado de confusão extrema) sistemas IDS/IPS ou até máquinas remotas.

Claro que há outros métodos clássicos de alterar pacotes, como o envio intencional de *checksums* incorretos e outras modificações de bits arbitrários do cabeçalho (por exemplo, usando o parâmetro *urgent* ou *flags TCP*). É possível usar ferramentas como o *hping* [4] para gerar pacotes completamente personalizados e, se você desejar integrar seu trabalho a linguagens de programação como Python, a ferramenta Scapy [5] deve ser do seu interesse.

A forma mais fácil de lidar com ataques de alteração de pacotes é ter um firewall que realize a reordenação de pacotes TCP. O *Iptables* no Linux, por exemplo, faz isso com os módulos de rastreamento de conexão (*connection tracking*), que reordenam pacotes automaticamente. O *PFsense* no FreeBSD, possui uma opção *scrub* que recebe o argumento *fragment reassemble*, que faz um buffer dos pacotes recebidos e os reorganiza em pacotes completos antes de enviá-los.

Essas duas ferramentas evidentemente introduzem mais latência, mas impedem que pacotes fragmentados

```
FIREWALL/IDS EVASION AND SPOOFING:  
-f; --mtu <val>: fragment packets (optionally w/given MTU)  
-D <decoy1,decoy2[,ME]...>; Cloak a scan with decoys  
-S <IP_Address>; Spoof source address  
-e <iface>; use specified interface  
-g; --source-port <port>; Set given port number  
--data-length <len>; Append random data to sent packets  
--ttl <val>; Set IP time-to-live field  
--spoof-mac <mac address/prefix>/<vendor name>; spoof your MAC address  
--badsum: Send packets with a bogus TCP/UDP checksum
```

Figura 1 Fragmentação de pacotes com Nmap.

com seções sobrepostas atravessem o firewall. A ideia geral é colocar um sistema operacional com uma pilha TCP robusta em frente a todos os sistemas com pilhas TCP fracas.

Juntamente com os avanços nas ferramentas de alteração de pacotes nos últimos anos, a maioria dos sistemas IDS e IPS também melhorou. O melhor exemplo disso é o projeto de código aberto *Snort* (sucessor do preprocessor Stream4). O Stream5 oferece reorganização TCP avançada e detecção de anomalias e descobre vários tipos de conexões e pacotes alterados. Fabricantes de sistemas IDS/IPS de código fechado também acompanharam o ritmo. Confira a documentação do fabricante do seu firewall e certifique-se de estar com as atualizações mais recentes.

Alteração de protocolo

O que constitui tráfego de rede “correto” e “válido” para um dado protocolo? Qualquer dado que o cliente ou servidor ao qual você está conectado aceite. O que os padrões dizem fica em um distante segundo lugar quando se trata de implementação. Isto significa que criar softwares de análise de protocolo realmente bons é quase impossível. Mesmo que você o faça seguindo as especificações, isso pode não importar porque os fabricantes (até os grandes) às vezes aceitam dados mal formados como

Quadro 1: Nomes de domínio internacionais

Talvez você pense que ainda pode simplesmente filtrar tráfego com base em nomes de domínio, criando uma lista negra dos bandidos. Infelizmente, com o IDN (*International Domain Names* [14]) pode-se terminar com múltiplas representações de um domínio usando IDN, UTF-7 e Punycode. Você provavelmente terá interesse em verificar se o seu produto trata nomes IDN e suas representações Punycode de forma adequada.

```

http://10.1.2.3/A random file.html
http://167838211/%41 random%2520file.html

http://examplex.com/A random file.html
http://xn--example-sxa.com.com/%E3%81 random file.html

http://example.org/%E0%81%81 random file.html
http://example.org/%U0041 random file.html

```

Figura 2 Alguns exemplos de codificações com porcento, duplo porcento, Unicode, UTF-8 e misturadas.

completamente válidos (uma forma educada de dizer que eles não seguem as especificações).

Um exemplo perfeito é o *sniffer* de pacotes Wireshark (antigo *Ethereal*), que possui várias centenas de disseadores de protocolos e 203 entradas no banco de dados de vulnerabilidades CVE – a maioria por falhas nos disseadores de protocolos.

Há várias ferramentas que permitem capitalizar esses recursos de protocolos fora do padrão que passam pelos sistemas IDS e IPS. Verificados dez diferentes fuzzers (testadores de softwares), cinco deles tinham capacidade de agir em rede. E desses cinco, o melhor é o *Peach Fuzzing Platform* [6], que ainda está em desenvolvimento ativo (a última atualização foi em abril de 2010). Algumas das outras ferramentas de alteração de protocolos tiveram seu desenvolvimento descontinuado. Por exemplo, o SPIKE não vê uma nova versão há vários anos.

Foco na web

Você não se surpreenderá em saber que muitas intrusões são provenientes do tráfego de Internet. Grande número de serviços e dispositivos agora são baseados na web ou ao menos interagem com ela (como sua impressora, scanner, servidores e dispositivos embarcados). Além disso, quase tudo que não é baseado na web tem um firewall, então os servidores web tendem a voar para o topo da lista de alvos dos invasores.

A Internet apresenta algumas oportunidades interessantes para o invasor: praticamente qualquer servidor web suporta uma ou mais linguagens de programação (scripts CGI, PHP, SQL etc.). Isto dá aos agressores muito mais oportunidades de interagir com o sistema de formas imprevistas que podem resultar em estouros de buffer – *SQL injection*, vulnerabilidades XSS (*Cross-Site Scripting*) e assim por diante.

O lado cliente também oferece um conjunto de tecnologias incrivelmente complexo e recheado de problemas. Todos os grandes navegadores (Internet Explorer, Firefox, Opera, Safari e Chrome) possuem um rico histórico de falhas de segurança. Além disso, considere a ubiquidade do Flash, que está instalado em praticamente todas as máquinas

Windows e na maioria das máquinas Linux. Se você quiser assistir a vídeos, é muito provável que venha a precisar do Flash – ao menos até o HTML5 se popularizar). O Flash tem um histórico de segurança terrível. No momento da confecção deste artigo, por exemplo, existe um ataque conhecido com código de abuso, e a Adobe anunciou que levará de duas a três semanas para corrigi-lo.

Embora ainda não seja muito popular, um método simples que os agressores podem usar para contornar completamente os sistemas IDS e IPS é usar sessões web HTTPS criptografadas para realizar ataques contra servidores e clientes. A menos que você possua uma *appliance* de平衡amento de carga HTTP entre o seu sistema IDS/IPS e o servidor de fato, não haverá qualquer forma fácil de visualizar o conteúdo enviado ao servidor.

No lado cliente, se você for suficientemente paranoico, pode comprar um produto como o *Packet Forensics* [7], que permite descriptografar sessões HTTPS dinamicamente instalando um certificado personalizado no cliente que se deseja proteger. Deve-se notar, no entanto, que esse produto tem como alvo principal a política em sua tarefa de “escutar” um único servidor web, sem o intuito real de proteger sistemas clientes (até onde eu sei, eles são bastante secretos). A pior parte de um agressor usar HTTPS é que o HTTPS é legítimo e obrigatório para muitos sites, o que dificulta seu bloqueio porque os usuários ficarão incomodados.

Codificar ataques é outra forma de invasores atravessarem seu sistema de detecção. Há várias técnicas para codificar requisições e respostas HTTP. Ao servidor, geralmente se envia texto puro, mas depois é possível especificar um *Content-Type*, que pode ter um dentre vários valores, incluindo UTF-8 e UTF-7. Além disso, é possível codificar a informação usando textos codificados por “porcento” (isto

Quadro 2: Tráfego legítimo

Tenha em mente que um agressor nem precisa empregar técnicas de intrusão convencionais para atacar sua rede. Mesmo que você tenha sucesso ao bloquear dados codificados, criptografados, comprimidos ou ocultados de outras formas, e permita somente requisições bem formadas, agressores inteligentes às vezes podem atacar uma rede enviando requisições completamente legítimas.

Por exemplo, considere o caso de um website que reserve voos permitindo que o visitante encontre um voo e reserve um assento específico. O sistema bloqueia o assento durante certo período, permitindo que o usuário digite informações de cartão de crédito etc. Um agressor poderia simplesmente estabelecer algumas poucas centenas de conexões e bloquear todos os assentos, selecionando novamente um assento com uma sessão diferente quando o tempo de bloqueio expirar e o assento for liberado. Capturar esse tipo de ataque com um IDS ou IPS é praticamente impossível.

é, como um espaço em branco, por exemplo que, é definido com o código `%20`), hexadecimais, decimais e nomes. Também é possível utilizar aspas duplas e uma variedade de páginas de código de idiomas internacionais ([quadro 1](#)). Além disso, às vezes é possível misturar as coisas (contanto que o servidor ou cliente aceite e decodifique adequadamente, isto é, para todos os propósitos do termo “legítimo”).

Como não há nenhuma forma de adicionar padrões para todas as codificações possíveis que um agressor pode usar, é preciso normalizar o tráfego antes de varrê-lo em busca de problemas. Isto significa que, em qualquer cabeçalho HTTP que seu IDS/IPS examine, ele primeiro precisa verificar se os dados estão codificados, determinar como decodificá-los, depois normalizá-los e varrê-los. Ele também precisa fazer isso para dados que podem estar codificados em múltiplas camadas ou múltiplas codificações diferentes dentro da mesma *string*.

A ferramenta de pesquisa de segurança *Nikto2* [\[8\]](#) se baseia na biblioteca *libwhisker* [\[9\]](#), que possui vários truques anti-IDS na manga, incluindo inserções de diretórios auto-referentes (`./`) e a inserção de parâmetros de URL falsos, como tabs, novas linhas e valores binários em lugar de espaços. Contra servidores Windows, também é possível usar case sensitive aleatório (porque a maioria dos servidores web Windows não são sensíveis à caixa do texto ao processar requisições) e trocar `/` por `\`. Outra possibilidade é simplesmente inserir caracteres UTF-8 aleatórios; infelizmente, isto geralmente causará problemas (acontece que a maioria dos programadores não são muito bons ao lidar com Unicode) ([figura 2](#)).

JavaScript e Flash

JavaScript e Flash são um sonho que virou realidade para fugir dos sistemas IDS e IPS. Como ambos são

essencialmente linguagens “turing” completas (isto é, são linguagens limpas e precisas que independem da semântica da máquina que as executa), não há nenhuma forma de determinar se o código que contém é hostil se não o observarmos durante a execução e o flagrarmos no ato.

O JavaScript (como a maioria das linguagens interpretadas) é um tanto verborrágico e costuma incluir bastante espaço em branco. O problema é que os sites querem ser rápidos, e o verborrágico e espacoso JavaScript resulta em arquivos maiores que levam mais tempo para ser baixados. Portanto, muitos sites legítimos empacotam o JavaScript de forma a reduzir o tamanho do código. A forma mais fácil de fazer isso é retirar todos os espaços em branco, o que, evidentemente, não reduz significativamente o tamanho.

Existem métodos mais avançados; um método popular é o *Packer* [\[10\]](#) de *Dean Edwards* ([figura 3](#)). O Packer essencialmente cria uma função *wrapper* para descomprimir os dados e amontoa o conteúdo do JavaScript em um formato comprimido, que depois é incluído no arquivo como uma string de dados. Além disso, o Packer consegue encolher os nomes de variáveis (o computador não se importa se é `username` ou simplesmente `a`) e codificar os dados em Base62 (de forma que somente `a-z`, `A-Z` e `0-9` sejam usados). Outra opção é o *YUI Compressor* [\[11\]](#) – o compressor de JavaScript e CSS do Yahoo!. De forma semelhante ao Packer, esta ferramenta reduz os nomes de variáveis, apaga espaços em branco e otimiza macros. Estas ferramentas são compressores JavaScript bem documentados e “educados”.

Os métodos menos educados (leia-se, maliciosos) usam truques como o `unescape()`, que permite que o intruso use codificações misturadas, por exemplo, enfiando caracteres codificados com `%` dentro do stream

de dados. O problema é que muitos sites (incluindo o Google) utilizam `unescape()` para compactar dados de forma que caracteres como `<` e `>` possam ser evitados, dificultando a distinção entre usos legítimos e nefastos.

Os aplicativos em Flash são escritos e depois compilados em arquivos com a extensão `.swf`, que são colocados em servidores web. Entretanto, como a maioria dos formatos binários bem definidos, eles são relativamente fáceis de descompilar e transformar de volta em código-fonte. Portanto, da mesma forma que o empacotamento do JavaScript (para desempenho), muitos sites ofuscaram seus arquivos Flash para protegê-los da descompilação.

Esses programas de ofuscação costumam renomear todas as variáveis para nomes aleatórios, criptografando dados sensíveis como senhas e strings, randomizando diretivas e modificando o fluxo de controle para torná-lo mais difícil de rastrear com um descompilador. Essas ferramentas oferecem uma forma de invasores obscurecerem suas intenções em um aplicativo Flash aparentemente inócuo.

Realisticamente, a melhor esperança para detectar um arquivo Flash ruim é encontrar uma cópia do arquivo malicioso e enviá-la a fabricantes de antivírus para que eles criem assinaturas de segurança.

PDF e Adobe Reader

Uma tecnologia ainda menos segura que JavaScript e Flash é o PDF. Não apenas o formato PDF tem um

<pre>original code: function say_hello() { alert('Hello world'); }</pre>	<pre>Minify (JSMin): function say_hello() {alert('Hello world');}</pre>
<hr/>	
<pre>Packer (Dean Edwards): eval(function(p,a,c,e,d){e=function(c){return c};if(!''.replace(/\w/,String)){while(c--)d[c]=k[c] c;k=[function(e){return d[e]}];e=function(){return ''\w+'';c=1;while(c--){if(k[c])p=p.replace(new RegExp('\\b'+e.c+'\\b','g'),k[c]);}return p;}('0 102\3\4\}\3.5;function say_hello alert Hello world'.split(''),0,{}))}}</pre>	

Figura 3 Um programa em JavaScript simples, comprimido usando JSMin e Packer.

grande número de problemas, como também é possível embutir neles virtualmente qualquer conteúdo desejado (inclusive JavaScript e arquivos Flash). Também é possível ofuscar arquivos PDF de formas que realmente me fazem questionar a equipe do Adobe Reader. Algumas técnicas de ofuscação de PDF [12] incluem:

- ▶ Executar *OpenAction* em objetos criados.
- ▶ Usar uma codificação especial para substituir caracteres (representação por nome).
- ▶ Dividir strings usando contrabarras (\) – é possível fazer um caractere por linha.
- ▶ Converter strings em formato hexadecimal e inserir espaços na string.
- ▶ Criptografia (novamente, para proteger o conteúdo).

Também é possível comprimir o PDF usando */FlatDecode*, criar um monte de anotações de documento aleatórias e depois usar *getAnnots()* [13], que retorna um vetor de anotações para criar um documento maior. Ou ainda, é possível simplesmente criar strings modificadas e usar a função *replace()* para convertê-las de volta para algo malicioso que é executado com *eval()*. É possível ainda, codificar um script JavaScript dentro de um PDF usando codificação octal (isto é, \72 para o caractere :); é possível codificar um ou mais caracteres e o PDF vai tratá-los sem problema.

Para resumir: um invasor pode usar codificação octal em vários caracteres dentro do JavaScript, depois quebrar o exploit em uma série de strings de aparência segura, substituir vários caracteres por outros seguros (a serem substituídos mais tarde pelo mecanismo de expressões regulares) e esconder as strings codificadas dentro de anotações do documento (que alguns sistemas talvez não varram porque são “seguras”).

Isto significa que, se você deseja varrer adequadamente um documen-

to PDF, precisará extrair virtualmente todas as strings de dados, executá-las através de expressões regulares contidas no documento, concatenar as strings e depois buscar nos resultados algo ruim.

Conclusão

Os agressores muito determinados (muitas vezes chamados de APT – de *Advanced Persistent Threat*, ou Ameaça Avançada Persistente) têm acesso às mesmíssimas ferramentas de hardware e software que você usa para defender suas redes. Os

fabricantes de sistemas IDS e IPS não fazem verificações históricas profundas em seus clientes antes de vender-lhes seus produtos. Portanto, os bandidos certamente encontrarão falhas nos produtos que você usa.

Minha recomendação é bloquear ao máximo os dados mal formados (como por exemplo, fragmentos TCP sobrepostos, tipos de codificação variados etc.) e enviar os demais para logs. Se um agressor ainda assim conseguir passar, pelo menos o log pode ajudar a descobrir como isso aconteceu. ■

Mais informações

- [1] Mascaramento de ataques via Craigslist: <http://arstechnica.com/old/content/2008/10/bank-robber-crowdsources-disguise-to-craigslist-floats-away.ars/>
- [2] Fragrouter: <http://archive.ubuntu.com/ubuntu/pool/universe/f/fragrouter/>
- [3] Fragroute: <http://monkey.org/~dugsong/fragroute/>
- [4] hping: <http://www.hping.org/>
- [5] Scapy: <http://www.secdev.org/projects/scapy/>
- [6] Plataforma de Fuzzing Peach: <http://peachfuzzer.com/>
- [7] Packet forensics: <http://www.wired.com/threatlevel/2010/03/packet-forensics/>
- [8] Nikto2: <http://cirt.net/nikto2/>
- [9] libwhisker: <http://www.wiretrip.net/rfp/lw.asp>
- [10] Packer: <http://dean.edwards.name/packer/>
- [11] YUI Compressor: <http://developer.yahoo.com/yui/compressor/>
- [12] Ofuscação de PDF: <http://blog.didierstevens.com/2008/04/29/pdf-let-me-count-the-ways/>
- [13] Ofuscação de PDF usando getAnnots(): <http://blog.fireeye.com/research/2010/01/pdf-obfuscation.html/>
- [14] Nomes de domínio internacionais: http://en.wikipedia.org/wiki/Internationalized_domain_name/

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lhn.com.br/article/4606>





Linux Pro ubuntu

Para o usuário
doméstico
e corporativo



COLEÇÃO Linux Pro

ubuntu

Acompanha sistema completo com suporte e
atualizações até 2011

Luciano Antonio Siqueira



Guia de adoção do Ubuntu
no ambiente doméstico
e corporativo

Em seu novo título,
Linux Pro Ubuntu, a
Linux Magazine oferece
uma visão mais aprofundada
e abrangente do sistema.
O objetivo da obra é atender
aos principais públicos do
Ubuntu: o usuário doméstico
e o corporativo, ambos em
processo de migração do
Microsoft Windows para
o Ubuntu.

**Garanta já o seu pelo
site da Linux Magazine!**

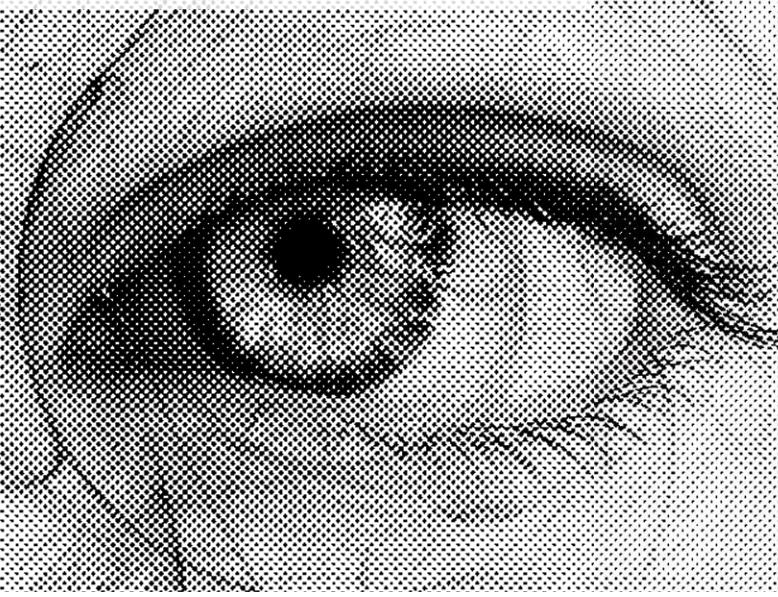
www.LinuxMagazine.com.br

Monitoramento de redes

De olho na rede

Descubra o que está gerando lentidão em sua rede, a origem e o destino do tráfego, protocolos utilizados e muito mais com o NTOP, ferramenta simples e útil.

por Adriano Matos Meier



O que seria de nós, pobres administradores de redes, sem os diversos utilitários existentes, que nos permitem monitorar e controlar o uso dos recursos da rede? Sem o acompanhamento e medição periódicos do uso desses recursos, teríamos a falsa impressão de que precisariam ser realizados investimentos urgentes em novos equipamentos e no aumento da capacidade dos servidores.

Felizmente, um *sysadmin* experiente, que está sempre de olho nas novidades e nos assuntos que andam em voga nos fóruns, encontra praticamente tudo o que precisa para gerenciar a demanda de usuários da rede. De início é possível que seja trabalhoso confi-

gurar servidores, serviços e outros equipamentos, mas normalmente o esforço vale a pena. Nada mais gratificante que precisar de informações sobre o funcionamento e o status da rede e ter uma ferramenta devidamente alimentada, pronta para gerar relatórios detalhados e, se possível, bonitos.

A história

Na Linux Magazine #33 [1], escrevi sobre o gerenciador de redes Cacti [2], e mencionei a possibilidade de integrá-lo a outra ferramenta, o NTOP [3]. Pois bem, chegou o momento de apresentá-lo aos que ainda não o conhecem. O NTOP foi desenvolvido em 1998 por Luca Deri para resolver problemas de desempenho

na rede da Universidade de Pisa, na Itália. Logo depois foi lançado sob a licença GPL, o que o fez evoluir para uma ferramenta robusta.

É escrito em linguagem C, e está disponível para os sistemas Microsoft Windows (95/98/NT/2000/XP/Vista/7) e para todos os sistemas POSIX (Linux/BSD/Unix/Solaris/MacOSX). Um detalhe é que a versão completa compilada para Windows é comercial e vendida por cerca de €49,95. O código-fonte pode ser obtido nos sites de projetos de softwares Freshmeat [4] e SourceForge [5]. No momento, a versão mais recente é a 4.0.1, que foi postada em 08 de agosto de 2010, o que mostra que os mantenedores do projeto não estão acomodados. Também está disponí-

vel nos repositórios da maioria das distribuições GNU/Linux.

Simples mas poderoso

Apesar de ser simples, o NTOP possui características e recursos bastante interessantes, e cito entre elas:

- ▶ Organizar as informações de acordo com os diversos protocolos existentes (por exemplo, TCP/UDP/ICMP/(R)ARP/IPX/Netbios), e pelo IP de origem e destino do tráfego de rede;
- ▶ A classificação do tráfego pode ser exibida com base em diferentes critérios (por exemplo, pelo horário ou pelo tipo: LAN/WAN);
- ▶ Gera estatísticas de uso dos protocolos, entre outras informações do tráfego, e as armazena em uma base RRD;
- ▶ Decodifica diversos protocolos da camada de aplicação como, por exemplo, os utilizados nos softwares “peer-to-peer” (softwares de compartilhamento de arquivos ponto a ponto, em sua maioria);
- ▶ Pode identificar, de forma passiva, a identidade, o sistema operacional e outras informações dos usuários e computadores da rede;
- ▶ Atua como coletor NetFlow/sFlow para os fluxos gerados pelos roteadores (por exemplo, Cisco [6] e Juniper) e pelos switches;
- ▶ Suporta múltiplas interfaces de rede (reais e virtuais);
- ▶ Web Server integrado com suporte a HTTP e HTTPS;
- ▶ Produz estatísticas de tráfego baseado no protocolo de gerenciamento RMON.

Caça aos consumidores de banda

O NTOP faz uso da biblioteca `libpcap` para coletar as informações, sendo assim, é necessário que seja

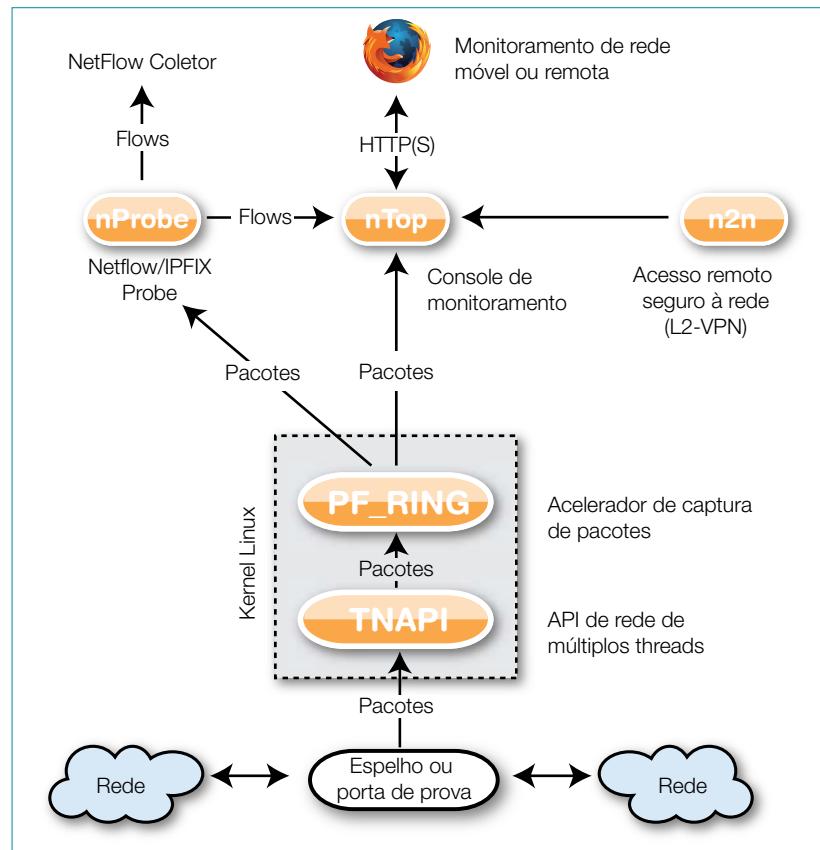


Figura 1 Posicionamento do gateway na rede.

instalado no gateway da rede. A **figura 1** mostra o posicionamento do gateway na rede. Para iniciar a caçada aos consumidores de recursos e banda da rede, começamos pela

instalação do NTOP. No Debian (e derivados), um simples `apt-get install ntop` é suficiente. Antes de realizar o primeiro acesso, é preciso executar o comando `ntop` para defi-

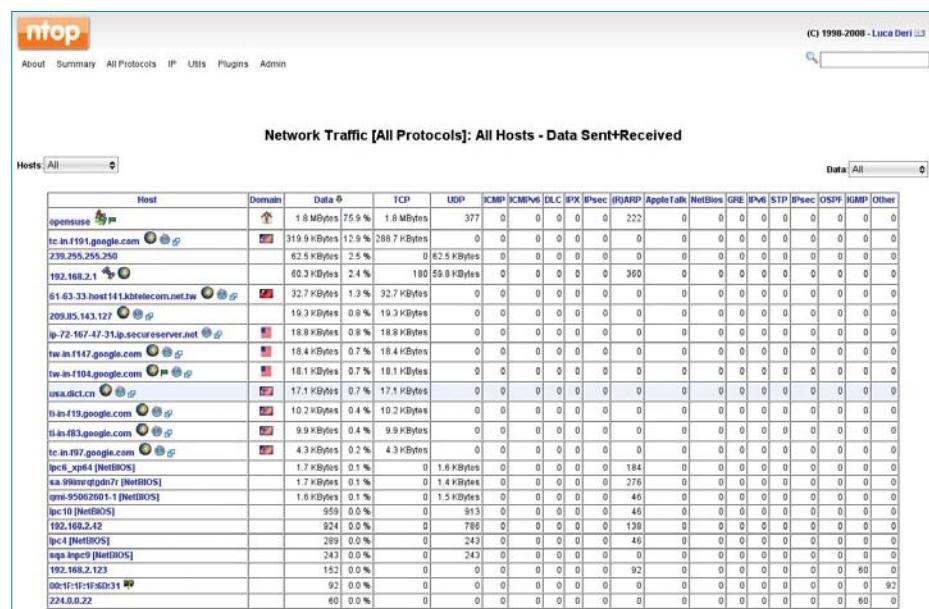


Figura 2 Riqueza de detalhes dos relatórios do NTOP.

Tabela 1: Principais parâmetros de uso no modo interativo

Parâmetro	Função
<code>-u usuário</code>	Informa qual o usuário a ser utilizado no NTOP.
<code>-a arquivo</code>	Informar em qual arquivo serão gravados os logs das requisições feitas ao servidor web do NTOP.
<code>-b</code>	Faz com que os decodificadores, responsáveis pela análise do tráfego, sejam desativados, a fim de reduzir o uso dos recursos do computador, porém, isso pode, entretanto, reduzir a quantidade de detalhes nas informações geradas.
<code>-d</code>	Faz com que o programa seja executado como um daemon (em segundo plano).
<code>-f arquivo</code>	Faz com que o programa capture informações de um arquivo no formato TCPdump e mostre os resultados na interface web. Para utilizar esse parâmetro, também deve ser utilizado o parâmetro <code>-m</code> .
<code>-m</code>	Informa ao programa o endereço IP e a máscara da rede em que o arquivo gerado com o parâmetro <code>-f</code> foi criado.
<code>-g</code>	Faz com que sejam capturados apenas os pacotes relacionados à rede local. Neste caso também deve ser utilizado o parâmetro <code>-m</code> .
<code>-i interface</code>	Indica qual interface deve ser monitorada. Para monitorar mais de uma interface, os nomes devem ser separados por vírgula.
<code>-l arquivo</code>	Gera os logs no formato do TCPdump. Deve ser usado juntamente com o parâmetro <code>-0</code> .
<code>-0 caminho</code>	Indica o caminho para a pasta de destino onde os logs serão gravados.
<code>-n</code>	Impede que o programa converta endereço IP em nome.
<code>-p</code>	Indica que apenas os pacotes que usam os protocolos informados (no parâmetro) devem ser examinados.
<code>-q</code>	Faz com que seja criado um arquivo no formato TCPdump com os registros do pacotes suspeitos, tendo em vista que o NTOP possui várias regras para determinar se um pacote é suspeito ou não. Também necessita do parâmetro <code>-0</code> .
<code>-w porta_http</code>	Indica em qual porta o NTOP será executado, utilizando o protocolo HTTP. O padrão é a porta 3000.
<code>-W porta_https</code>	Indica em qual porta o NTOP será executado, utilizando o protocolo HTTPS, que conta com vários recursos de segurança. O padrão é a porta 3001.
<code>-A</code>	Para alterar a senha do administrador.
<code>-r segundos</code>	Especifica o tempo entre cada atualização da página no navegador. O padrão é 3 segundos.

nir a senha do usuário *admin*. Isso é necessário, pois caso contrário, o serviço não entrará em execução.

Uma vez definida a senha, as próximas execuções podem ser feitas sob a forma de *daemon*, com o comando `/etc/init.d/ntop start`. Assim que o NTOP estiver em execução, basta aguardar que ele faça o seu trabalho, que é coletar o tráfego que passar pelo gateway e gerar os relatórios e estatísticas.

Para acessar interface web do NTOP, além de informar o endereço do servidor, no final da URL, deve ser informada a porta 3000, por exemplo, <http://monitorntop:3000> (para o protocolo HTTPS deve ser informada a porta 3001). Apesar de utilizar uma interface acessível no navegador, não é necessário instalar o Apache, por exemplo, pois o pacote do NTOP já possui um servidor web nativo. Também é pos-

sível utilizá-lo em modo interativo no shell. Como não possui arquivo de configuração, para alterar detalhes do seu funcionamento, assim como para utilizá-lo em modo interativo, devem ser usadas as opções da **tabela 1**. As demais configurações devem ser realizadas através da interface web, através do menu *Admin/Configure*.

A **figura 2** mostra a riqueza de detalhes que o NTOP produz sob

a forma de relatório sobre as conexões ativas. Na primeira coluna são identificados os *hosts* envolvidos. De acordo com o tipo de tráfego detectado, ele adiciona ícones que representam, por exemplo, servidores web, servidores DNS, roteadores, impressoras, entre diversos outros. Também identifica o país ao qual um domínio que está sendo acessado pertence, a quantidade de tráfego transferido para cada um deles e a quantidade de pacotes para cada tipo de protocolo suportado. A **figura 3** ilustra os gráficos de uso dos protocolos, assim como a quantidade de tráfego e a porcentagem que isso representa da banda da rede. Uma opção importante é a possibilidade de restringir o acesso a determinadas áreas da ferramenta. Isso é feito através do menu *Admin/Configure* e selecionando a opção *Protect URLs*, onde devem ser adicionados os usuários com permissão de acesso (através de senha).

Conclusão

Existem diversas outras ferramentas que possuem a mesma função do Ntop, como o Netflow Analyzer [7], da Manage Engine, e o Scrutinizer [8], da Plixer. Ambas são ferramentas comerciais, mas é possível utilizá-las livremente com limitações dos recursos (por exemplo, monitoramento de, no máximo, duas interfaces simultaneamente), sem prazo de expiração, mas o Ntop ainda figura entre a preferência de grande parte dos administradores de sistemas. ■

Sobre o autor

Adriano Matos Meier (matos@sc.senai.br) é Tecnólogo em Redes de Computadores e Pós-Graduando em Gestão de Segurança da Informação. Atualmente é analista de redes no SENAI de Santa Catarina. Também atua como instrutor de treinamento GNU/Linux.

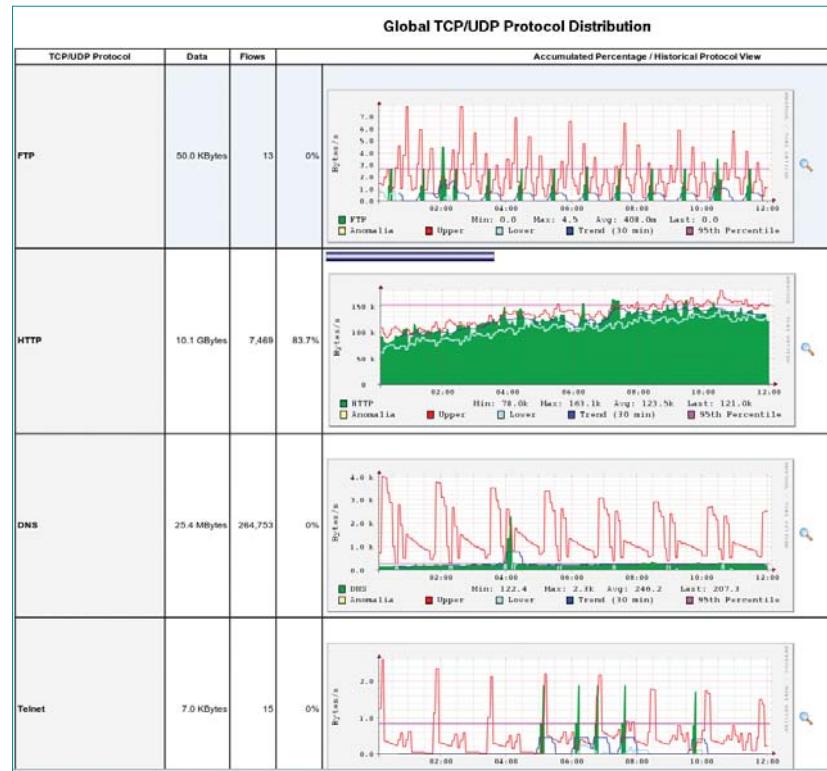


Figura 3 Gráfico com informações sobre o uso dos protocolos da rede.

Mais informações

- [1] Edição #33 da Linux Magazine: http://www.linuxmagazine.com.br/issue/lm_33_dual_core
- [2] Página oficial do Cacti: <http://www.cacti.net/>
- [3] Página oficial do Ntop: <http://www.ntop.org/>
- [4] Ntop no Freshmeat.net: <http://freshmeat.net/projects/ntop/>
- [5] Ntop no SourceForge.net: <http://sourceforge.net/projects/ntop/>
- [6] Tecnologia NetFlow, desenvolvida pela Cisco: <http://www.cisco.com/web/go/netflow>
- [7] Página oficial do NetFlow Analyzer: <http://www.manageengine.com/products/netflow>
- [8] Página oficial do Scrutinizer: <http://www.plixer.com/products/netflow-sflow/free-netflow-scrutinizer.php>

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4577>



Programação shell script

Shell script: trabalhando com pipes

Ferramentas especiais do shell auxiliam na combinação de comandos para criar aplicativos de maior complexidade.

por Martin Streicher

A linha de comando do Linux (conhecida simplesmente por shell, Bash ou terminal) oferece centenas de pequenos utilitários para ler, escrever e analisar dados. Com alguma digitação extra é possível combinar esses utilitários em numerosos aplicativos improvisados e de maior complexidade, para fins diversos. Por exemplo, imagine que é preciso extrair as falas de um ator. Com o texto exibido na **listagem 1**, é preciso produzir *That's what they call a sanity clause* do Groucho. O comando `grep` encontra substrings, strings e padrões em um arquivo de texto. Usamos o comando `grep` para encontrar todas as falas que começam com a string `GROUCHO`. Depois, usamos o parâmetro `cut` (cortar) para dividir as linhas correspondentes em pedaços e combinar os dois comandos com o pipe (`|`).

O comando `grep` faz uma busca no arquivo `marx.txt` por todas as ocorrências da string que aparecem no início de uma linha (`-E '^Groucho'`), ignorando letras em maiúsculas ou minúsculas (`-i`). O `cut` separa a linha em campos delimitados por dois pontos (`-d ':'`) e seleciona o segundo campo (`-f 2`). O operador pipe transforma a saída de `grep` na entrada para o parâmetro `cut`.

O pipe conecta dois comandos quaisquer, possibilitando a construção

de uma longa cadeia de comandos com vários pipes. Por exemplo, se quiser contar o número de palavras ditas por Groucho, adicione `| wc -w` ao comando anterior.

O pipe é apenas uma das formas de redirecionamento. Ferramentas de redirecionamento podem alterar a fonte ou o destino, ou ambos, dos dados processados. O shell oferece formas de redirecionamento também, e aprender a lidar com essas ferramentas é a chave para dominar o shell.

Dados que entram, dados que saem

Caso o `grep` seja executado sozinho, ele irá ler dados do *standard input device* (`stdin` – dispositivo de entrada padrão) e emitir os resultados para o *standard output device* (`stdout` – dispositivo de saída padrão). Os erros são enviados para um terceiro canal chamado *standard error device* (`stderr` – dispositivo de erro padrão).

Normalmente, os dados para o `stdin` são fornecidos pelo usuário através do teclado e, por padrão, o `stdout` e o `stderr` são enviados ao terminal conectado ao shell. No entanto, tudo isso pode ser redirecionado. Por exemplo, é possível redirecionar o `stdin` para que este

leia dados de um arquivo ao invés de ler a entrada do teclado. Também é possível redirecionar o `stdout` e o `stderr` (separadamente) para que os dados sejam escritos em outro lugar que não seja a janela do terminal.

A sintaxe do redirecionamento depende do terminal utilizado, mas quase todos eles suportam as seguintes operações:

- ▶ < `input_file` redireciona o `stdin` para ler dados de um determinado arquivo (neste caso, `output_file`).
- ▶ `> output_file` redireciona o `stdout`, enviando os resultados de um comando ou de um pipe (mas não os erros) para o arquivo especificado (neste caso `output_file`). Se o arquivo não existe, ele é criado; caso exista, seu conteúdo é substituído pelo resultado.
- ▶ `>> output_file` é similar a `>` mas adiciona o `stdout` ao conteúdo do arquivo determinado. Caso o arquivo não exista, será criado; no entanto, se ele existir, seu conteúdo é preservado e os resultados são adicionados a ele.
- ▶ `& output_file` funciona como o `>` mas captura `stdout` e `stderr` no arquivo especificado, criando o arquivo caso necessário, e sobrescrevendo seu conteúdo no caso dele já existir.

Alguns exemplos são mostrados na **listagem 2**. O primeiro comando deve ser conhecido. O adicional `>groucho.txt` salva a saída da linha de comando para um arquivo chamado `groucho.txt`. O segundo comando anexa a string `I started work on Nov 2 at 9 am` ao arquivo `timecard.txt`. O terceiro comando executa o script Ruby `myapp.rb`. A entrada é tirada de um arquivo chamado `data` e o `stdout` e o `stderr` do comando são capturados no arquivo log.

Uso avançado do pipe

Caso seja necessário buscar um arquivo específico em seu diretório `home` ou em todo o sistema, o utilitário `find` é imprescindível. Por exemplo, para encontrar todos os arquivos do seu diretório `home` que possuem a palavra “time” no nome, digite (lembre-se que `~` é o substituto de `$HOME`): `$ find ~ -name '*time*'`.

O comando `find` pode buscar arquivos usando vários critérios, incluindo modificações de tempo e tamanho e também pode ser usado como base para todo tipo de análise de arquivos. Por exemplo, considere a seguinte combinação na linha de comando:

```
$ find /caminhos/dos/arquivos →
-type f | xargs grep -H -I →
-i -n string
```

Esse comando enumera todos os arquivos simples no caminho indicado, procura em cada um deles ocorrências de uma determinada string e gera uma lista de arquivos que contêm a string, incluindo o número da linha no texto específico correspondente. O comando `find` faz uma busca em toda a hierarquia em `/caminho/dos/arquivos`, procurando por arquivos simples (`-type f`). A saída é uma lista de arquivos.

O parâmetro `xargs` é especial, pois inicia um comando – no exemplo, trata-se do `grep` mais todo o resto até o fim da linha – uma vez para cada

arquivo listado pelo `find`. As opções `-H` e `-i` prefaziam cada combinação com o nome do arquivo e o número da linha de cada combinação, respectivamente. A opção `-n` ignora maiúsculas e minúsculas. A opção `-I` não computa arquivos binários.

Assumindo que o diretório `/caminho/da/fonte` contém os arquivos `a`, `b` e `c`, o uso do `find` junto com o `xargs` é o equivalente a:

```
$ find /caminho/da/fonte
a
b
c
$ grep -H -I -i -n string a
$ grep -H -I -i -n string b
$ grep -H -I -i -n string c
```

Na verdade, a busca de vários arquivos é tão comum que o `grep` possui sua própria opção para recuperar a hierarquia de um sistema de arquivos. Use o parâmetro `-d recurse` ou seus sinônimos `-R` ou `-r`. Por exemplo, o comando `grep -H -I -i`

`-n -R string /caminho/para/fonte` funciona tão bem quanto a combinação de `find` e `xargs`. No entanto, caso precise ser seletivo e recuperar apenas tipos específicos de arquivos, use o `find`.

Cemitério dos bits

Como vimos, a maioria dos comandos emite saídas de um tipo ou outro. A maioria dos comandos de linha de comando usa `stdout` e `stderr` para mostrar algum tipo de resultado e mensagens de erro, nessa ordem. Se quiser ignorar esse tipo de produção – o que é útil, pois isso geralmente interfere com o trabalho na linha de comando – redirecione sua saída para o “cemitério dos bits”, em `/dev/null`. Os bits entram, mas não saem.

A **listagem 3** mostra um exemplo simples. Se redirecionar a saída padrão do comando `cat` para `/dev/null`, nada é exibido (todos os bits são jogados no arquivo virtual vertical). No entanto, caso um erro ocorra, as mensagens de erro, que são enviadas

Listagem 1: Trecho de um script dos irmãos Marx

```
01 GROUCHO: That's what they call a sanity clause.
02 CHICO: Ah, you fool wit me. There ain't no Sanity Claus!
01 $ grep -i -E '^Groucho' marx.txt | cut -d ':' -f 2
02 That's what they call a sanite clause.
```

Listagem 2: Exemplos de redirecionamento

```
01 $ # Primeiro comando
02 $ grep -i -E '^Groucho' marx.txt | cut -d ':' -f 2 > groucho.txt
03 $ cat groucho.txt
04 That's what they call a sanity clause.
05
06 $ cat timecard.txt
07 I started work on Nov 1 at 8.15 am.
08 I finished work on Nov 1 at 5 pm.
09
10 $ # Segundo comando
11 $echo 'I started work on Nov 2 at 9 am.' >> timecard.txt
12
13 $ cat timecard.txt
14 I started work on Nov 1 at 8.15 am.
15 I finished work on Nov 1 at 5 pm.
16 I started work on Nov 2 at 9 am.
17
18 $ # Terceiro comando
19 $ ruby myapp.rb < data >& log
```

para `stderr`, serão exibidas. Se quiser ignorar todas as saídas, utilize o operador `>&` para enviar `stdout` e `stderr` para o cemitério dos bits.

Também é possível usar `/dev/null` como um arquivo sem tamanho para esvaziar arquivos existentes ou criar novos arquivos vazios ([listagem 4](#)).

Outros truques

Além do redirecionamento, o shell oferece vários outros truques para poupar tempo e esforço. Utilizar argumentos entre crases (`...`) expande alguns comandos. Uma frase entre crases é executada primeiro, enquanto o shell interpreta a linha de comando, e sua saída substitui a frase original. É possível usar crases para dar prioridade, por exemplo, a um nome de arquivo ou determinado dado:

Listagem 3: O cemitério dos bits

```
01 $ ls
02 secret.txt
03 $ cat secret.txt
04 I am the Walrus.
05 $ cat secret.txt > /dev/null
06 $ cat socrates.txt > /dev/null
07 cat: socrates.txt: No such file or ↵
    directory
08 $ cat socrates.txt >& /dev/null
09 $ echo Done.
10 Done.
```

Listagem 4: Arquivos vazios

```
01 $ cat secret.txt
02 Anakin Skywalker is Darth Vader.
03 $ cp /dev/null secret.txt
04 $ cat secret.txt
05
06 $ echo "The moon is made of ↵
    cheese!" > secret.txt
07 $ cat secret.txt
08 The moon is made of cheese!
09 $ cat /dev/null > secret.txt
10 $ cat secret.txt
11
12 $ cp /dev/null newsecret.txt
13 $ cat newsecret.txt
14
15 $ echo Done.
16 Done.
```

```
$ ps > state.`date '+%F'`
$ ls state*
state.2009-11-21
$ cat state.2009-11-21
13842 ttys001 0:00.54 -bash
30600 ttys001 1:57.15
ruby ./script/server
$ cat `ls state.*`
13842 ttys001 0:00.54 -bash
30600 ttys001 1:57.15
ruby ./script/server
```

A primeira linha de comando captura a lista de processos em execução em um arquivo chamado algo como `state.AAAA-MM-DD`, onde a parte de data do nome é gerada pelo comando `date '+ %F'`. As aspas simples em torno do argumento evitam que o shell interprete + e %. O último comando mostra um outro exemplo da crase. A execução de `ls state.*` produz um nome de arquivo.

Falando de resultados de captura, se for preciso capturar a saída de uma série de comandos, combine-os dentro de chaves ({...}): `$ { ps; w } > state.`date '+%F'``. No comando anterior, `ps` é executado, seguido por `w` (que mostra quem está usando a máquina) e a saída de tudo é capturada em um arquivo.

É possível também colocar uma sequência de comandos entre parênteses para alcançar o mesmo resultado, com uma diferença importante: a série de comandos entre parênteses é executada em um subshell, e não afeta o estado do shell corrente.

Por exemplo, espera-se que o comando `{ cd $HOME; ls -1}; pwd` produza a mesma saída de `(cd $HOME; ls); pwd`; no entanto, os comandos entre chaves alteram o diretório de trabalho do shell corrente. A segunda técnica não faz isso.

O uso de uma combinação ou um subshell depende de suas intenções, embora o subshell seja muito mais poderoso. É possível usar um subshell para expandir um comando, assim como com crases. Melhor

ainda, um subshell pode conter outro subshell, desse modo uma expansão pode conter outra.

O comando a seguir: `$ {ps; w} > state.$(date '+%F')` é idêntico a `{ ps; w } > state.`date '+%F'``. A notação `$()` executa os comandos dentro dos parênteses que depois são substituídos pela saída. Em outras palavras, `$()` expande o comando, do mesmo modo que a crase; no entanto, diferentemente da crase, utilizar `$()` pode ser bem complexo e pode até incluir outras expansões `$()`:

```
$ (cd $(grep strike /etc/passwd | cut -f6 -d':'); ls)xw
```

Esse comando busca o arquivo de senha do sistema para encontrar uma entrada para o usuário `strike`, retém o campo do diretório `home` (campo 6 no arquivo de senhas, contando a partir do zero), vai até esse diretório e lista seu conteúdo. A saída de `grep /etc/passwd strike | cut -f6 -d':'` é expandida antes de qualquer outra operação. O subshell possui muitas utilizações, por isso é preferível usá-lo no lugar dos operadores `{ }` ou das crases.

Conclusão

Consulte a documentação do seu terminal shell para aprender suas características especiais e truques. Se estiver usando um shell mais recente em vez do Bash, é possível encontrar opções adicionais disponíveis. Por exemplo, o Z Shell fornece redirecionamento multi-way para ler vários arquivos de entrada e emitir várias cópias de saída. ■

Gostou do artigo?

Queremos ouvir sua opinião.
Fale conosco em
cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lmn.com.br/article/4572>

Monitoramento personalizado

Monitore os daemons

Os administradores geralmente escrevem programas personalizados de monitoramento para garantir que seus daemons ofereçam a disponibilidade necessária. Mas as ferramentas simples do shell também são bem adaptadas para essa tarefa, e não apenas para sistemas com poucos recursos.

por Harald Zisler



Os daemons Unix normalmente fazem seu trabalho discretamente em segundo plano. A tabela de processos, que é a saída do comando `ps`, só mostra que os serviços foram iniciados, embora na pior das hipóteses, só estejam ali como zumbis, ou seja, inativos. Se um daemon está realmente trabalhando ou não, não é algo que a tabela de processos irá mostrar. Em outras palavras, é preciso realizar um diagnóstico mais detalhado. A ideia subjacente é a de escrever um script sensível para serviços, que execute uma verificação concreta da disponibilidade de cada um deles.

Quase todos os programas devolvem códigos de saída padronizados quando são terminados. O parâmetro

`0` significa processamento livre de erros, enquanto `1` indica que alguns problemas foram encontrados. Esse valor é armazenado na variável do shell `$?`, que avalia o status do serviço. Vários programas são adequados para acesso automatizado, sem intervenção humana ao serviço prestado por um daemon e todos eles são executados no shell sem interface gráfica. Esses programas costumam oferecer uma opção (geralmente `-q`) que suprime a saída. Logs de erro podem ser obtidos através do redirecionamento da saída de erro em um arquivo ou, se disponível, definindo a opção do programa correspondente.

O necessário é encontrar um programa cliente correspondente para testar a operação de cada serviço.

Servidores web

Para verificar um servidor web, é possível usar o utilitário `wget`. A linha de comando do script shell para isso seria: `wget --spider -q ip-address`.

A opção `--spider` avisa o `wget` para verificar se a página existe, mas não para carregá-la. Definir o endereço IP em vez do nome do *host* evita um falso positivo, caso a resolução de nomes baseada em DNS falhe por algum motivo.

Quase todos os bancos de dados conhecidos incluem um programa cliente em linha de comando – por exemplo, o `mysql` para o MySQL ou `psql` para o PostgreSQL. Como alternativa, é possível usar o ODBC para acessar o banco de dados no

Listagem 1: Monitoramento de banco de dados

```

01 #! /bin/sh
02
03 while true
04 do
05
06 time=$(date +%d.%m.%y\ %H:%M\)
07
08 psql -U monitor -d monitor -c "select * from watch;" ↵
09
10 if $? -eq;
11
12 then
13
14 echo "$time: Database is not accessible! **" >> ↵
    dba.log
15 /usr/local/etc/rc.d/002pgsql.sh start
16 sleep 15
17 psql -U monitor -d monitor -c "select * from watch;" ↵
18
19 if [ $? -eq 0 ];
20
21 then
22
23 echo "$time: Database online!++++" >> dba.log
24
25 else
26
27 echo "$time: Database: serious error! ➔
    *****" >> dba.log
28 echo "$time:Unable to restart! *****" >> ↵
    dba.log
29 while true
30 do
31 psql -U monitor -d monitor
32
33 if [ $? -eq 0 ];
34
35 then
36
37 time=$(date +%d.%m.%y\ %H:%M\)
38 echo "$time: Database online! ++++" >> dba.log
39 break
40
41 fi
42 sleep 15
43 done3
44
45 fi
46
47 fi
48 sleepd 15
49
50 done

```

seu script de monitoramento, como a ferramenta `isql` fornecida pelo projeto Unix ODBC.

Para maior facilidade de acesso, talvez seja necessário criar um usuário (sem privilégios), um banco de dados e uma tabela para o teste de consulta no servidor de banco de dados. Se escolher a opção ODBC, também será preciso utilizar um arquivo `.odbc.ini` com as credenciais de acesso corretas.

O cliente shell `psql` do banco de dados PostgreSQL apresenta também

o problema de códigos de saída não-padrão. O valor 1 corresponde a um erro na consulta, embora a tentativa de conexão tenha sido bem sucedida e o valor 2 indica um erro de conexão. Um teste de conexão com `psql` ficaria assim:

```
psql -U User -d Database -c ↵
"select * from test_table;"
```

Para acessar o ODBC, será preciso canalizar a consulta SQL para o cliente:

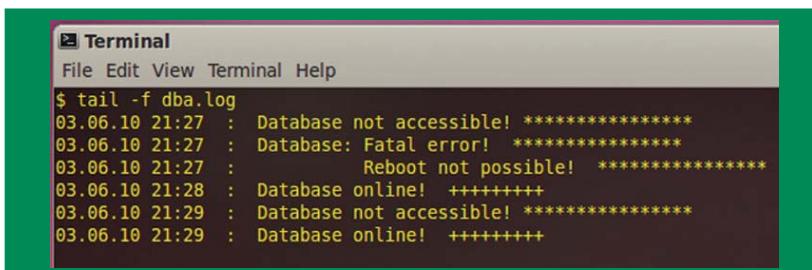


Figura 1 Após ser iniciado, o script devolve o log no console: disponibilidade, erro, reinicialização e banco de dados em operação.

```
echo "select * from test_table;" ↵
| isql ODBC_data_source user
```

Para o daemon de impressão `cups`, o `lpq` oferece um método simples para verificar se o daemon está ativo. Se precisar verificar o acesso a impressoras individuais, além disso, será preciso fornecer o nome da fila de impressão e usar o `grep` no código de saída. Para certificar-se de que o código de saída está em conformidade com esse comportamento, o `grep` verifica a saída que é recebida se a impressora estiver ativa:

```
lpq -Pprinter | grep -q "printer ➔
is ready"
```

Para coincidir com a saída do comando `lpq`, será preciso modificar a string de busca para `grep`.

Já o comando `ping` checa as conexões de rede. Os códigos de erro de saída diferem, dependendo do

seu sistema operacional. O ping do FreeBSD usa o valor `2` e o ping do Linux usa o valor `1`.

O número de pacotes de teste é limitado pela opção de pacotes `-c`, o que melhora o tempo de execução do script e evita o tráfego de rede desnecessário. O uso de um endereço IP como alvo, evita-se o risco de falsos positivos de resolução de nomes com erros: `ping -c1 ip_address`.

Scripts de monitoramento podem, obviamente, ser estendidos para cobrir muitos outros parâmetros do sistema, tais como o uso de espaço em disco (`df`), os usuários conectados (`who`), e muito mais.

Se um erro ou infração de valor ocorre, o script pode usar essas informações para gerar uma mensagem e notificar o administrador do sistema.

A mensagem deve incluir o *hostname*, a data e a hora em que o erro ocorreu. As mensagens podem ser armazenadas em um arquivo sobre o qual o administrador do sistema tenha acesso permanente. Para permitir que isso aconteça, basta exibir o arquivo de log em um terminal e usar `tail -f`, mas outras formas de comunicação também são possíveis, como o `-SMS`, por exemplo.

Se o script shell tiver os privilégios corretos, ele pode agir e reiniciar um servidor, remover arquivos em bloco, ou mesmo reiniciar o sistema inteiro. É aconselhável evitar executar esse tipo de script como *root*, e uma alternativa é definir usuários e grupos especiais para o script e o processo (o que é o caso de muitos daemons).

Reiniciar o banco de dados

O script de exemplo presente na **listagem 1** monitora uma instância de banco de dados ativa e notifica o administrador se o banco de dados

Listagem 2: Monitoramento do CUPS

```
01 #! /bin/sh
02
03 while true
04 do
05
06 lpq -Plp | grep -q "lp is ready"
07
08 if [ $? -gt 0 ]
09 then
10 cupenable lp
11 if
12
13 sleep 15
14
15 done
```

por acaso falhar e, em seguida, for reiniciado com sucesso (**figura 1**). Se não for possível iniciar o daemon, ele espera que o administrador interveña e controle a situação.

Reiniciar a impressora

O segundo script de exemplo refere-se ao serviço de impressão. O que pode ser visto na **listagem 2** é tirado de um exemplo de produção, no qual o servidor `cupsd` tem um problema desconhecido com uma impressora de rede. A impressora foi desativada várias vezes, causando muita frustração para os usuários e um trabalho desnecessário para os administradores do sistema. O script não devolve mensagens de saída; em vez disso, simplesmente reinicia o serviço. Esses scripts po-

dem ser executados manualmente (para uma correção temporária ou então uma verificação rápida) ou como scripts RC.

Conclusão

Os administradores não precisam de um conjunto de monitoramento complexo que abranja todos os aspectos do ambiente e que tenha uma curva de aprendizado semanal. Com algum conhecimento de scripts, é possível criar com facilidade seus próprios scripts para monitorar processos de servidor e reiniciá-los de forma autônoma se assim for preciso. O uso de scripts para monitorar daemons e outras funções do sistema não é restrito a pequenos sistemas embarcados. Com scripts sob medida para atender suas necessidades, é possível criar seu próprio arsenal de solução de problemas. ■

Sobre o autor

Harald Zisler trabalha com sistemas operacionais do tipo Unix desde o início de 1990.

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site:
<http://lnm.com.br/article/4574>



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 3675-2600 ou anuncios@linuxmagazine.com.br

Fornecedor de Hardware = 1

Redes e Telefonia / PBX = 2

Integrador de Soluções = 3

Literatura / Editora = 4

Fornecedor de Software = 5

Consultoria / Treinamento = 6

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
Bahia										
IMTECH	Salvador	Av. Antonio Carlos Magalhaes, 846 – Edifício MaxCenter – Sala 337 – CEP 41825-000	71 4062-8688	www.imtech.com.br	✓	✓	✓	✓	✓	✓
Magiclink Soluções	Salvador	Rua Dr. José Peroba, 275. Ed. Metrópolis Empresarial 1005, STIEP	71 2101-0200	www.magiclink.com.br	✓	✓	✓	✓	✓	✓
Ceará										
F13 Tecnologia	Fortaleza	Rua Padre Valdevino, 526 – Centro	85 3252-3836	www.f13.com.br	✓	✓	✓	✓	✓	✓
Nettton Tecnologia e Segurança da Informação	Fortaleza	Av. Oliveira Paiva, 941, Cidade dos Funcionários – CEP 60822-130	85 3878-1900	www.nettton.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 – sl 201, 202 – Praia do Canto CEP: 29055-410	27 3315-2370	www.megawork.com.br	✓	✓	✓	✓	✓	✓
Spirit Linux	Vitória	Rua Marins Alvarino, 150 – CEP: 29047-660	27 3227-5543	www.spiritlex.com.br	✓	✓	✓	✓	✓	✓
Goiás										
3WAY Networks	Goiânia	Av. Quarta Radial, 1952. Setor Pedro Ludovico – CEP: 74830-130	62 3232-9333	www.3way.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	✓	✓	✓	✓	✓	✓
Zarafa Brasil	Belo Horizonte	Rua dos Goitacazes, 103 – Sala 2001 – CEP: 30190-910	31 2626-6926	www.zarafabrasil.com.br	✓	✓	✓	✓	✓	✓
Paraná										
iSolve	Curitiba	Av. Cândido de Abreu, 526, Cj. 1206B – CEP: 80530-000	41 252-2977	www.isolve.com.br	✓	✓	✓	✓	✓	✓
Mandriva Conectiva	Curitiba	Rua Tocantins, 89 – Cristo Rei – CEP: 80050-430	41 3360-2600	www.mandriva.com.br	✓	✓	✓	✓	✓	✓
Telway Tecnologia	Curitiba	Rua Francisco Rocha 1830/71	41 3203-0375	www.telway.com.br	✓	✓	✓	✓	✓	✓
Pernambuco										
Fuctura Tecnologia	Recife	Rua Nicarágua, 159 – Espinheiro – CEP: 52020-190	81 3223-8348	www.fuctura.com.br	✓	✓	✓	✓	✓	✓
Rio de Janeiro										
Clavis Segurança da Informação	Rio de Janeiro	Av. Rio Branco 156, 1303 – Centro – CEP: 20040-901	21 2561-0867	www.clavis.com.br	✓	✓	✓	✓	✓	✓
Linux Solutions Informática	Rio de Janeiro	Av. Presidente Vargas 962 – sala 1001	21 2526-7262	www.linuxsolutions.com.br	✓	✓	✓	✓	✓	✓
Múltipla Tecnologia da Informação	Rio de Janeiro	Av. Rio Branco, 37, 14º 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	✓	✓	✓	✓	✓	✓
RedeHost Internet	Gravataí	Rua Dr. Luiz Bastos do Prado, 1505 – Conj. 301 CEP: 94010-021	51 4062 0909	www.redehost.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	✓	✓	✓	✓	✓	✓
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3301-1408	www.tehospedo.com.br	✓	✓	✓	✓	✓	✓
Propus Informática	Porto Alegre	Rua Santa Rita, 282 – CEP: 90220-220	51 3024-3568	www.propus.com.br	✓	✓	✓	✓	✓	✓
São Paulo										
Ws Host	Arthur Nogueira	Rua Jerere, 36 – Vista Alegre – CEP: 13280-000	19 3846-1137	www.wshost.com.br	✓	✓	✓	✓	✓	✓
DigiVoice	Barueri	Al. Juruá, 159, térreo - Alphaville – CEP: 06455-010	11 4195-2557	www.digivoice.com.br	✓	✓	✓	✓	✓	✓
Dextra Sistemas	Campinas	Rua Antônio Paioli, 320 – Pq. das Universidades – CEP: 13086-045	19 3256-6722	www.dextra.com.br	✓	✓	✓	✓	✓	✓
Insigne Free Software do Brasil	Campinas	Av. Andrade Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignefreesoftware.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	✓	✓	✓	✓	✓	✓

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
São Paulo (continuação)										
Epopéia Informática	Marília	Rua Goiás, 392 – Bairro Cascata – CEP: 17509-140	14 3413-1137	www.epopeia.com.br						✓
Redentor	Osasco	Rua Costante Piovan, 150 – Jd. Três Montanhas – CEP: 06263-270	11 2106-9392	www.redentor.ind.br	✓					
Go-Global	Santana de Parnaíba	Av. Yojiro Takaoca, 4384, Ed. Shopping Service, Cj. 1013 – CEP: 06541-038	11 2173-4211	www.go-global.com.br		✓	✓			
AW2NET	Santo André	Rua Edson Soares, 59 – CEP: 09760-350	11 4990-0065	www.aw2net.com.br	✓		✓			
Async Open Source	São Carlos	Rua Orlando Damiano, 2212 – CEP 13560-450	16 3376-0125	www.async.com.br	✓		✓			
Delix Internet	São José do Rio Preto	Rua Voluntário de São Paulo, 3066 9º – Centro – CEP: 15015-909	11 4062-9889	www.delixhosting.com.br	✓	✓	✓			
2MI Tecnologia e Informação	São Paulo	Rua Franco Alfano, 262 – CEP: 5730-010	11 4203-3937	www.2mi.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		✓	✓			
Blanes	São Paulo	Rua André Ampère, 153 – 9º andar – Conj. 91 CEP: 04562-907 (próx. Av. L. C. Berrini)	11 5506-9677	www.blanes.com.br	✓	✓	✓			
Bull Ltda	São Paulo	Av. Angélica, 903 – CEP: 01227-901	11 3824-4700	www.bull.com	✓	✓	✓			
Commlogik do Brasil Ltda.	São Paulo	Av. das Nações Unidas, 13.797, Bloco II, 6º andar – Morumbi – CEP: 04794-000	11 5503-1011	www.commlogik.com.br	✓	✓	✓			
Computer Consulting Projeto e Consultoria Ltda.	São Paulo	Rua Caramuru, 417, Cj. 23 – Saúde – CEP: 04138-001	11 5071-7988	www.computerconsulting.com.br	✓	✓	✓			
Consist Consultoria, Sistemas e Representações Ltda.	São Paulo	Av. das Nações Unidas, 20.727 – CEP: 04795-100	11 5693-7210	www.consist.com.br	✓	✓	✓			
Domínio Tecnologia	São Paulo	Rua das Carnaubeiras, 98 – Metrô Conceição – CEP: 04343-080	11 5017-0040	www.dominiotecnologia.com.br	✓		✓			
Ética Tecnologia	São Paulo	Rua Nova York, 945 – Brooklin – CEP: 04560-002	11 5093-3025	www.ethica.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	✓	✓	✓			
Komputer Informática	São Paulo	Av. João Pedro Cardoso, 39 2º andar – Cep.: 04335-000	11 5034-4191	www.komputer.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		✓	✓			
Locaweb	São Paulo	Av. Pres. Juscelino Kubitschek, 1.830 – Torre 4 Vila Nova Conceição – CEP: 04543-900	11 3544-0500	www.locaweb.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	✓	✓	✓			
Savant Tecnologia	São Paulo	Av. Brig. Luis Antonio, 2344 cj 13 – Jd. Paulista – CEP: 01402-000	11 2925-8724	www.savant.com.br	✓	✓	✓			
Simples Consultoria	São Paulo	Rua Mourato Coelho, 299, Cj. 02 Pinheiros – CEP: 05417-010	11 3898-2121	www.simplescopytoria.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	✓	✓	✓			
Sybase Brasil	São Paulo	Av. Juscelino Kubitschek, 510, 9º andar Itaim Bibi – CEP: 04543-000	11 3046-7388	www.sybase.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		✓	✓			
Webnow	São Paulo	Av. Nações Unidas, 12.995, 10º andar, Ed. Plaza Centenário – Chácara Itaim – CEP: 04578-000	11 5503-6510	www.webnow.com.br	✓	✓	✓			
WRL Informática Ltda.	São Paulo	Rua Santa Ifigênia, 211/213, Box 02–Centro – CEP: 01207-001	11 3362-1334	www.wrl.com.br	✓	✓	✓			
Systech	Taquaritinga	Rua São José, 1126 – Centro – Caixa Postal 71 – CEP: 15.900-000	16 3252-7308	www.systech-ltd.com.br	✓	✓	✓			

Calendário de eventos

Evento	Data	Local	Informações
Campus Party	17 a 23 de janeiro	São Paulo, SP	www.campus-party.com.br/
V Workshop de Tecnologia Adaptativa – WTA 2011	31 de Janeiro	São Paulo, SP	www.poli.usp.br/
CNASI – Congresso de Auditoria de TI, Segurança da Informação e Governança	28 de março	Brasília, DF	www.cnasi.com.br/
Seminário de Cloud Computing	13 de abril	São Paulo, SP	www.ideti.com.br/cloud/
8º CONTECSI	1 a 3 de junho	São Paulo, SP	http://www.tecsifea.usp.br/eventos/contecsi/

Índice de anunciantes

Empresa	Pág.
Rede Host	02
Central Server	07
Globo.com	08
Uol Host	11
WatchGuard	13
Impacta	19
Vectory	21
Unodata	23
LPI	31
F13	55
Bull	83
Sony	84



Nerdson – Os quadrinhos mensais da Linux Magazine

Nerdson não vai à escola



creative commons
nerdson.com

FIGURAS LENDÁRIAS DA INTERNET

Luke Skywalker decidiu fazer um curso de computação em uma universidade pública...

NESTA DISCIPLINA,
USAREMOS O WINDOWS E
CRIAREMOS PROGR...

"VOCÊ ENSINARÁ
COM SOFTWAREES
LIVRES."

...ER... NÃO, NA
VERDADE USAREMOS
O DEBIAN...

"E USARÁ
A FORÇA".

...E VAMOS SUBMETER
PATCHES PARA ALGUM
PROJETO LIVRE,
VALENDO NOTA!

...e foi um padawan feliz.

creative commons
nerdson.com

EXTENDVOIP p.22
Uma história de sucesso na implantação da solução.

MOBILIDADE COM ECONOMIA p.10
Ampla gama de soluções de tecnologia em comunicações.



LINUX MAGAZINE

#4 Setembro 2010

AL ESPECIAL
ESPECIAL
SPECIAL AL ESPECIAL
ESPECIAL

VoIP

A TECNOLOGIA QUE
REVOLUCIONOU O MERCADO
DAS TELECOMUNICAÇÕES

Panorama do mercado, os melhores fornecedores, artigos e tutoriais completos para quem deseja montar, gerenciar e economizar com seu próprio PABX Asterisk.



LINUX NEW MEDIA
LME #4
R\$ 14,90
€ 6,50
00004
9 77980 463000
Barcode
QR code

TELEFONIA OPENSOURCE DO FUTURO p.58

Aprenda a utilizar o FreeSWITCH para criação de centrais PABX.

ASTERISK DESCOMPLICADO p.62

Monte instâncias de um PABX Asterisk independente do sistema operacional.

EM SINTONIA p.68

Utilize o Skype em servidores de telefonia livre Asterisk.

CENTRAL TELEFÔNICA INTELIGENTE p.47

Entenda o funcionamento do plano de discagem.

WWW.LINUXMAGAZINE.COM.BR

LINUX MAGAZINE ESPECIAL VOIP

Panorama do mercado, os melhores fornecedores, artigos e tutoriais completos para quem deseja montar, gerenciar e economizar com seu próprio PABX Asterisk.

Asterisk
FreeSWITCH
PABX
Wireshark
Skype
Wondershaper
Webhtb
Opensips

A tecnologia que revolucionou o mercado das telecomunicações. Adquira o seu exemplar nas bancas de todo o país ou pelo site da Linux Magazine.

Linux Magazine #75

PREVIEW



Android

Já conhecido como um dos sistemas operacionais para dispositivos móveis mais promissores dos últimos tempos, o Android agrada até ao gosto do mais exigente dos usuários. Flexibilidade, robustez, leveza e é claro, facilidade no desenvolvimento de aplicativos, estão entre suas principais características. ■

VoIP com Asterisk – parte IV

Confira na próxima edição, a quarta parte do super tutorial de Asterisk, abordando ramificações no plano de discagem, cálculos e operações sobre texto. ■

Ubuntu User #21



Organização de imagens

Aplicativo de respostas rápidas e recursos incomuns, o Geeqie é uma pérola entre os softwares de exibição e organização de imagens. ●●●

Organize-se!

Gerencie de forma eficiente seus emails, tarefas diárias, ligações telefônicas e muito mais, com o ThinkingRock, ferramenta imprescindível nos dia atribulados de hoje. ●●●

Jogo: Eschalon

Conheça o divertido e inteligente RPG medieval Eschalon Book II. ●●●

Virtual Shore™



Bull Brasil
50 ANOS

A Revolução em Desenvolvimento Colaborativo

A Bull, pioneira em "Fábricas de Software", lança o "Virtual Shore™", nova modalidade de desenvolvimento de sistemas que associa a capacidade de industrialização de Centros de Serviços à flexibilidade dos ambientes colaborativos e à riqueza do Software Livre de Código Aberto.

Saiba mais sobre o Virtual Shore em www.bull.com

BULL
Architect of an Open World™

SONY
make.believe



MAIS FINO E MAIS LEVE • 160 GB • BLU-RAY, DVD E CD • WI-FI
ADESÃO GRATUITA À PLAYSTATION® NETWORK • SAÍDA HDMI



ENCONTRE UMA INFINIDADE DE JOGOS PARA PLAYSTATION 3 COM OS DISTRIBUIDORES DA SONY. É A MANEIRA MAIS CONFIÁVEL DE COMPRAR E A QUE OFERECE MAIS VARIEDADE PARA VOCÊ. ISSO SIGNIFICA MUITO MAIS CONFIABILIDADE, SUPORTE E UM ANO DE GARANTIA COM ASSISTÊNCIA TÉCNICA QUE SÓ QUEM É OFICIAL PODE OFERECER.

Distribuidor oficial:



11 3546.4310

www.techdata.com.br

playstation@techdata.com.br



Sony "make.believe" é uma marca comercial registrada pela Sony Corporation. "PlayStation", o logotipo da família "PS", God of War, Heavy Rain, Modnation, Gran Turismo e Uncharted são marcas registradas pela Sony Computer Entertainment. Devido a diferenças de fabricação, alguns discos ópticos podem não funcionar corretamente. Alguns recursos ou serviços podem exigir taxas adicionais. O usuário é responsável por todas as tarifas de internet aplicáveis. A saída de vídeo em HD requer cabos e uma tela ou monitor compatível com HD, ambos vendidos separadamente. Cabo HDMI não incluído. Se um dispositivo que não for compatível com o padrão HDCP (Proteção de Conteúdo Digital de Alta Largura de Banda) for conectado ao sistema usando um cabo HDMI, o sistema não poderá reproduzir vídeo nem áudio. Produtos vendidos separadamente.