

**HACK AND BEER p.26**  
Maddog conta como foi o evento no Rio de Janeiro.

**TAURION p.28**  
Existem soluções para enfrentar o trânsito?

**WAYLAND p.14**  
Adeus ao XServer. Você está preparado?

# 73 Dezembro 2010



# sistemas de **ARQUIVOS** DISTRIBUÍDOS

NO CLUSTER, NA NUVEM OU EM REDES CORPORATIVAS, OS SISTEMAS DE ARQUIVOS DISTRIBUÍDOS RESOLVEM SEUS PROBLEMAS DE INFRAESTRUTURA **p.29**

- » KosmosFS: Hadoop e GoogleFS combinados **p.30**
- » Cluster compartilhado com OCFS2 **p.35**
- » O clássico NFSv4 e suas funções de segurança **p.42**
- » Segurança e escalabilidade com OpenAFS **p.49**

## TUTORIAL: SPACEWALK **p.56**

Elimine o trabalho pesado do gerenciamento de rede.

## SEGURANÇA: ECRYPTFS **p.68**

Criptografe seus dados com transparência e garanta proteção extra contra roubo de informações.

## VEJA TAMBÉM NESTA EDIÇÃO:

- » Icinga: o Nagios renasce **p.72**
- » VoIP com Asterisk – parte II **p.64**
- » Synergy, uma central de controle multiplataforma **p.54**

exemplar de  
**Assinante**  
venda proibida





## IDENTIDADE DIGITAL CAIXA - A SOLUÇÃO MAIS AVANÇADA EM SEGURANÇA NA INTERNET AO SEU ALCANCE.

A Identidade Digital CAIXA é o certificado digital ICP-Brasil emitido pela CAIXA. É um arquivo eletrônico que permite identificar as pessoas na internet. O uso do certificado digital confere validade jurídica aos documentos eletrônicos assinados digitalmente, além de garantir autenticidade das partes e confidencialidade nas trocas de mensagens e transações pela internet.

É o pioneirismo da CAIXA levando mais benefícios para toda a sociedade.

## 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, Udo Seidel,  
Thorsten Scherf, Cesar Taurion, Artur Moura,  
Eduardo Moura e Juliet Kemp.

### Tradução

Diana Ricci Aranha

### Revisão

Ana Carolina Hunger

### Editores internacionais

Ulli Bantle, Andreas Bohle, Jens-Christoph Brendel,  
Hans-Georg Eßer, Markus Feilner, Oliver Frommel,  
Marcel Hilzinger, Mathias Huber, Anika Kehler,  
Kristian Kißling, 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](http://www.linuxmagazine.com.br) – Brasil  
[www.linux-magazin.de](http://www.linux-magazin.de) – Alemanha  
[www.linux-magazine.com](http://www.linux-magazine.com) – Portal Mundial  
[www.linuxmagazine.com.au](http://www.linuxmagazine.com.au) – Austrália  
[www.linux-magazine.es](http://www.linux-magazine.es) – Espanha  
[www.linux-magazine.pl](http://www.linux-magazine.pl) – Polônia  
[www.linux-magazine.co.uk](http://www.linux-magazine.co.uk) – Reino Unido  
[www.linuxpromagazine.com](http://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 advenham de seu uso. A utilização de qualquer material da revista ocorre por conta e risco do leitor.

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

Linux é uma marca registrada de Linus Torvalds.

Linux Magazine é publicada mensalmente por:

Linux New Media do Brasil Editora Ltda.

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 - 2010:

Linux New Media do Brasil Editora Ltda.

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

### Atendimento Assinante

[www.linuxnewmedia.com.br/atendimento](http://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

# PNBL

Um dos maiores desafios para o Brasil atingir níveis de competitividade semelhantes aos de nações desenvolvidas ou (pelo menos) similares aos de países do BRIC – sigla usada para destacar os quatro países, que se destacaram no cenário mundial pelo rápido crescimento das suas economias em desenvolvimento: Brasil, Rússia, Índia e China – é a atualização de sua infraestrutura, em diversos níveis e segmentos. Segundo estudo realizado pelo Instituto de Logística e Supply Chain (ILOS), no final de 2009, o país dispunha de uma das piores infraestruturas de logística entre os países do grupo, Estados Unidos e Canadá. Outra questão crítica é a carga tributária nacional: de acordo com dados que fazem parte do levantamento “Carga Tributária no Mundo – Um comparativo Brasil versus BRICs”, apresentado em novembro do corrente ano pelo escritório de advocacia Machado-Meyer, o Brasil é o país que tem a maior carga tributária entre os BRICs. São 34% do Produto Interno Bruto, contra 23% da Rússia, 20% da China e 12,1% da Índia.

Enquanto uma (necessária) reforma tributária não vem, o governo nacional vem buscando minorar o atraso da infraestrutura na *terra brasilis* nos diversos segmentos em que a necessidade de avanços é premente, através de diversas iniciativas, entre as quais a mais importante é o alardeado Programa de Aceleração do Crescimento, ou PAC. Como este é um periódico que trata especificamente de tecnologia da informação, vale ressaltar entre as iniciativas para o setor, o Plano Nacional de Banda Larga (PNBL), especialmente em tempos de *Cloud Computing*.

É sabido que o processo de privatização das prestadoras de serviços de telecomunicação no país, enquanto necessário, acabou por gerar monopólios regionais. O Serviço Telefônico Fixo Comutado (STFC) foi disseminado com grande sucesso no país nas últimas duas décadas, mas a um custo exorbitante. Dois efeitos colaterais oriundos da concentração da oferta nas mãos de poucas operadoras são o (alto) custo e o (péssimo) alcance e qualidade da banda larga no país. No ranking de 159 países elaborado pela União Internacional de Telecomunicações (ITU), o País aparece em 60º lugar em acesso e em 87º em custos – entre outros desastres.

Em face do exposto acima, só podemos saudar a escolha de uma estatal – a renascida Telebras – como gestora do PNBL. Quando megacorporações internacionais insistem em entregar serviços de baixa qualidade e alto preço ao consumidor (corporativo e doméstico), é hora de um órgão regulador aparecer fazendo mais do que simplesmente definir regras, arreganhando as mangas e servindo de concorrência efetiva para os fornecedores de serviço de plantão.

O leitor talvez deva estar se perguntando quanto ao porquê deste editorial abordar esse tema, e aqui segue a resposta: Rogério Santanna dos Santos, ex-Secretário de Logística e Tecnologia da Informação do Ministério do Planejamento, designado para assumir a presidência da Telebras, declarou reiteradas vezes que o software proprietário só será usado pelo governo em duas situações: em sistemas legados e quando houver ganho tecnológico – caso contrário, a opção deverá ser pelo uso de Software Livre e de Código Aberto (SL/CA). Com isso, a necessidade de mão de obra qualificada em SL/CA deve aumentar – junto com o seu salário! Prepare-se. ■

Rafael Peregrino da Silva

Diretor de Redação



## CAPA

### Em busca do melhor

29

Para garantir tolerância à falhas, proteção e consistência dos dados e replicação segura – entre outros atributos –, a escolha do melhor sistema de arquivos distribuídos é imprescindível.

### O sistema que veio do Kosmos

30

Sistemas de arquivos distribuídos facilmente manipulam arquivos de tamanhos nas faixas dos gigabytes e terabytes. O sistema de arquivos Kosmos impressiona seus concorrentes.

### Cluster compartilhado

35

O OCFS2, que já está presente no kernel básico do Linux desde a versão 2.6.16 é anterior ao GFS2, sistema de arquivos mais popular. Apesar de, nos bastidores, o OCFS2 não ser trivial, ele é de fácil utilização.

### Armazenamento com segurança

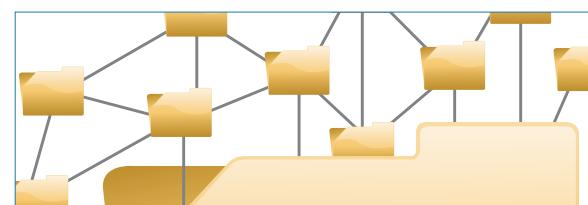
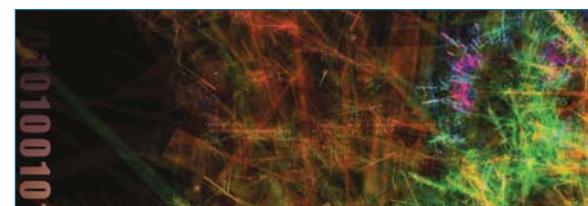
42

O NFS é o sistema de arquivos de rede clássico do Linux. Este artigo apresenta o NFSv4 e suas funções de segurança.

### Seguro e escalonável

49

Repleto de funções, o OpenAFS surpreende pela segurança e escalabilidade.



**COLUNAS**

<b>Klaus Knopper</b>	<b>08</b>
<b>Charly Kühnast</b>	<b>10</b>
<b>Zack Brown</b>	<b>12</b>
<b>Augusto Campos</b>	<b>14</b>
<b>Kurt Seifried</b>	<b>16</b>
<b>Alexandre Borges</b>	<b>20</b>

**NOTÍCIAS**

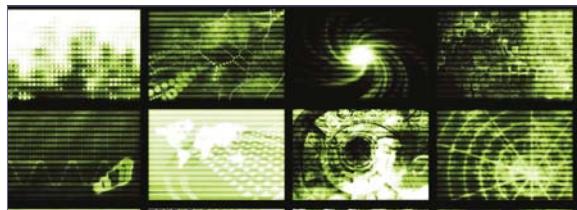
<b>Geral</b>	<b>22</b>
‣ Apple passa a contribuir com o projeto OpenJDK	
‣ Lançada atualização de segurança para o ProFTPD	
‣ Citrix lança nova versão do XenServer	
‣ Red Hat lança Red Hat Enterprise Linux 6, trazendo inovações	

**CORPORATE**

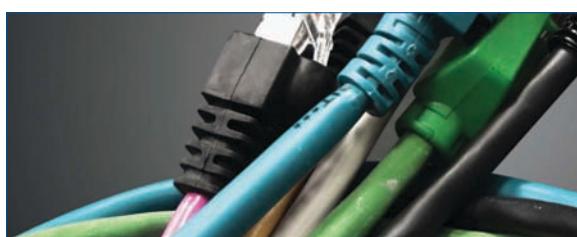
<b>Notícias</b>	<b>24</b>
‣ Intel anuncia novo diretor geral para América Latina	
‣ Lenovo do Brasil anuncia novo Diretor de Vendas	
‣ Nokia anuncia o fim da Fundação Symbian	
‣ Presidente da Microsoft vende 12% de sua participação na empresa	
‣ Citrix OpenCloud ganha prêmio	
<b>Coluna: Jon "maddog" Hall</b>	<b>24</b>
<b>Coluna: Cesar Taurion</b>	<b>26</b>

**ANÁLISE**

<b>Plataformas conectadas</b>	<b>54</b>
As muitas abordagens para gerenciar computadores remotamente incluem o VNC, o Nomachine e o SSH. O Synergy é uma ferramenta útil que conecta vários computadores para criar um ambiente de desktop virtual.	

**TUTORIAL**

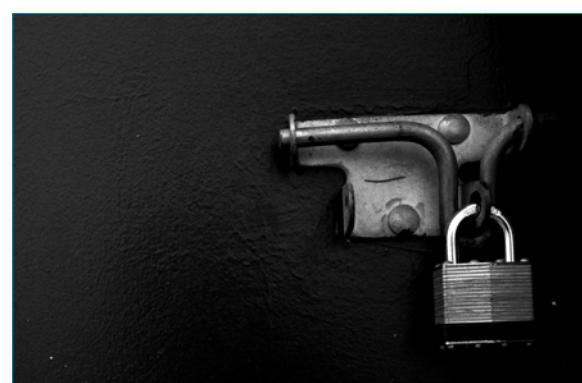
<b>Gerenciamento ágil</b>	<b>56</b>
Conforme sua rede cresce, o gerenciamento manual do sistema torna-se moroso e fica impraticável. Conheça o Spacewalk, uma ferramenta de código aberto que elimina o trabalho pesado do gerenciamento de rede.	

**VoIP com Asterisk – parte II****64**

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**

<b>Criptografia de arquivos e diretórios</b>	<b>68</b>
O eCryptfs criptografa seus dados com transparência, oferecendo uma proteção extra contra invasões e roubos de informações.	

**REDES**

<b>O observador</b>	<b>72</b>
Os desenvolvedores do Icinga se cansaram de esperar por atualizações da popular ferramenta de monitoramento de redes Nagios, e começaram o seu próprio e promissor projeto.	

**SERVIÇOS**

<b>Editorial</b>	<b>03</b>
<b>Emails</b>	<b>06</b>
<b>Linux.local</b>	<b>78</b>
<b>Preview</b>	<b>82</b>

Emails para o editor

# Permissão de Escrita

## Monitoramento já ☐

Gostaria de parabenizar a Linux Magazine pela iniciativa de publicar uma edição voltada para Monitoramento de Redes. Gostaria ainda de solicitar o aprofundamento e a publicação de mais matérias sobre o assunto, pois é muito escasso o material disponível com este nível de qualidade.

Como sugestão, gostaria de registrar a ideia de a Linux Magazine disponibilizar suas matérias em vídeos. Obrigado e continuem com o ótimo trabalho!

Edilson Souza

## Resposta

Caro Edilson, agradecemos os elogios. Certamente continuaremos a publicar conteúdo voltado para a área de monitoramento de redes e segurança da informação em geral. Ficamos felizes que tenha gostado.

Sobre disponibilizar as matérias em vídeos, é uma ideia interessante e que iremos analisar!



## Escreva para nós! ☐

Sempre queremos sua opinião sobre a Linux Magazine e nossos artigos. Envie seus emails para [cartas@linuxmagazine.com.br](mailto: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.

## Open Web Services Manager ☐

Olá pessoal!

Gostaria de ver na Linux Magazine, alguma matéria sobre Open Web Services Manager – [openwsman](#) – e como utilizá-lo para interação com o Microsoft Windows. Um abraço a toda equipe!

Miguel Penteado

## Resposta

Miguel, em primeiro lugar, obrigada por seu email!

O Open Web Services Manager é um tema que pretendemos abordar em breve, pois o gerenciamento remoto de computadores é um assunto atraente e interessante para diversos administradores de sistema. Agradecemos pela sugestão!



**Este espaço que está  
sobrando custou dinheiro.**

**É exatamente isso que você faz  
com os servidores da sua empresa:  
paga pelo que não usa.**

Com o **Cloud Server Pro** é diferente.  
O tamanho de sua demanda determina  
exatamente quanto você vai gastar.  
É a evolução do Cloud Computing, com muito  
mais economia, performance e segurança.  
Aumente a inteligência do seu ambiente de TI.



*Para saber mais, acesse:  
[Locaweb.com.br/CloudServerPro](http://Locaweb.com.br/CloudServerPro)*



*Coluna do Klaus*

# Pergunte ao Klaus

*Inicialização do Knoppix em uma unidade removível e problemas com o Compiz no Ubuntu são as dúvidas deste mês.*

## Configurações do Compiz

Meu computador doméstico usa o Ubuntu 10.04.1 LTS, mas quando utilizo as configurações padrão do Knoppix 6.2, não consigo que o Compiz funcione a contento. Por exemplo, o modo em que o menu Startup se mexe quando é aberto não acontece no Ubuntu. Muitas configurações do padrão do Ubuntu acabam voltando, sem manter as alterações.

Como tenho o Knoppix em Live CD, posso executá-lo no meu hardware e, então, o Compiz funciona bem. Isso me diz que o hardware não é o problema, mas sim as configurações do Ubuntu. Agora percebo que esse é um problema do Ubuntu, mas você teria alguma explicação para essa questão da configuração do Compiz?

Bob Wooden.

### Resposta

O Compiz guarda sua configuração em `.config/compiz/compizconfig`, mas também suporta o estilo *Gnome gconf* de configuração e perfis para seleção automática. Com a sua descrição, não sei dizer o que está acontecendo de errado quando o Compiz perde as configurações na sua distribuição, mas uma verificação no diretório mencionado acima, antes e depois de reiniciada uma sessão, pode ajudar.

No pior dos casos, um script que restaura sua configuração customizada antes da inicialização do ambiente gráfico pode ser usado para resolver a questão. Apenas para testar configurações modificadas, reinicie o Compiz com `compiz --replace`. O gerenciador de configuração do Compiz deve fazer isso automaticamente.

Diferentes versões do Compiz suportam diferentes opções em seus arquivos de configuração. Pode ser por isso que os arquivos de configuração de uma versão do Compiz do Knoppix não funcionam direito no Ubuntu, mas elas podem ser encontradas através do `compizconfig` em um local diferente.

## Problemas com Bootloader

Instalei o Knoppix 6.3 em um drive USB sem problemas, mas minha instalação no disco rígido não inicializa. A instalação é bem sucedida, porém o problema parece ser no GRUB. Agradeço seus conselhos. Antonio.

### Resposta

Se a instalação correu bem, a única coisa que está faltando é o *bootloader*, que reside nos primeiros bytes (no *Master Boot Record – MBR*) do seu disco rígido.

O computador normalmente possui uma sequência de busca programada na BIOS, que pode ser alterada através do painel de configurações. Depois da instalação no disco rígido, este precisa ser configurado para ser a primeira mídia a ser pesquisada e deve conter a mídia de inicialização, ou será preciso excluir toda a mídia removível que poderia interferir na inicialização.

Para saber por que a inicialização via MBR não funciona, uma descrição mais detalhada do erro ajudaria bastante. O computador nem tenta inicializar pelo disco? Ou há alguma mensagem do GRUB indicando que há uma tentativa de carregar o kernel Linux que acaba travando e, consequentemente, o processo não continua? Confira a instalação do *bootloader* sem reinstalar o Knoppix. Initialize com o Live CD, monte a partição do sistema e execute mais uma vez a instalação do GRUB para o MBR:

```
mount /media/sda2
grub-install
--root=/media/sda2 /dev/sda
```

Se houver uma mensagem de erro indicando um mapeamento incorreto de dispositivo, edite o arquivo `/media/sda2/boot/grub/device` e remova tudo que não seja o disco de inicialização correto. ■

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

# 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](http://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



*Coluna do Charly*

# Log descomplicado

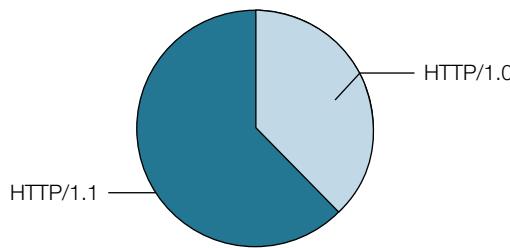
São tantos os arquivos de log analisados por um administrador de sistema, que é comum confundir-se. Charly apresenta a cura para isso: Lire.

**R**ecentemente, tive que avaliar arquivos de *log* em três servidores de email diferentes (*Exim*, *Postfix* e *Sendmail*), e percebi que estava constantemente confundindo os parâmetros de configuração das três ferramentas de avaliação na linha de comando.

Um alívio para o cérebro carcomido de um administrador que passa por problemas como os meus é o Lire [1], uma impressionante coleção de programas baseada em um pequeno número de comandos. Preciso de apenas um deles, o `lre_log2report`, para avaliar meus logs. Geralmente, uso dois parâmetros para isso. No seguinte exemplo de um log de servidor web: `lre_log2report combined /var/log/apache2/access.log` a opção `combined` informa ao programa qual formato de arquivo de log ele terá que encarar. Nesse caso, é o log estendido do servidor web Apache.

O segundo parâmetro fornece o caminho do log. Os resultados aparecem na linha de comando logo depois. Como alternativa, é possível pedir ao Lire que ele devolva seus resultados em formato HTML:

```
lre_log2report combined
/var/log/apache2/access.log
-o html /var/www/avalicao/
```



**Figura 1** O Lire pode analisar o protocolo HTTP usado pelos clientes. HTTP 1.0 indica que os clientes estão usando um proxy.

Os resultados da avaliação são enviados para o caminho que vem após o parâmetro `-o html`. Além das avaliações típicas, o Lire pode fornecer melhores detalhes sobre pontos específicos. Por exemplo, é possível analisar o protocolo HTTP usado por seus clientes (figura 1).

A ferramenta pode ainda, avaliar com que frequência os *web bots* e *web spiders* visitaram seu servidor.

## Panorama

As opções de avaliação são tão amplas, que é possível ainda utilizar o seguinte comando: `lre_log2report --help dlf converters`. Sua saída é uma lista de todos os formatos que o Lire pode interpretar. São quase quarenta e incluem protocolos de seis servidores de email, várias versões do servidor de nomes BIND e tinydns, Snort, Apache, MySQL e PostgreSQL, SpamAssassin e Squid.

O Lire também é flexível com os formatos de saída: além do texto simples e HTML, ele devolverá dados no formato PDF e até mesmo utilizará o formato de planilhas XLS da Microsoft.

O software dá aos administradores uma ampla gama de opções de customização. A documentação [2] é bem abrangente e cheia de exemplos. ■

## Mais informações

[1] Lire: <http://logreport.org/>

[2] Manual do Lire: <http://download.logreport.org/pub/current/doc/user-manual.pdf>

**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.

Gerencie o seu servidor  
Linux

A PARTIR DE  
**59, 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](http://www.centralserver.com.br)





*Coluna do Zack*

# Crônicas do kernel

O cronista Zack Brown relata as últimas novidades, visões, dilemas e desenvolvimentos na comunidade kernel do Linux.

**A**ndi Kleen apresentou um patch de correção para converter a opção `CONFIG_SYSFS_DEPRECATED` em uma seleção *runtime* que poderia ser feita na linha de comando do kernel. Basicamente, é possível inicializar o mesmo kernel no moderno SysFS ou na versão mais antiga que está sendo substituída gradualmente. Isso só é útil para pessoas que precisam manter os sistemas抗igos em funcionamento, como Andi faz.

Greg Kroah-Hartman aceitou o patch, por isso parece que este será realmente incluído no kernel. Estou um pouco surpreso, porque essa é uma necessidade muito específica; eu imaginei que Greg ou Linus dissessem para Andi apenas aplicar os procedimentos executados pelo patch manualmente para uso em seu próprio kernel. Por outro lado, isso não parece importar muito, porque o código antigo será removido em algum momento, e o patch extra do Andi será removido junto com ele.

## Repositório Git para patches

James Bottomley anunciou a criação de um novo repositório Git de patches para código de armazenamento, incluindo SCSI, ATA, dispositivos de bloco etc. Ele

estava disposto a acrescentar VFS e sistemas de arquivos também, se os usuários assim o quisessem. Dave Chinner reclamou que o repositório de James, sendo uma árvore mesclada feita nas horas extras, seria muito chata de usar. Ele disse, “se eu gostasse da dor de rebasear árvores mescladas descartáveis todos os dias, então eu já estaria usando `linux-next`”.

James respondeu: “Para ser honesto, isso é o que as pessoas queriam quando a questão foi levantada na LSF10. No entanto, ao contrário da rede, o armazenamento nunca teve um único mantenedor, por isso é um pouco mais político do que fazer isso por decreto; e mais, nem todos os mantenedores atuais de árvores de armazenamento estavam lá. Então, concordamos (relutantemente) em iniciar com uma árvore automática e ver quanto do problema atual foi resolvido. Se a árvore automática acabar por não ser muito útil, podemos revisitá-la e ideia de um mantenedor de armazenamento.” James também ressaltou que uma das razões a favor de uma árvore de armazenamento separada, ao invés de apenas utilizar `linux-next`, era que o `linux-next` era muito maior e, portanto, mais difícil de seguir. Uma árvore de armazenamento separada seria pequena, elegante, e todos os patches atualmente na árvore tinham menos de um único megabyte.

Dave bateu o pé, dizendo que razões de ordem técnica, não política, devem determinar o curso apropriado de ação. Ele disse: “Uma árvore de manutenção de armazenamento não poderia substituir o pequeno feudo de ninguém, o que precisamos é de um ponto de integração muito antes das coisas chegarem até o Linus...”.

James disse que política era inevitável. Os mantenedores de armazenamento atuais tinham uma certa

**Dave Chinner reclamou que o repositório de James, sendo uma árvore mesclada feita nas horas extras, seria muito chata de usar.**

linha direta com Linus Torvalds. Colocar essa nova árvore Git entre eles e Linus alteraria substancialmente a relação. Como não houve consenso entre os mantenedores (porque não foram todos à reunião), James explicou que o único caminho a seguir era o de demonstrar que a nova árvore Git seria melhor do que o sistema atual. Uma construção automática foi um pouco menos intrusiva do que ter um mantenedor humano separado para a nova árvore, por isso, eles decidiram tentar agir desta forma primeiro para ver o que seria resolvido.

Não houve uma discussão mais aprofundada, mas claramente não houve consenso.

## Status do BKL

O BKL – *The Big Kernel Lock* – vem morrendo há anos, e ainda está morrendo. Ele ainda está na árvore oficial do kernel em muitos lugares, mas a árvore do [Linux-next](#) quase o eliminou por completo. Arnd Bergmann postou recentemente uma lista das partes restantes do kernel que precisavam dele – alguns pontos do sistema de arquivos, um par de elementos de rede, e dois drivers. Isso posto, menos de 20 pontos ainda precisam ser corrigidos.

A maioria dos problemas remanescentes existe em código antigo sem mantenedores, e não está claro quem mais poderia estar bem familiarizado com essas partes do kernel para fazer a transição em segurança do BKL para algum outro mecanismo de travamento. Mas, em outros casos, há trabalhos anti-BKL ativos acontecendo.

Após o anúncio de Arnd, várias pessoas se ofereceram para tomar conta de diversos itens; mas alguns ainda serão não-triviais. Arnd acrescentou ainda uma entrada *Config BKL* para o sistema de configuração do kernel, para que os usuários sejam capazes de construir um kernel totalmente não-BKL apenas por exclusão de partes diferentes de código que ainda dependem dele. A ideia é que isso irá ajudar a destacar os retardatários restantes e fazer com que os desenvolvedores trabalhem para eliminá-los. Atualmente, o código de bloqueio de arquivo do kernel ainda depende do BKL. Assim, até que isso seja consertado, a opção *Config BKL* sempre precisará ser selecionada. Quando isso mudar, haverá muita gente testando kernels inteiramente sem BKL.

## Suporte GCC

De vez em quando, as pessoas começarem a especular sobre quais versões do GCC ainda são capazes de compilar o kernel e quais devem continuar a ser suportadas e porquê. A discussão pode ficar muito envolvente. Dessa

vez, Florian Mickler postou um patch para o *MAKEFILE*, alertando os usuários para o fato de que o GCC versão 3.3.3 estava com problemas, e a versão 3.4 era a única que ainda compilava o kernel.

No entanto, Peter Zijlstra parecia lembrar que até a versão 3.4 não estava lá essas coisas, com relação ao kernel. H. Peter Anvin respondeu que o GCC 3.4 realmente ainda compilava o kernel, mas que era extremamente difícil e tedioso se certificar de que isso continua a ser o caso para cada nova versão do kernel; ele realmente desejava que as pessoas concordassem em deixar essa versão do compilador e passassem a utilizar o GCC 4.x.

H. Peter também identificou vários problemas fascinantes com a compatibilidade do compilador. Ele disse que algumas distribuições Linux vêm com uma versão do GCC 3.3.3, que continha várias correções vindas do GCC 3.4. Isso significava que qualquer patch alertando para os males do GCC 3.3.3 apenas confundia os usuários dessas distribuições, porque a versão 3.3.3 funcionava muito bem lá.

*A maioria das pessoas que trabalha em sistemas embarcados depende do GCC 3.4, então ainda é importante oferecer suporte a essa versão, apesar da dificuldade cada vez maior para fazê-lo.*

Ele também destacou que a maioria das pessoas que trabalha em sistemas embarcados depende do GCC 3.4, então ainda é importante oferecer suporte a essa versão, apesar da dificuldade cada vez maior em fazê-lo.

Russell King mencionou que usou o GCC 3.4 para compilar o kernel em arquiteturas ARM. Disse também que a versão 3.4.3 foi notavelmente mais rápida que o compilador 4.3.2, não só na arquitetura ARM, mas em hardware x86 também. H. Peter confirmou que não havia propostas ativas para parar de oferecer suporte ao GCC 3.4 até o momento. ■

---

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 extraír significado! Sua newsletter Kernel Traffic esteve em atividade de 1999 a 2005.

---



Coluna do Augusto

# Wayland: futuro das interfaces gráficas?

O X11 domina as interfaces gráficas do Unix e de seus derivados desde a década de 1980, estando presente em cada uma das gerações destes produtos.

Muitos usuários “clássicos” de Linux devem se lembrar das muitas horas gastas editando o arquivo de configuração [XF86Config](#) até conseguir alcançar a resolução desejada da tela, o suporte correto ao mouse, teclado e outros detalhes.

O X [\[1\]](#) evoluiu bastante nos últimos anos, juntamente com as tecnologias de identificação e configuração de hardware, a ponto de hoje ser rara a necessidade de edição manual de seus arquivos de configuração nos desktops mais comuns. Mas trata-se de uma evolução que em grande parte acontece acrescentando camadas mais modernas sobre fundamentos que foram planejados e inicialmente implementados há mais de 20 anos, quando os requisitos eram outros, e alguns recursos hoje disponíveis nos desktops mais comuns não eram sequer imaginados.

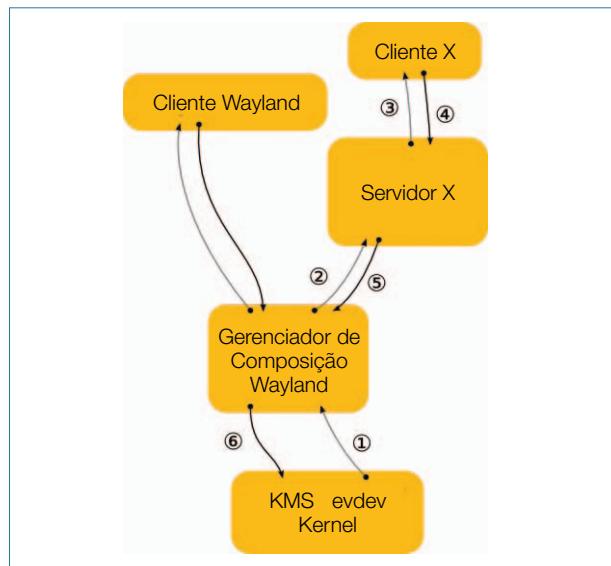
Essa preservação dos fundamentos é ótima para manter a compatibilidade, e boa parte dos requisitos originais do X têm tanto valor hoje como no passado,

especialmente nos ambientes para os quais ele foi inicialmente planejado – e desenvolvedores, administradores de redes e usuários avançados sabem tirar proveito de suas características menos óbvias.

Mas a tecnologia avança, e em 2008 foi apresentado o Wayland, um novo servidor de exibição gráfica criado como uma alternativa ao venerado X11, mas fazendo uso de tecnologias atuais disponíveis no kernel Linux, como o DRM – Direct Rendering Manager e o GEM – Graphics Execution Manager para aumentar o desempenho e a precisão. Seu desenvolvimento vem sendo constante desde então, e suas vantagens visíveis motivaram os responsáveis por distribuições como Ubuntu, Fedora e MeeGo a anunciar, em novembro, seus planos de adotar o Wayland como um sucessor para o X11.

Trata-se de um plano a médio prazo, pois o Wayland ainda não tem a maturidade necessária para sustentar esse papel – e mesmo após entrar em vigor, o X11 ainda estará presente para garantir a compatibilidade dos aplicativos que não forem portados, mais ou menos como ocorre com o Mac OS X. Confira na [figura 1](#), como funciona o Wayland.

Mas se você desenvolve para Linux ou atua “debaixo do capô” de seu desktop, vale a pena se adiantar. No site do projeto [\[2\]](#) você já encontra as informações técnicas necessárias para começar! ■



**Figura 1** Funcionamento do Wayland.

## Mais informações

[1] Site oficial do X.org: <http://www.x.org/>

[2] Site oficial do Wayland  
<http://wayland.freedesktop.org/>

**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.

# Programa de Afiliados

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

"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

BORGHIERI/LOWE



**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 Kurt*

# Mais código, mais problemas

*Os plugins proporcionam muitos recursos, mas, dependendo de sua qualidade, podem proporcionar também questões indesejadas de segurança.*

O software de código aberto está sempre me surpreendendo. De tudo que já vi, nada pode ser modificado, moldado, estendido e melhorado com tanta facilidade. Com tantos programas que suportam plugins e extensões externas, esse processo foi ainda mais facilitado. Alguns exemplos incluem o Firefox, o TYPO3, o WordPress e, logicamente, o kernel Linux.

Então, por que os plugins (extensões, módulos etc.) são uma coisa tão legal? Os plugins permitem experimentar novas ideias e conceitos em qualquer software sem a necessidade de concordância ou cooperação com o projeto principal (basta usá-los). Algumas vezes, por motivos técnicos, legais, de marketing ou políticos, os projetos de software não oferecem ou não conseguem oferecer certos recursos (como por exemplo, o Firefox e o plugin AdBlockPlus).

Além disso, em projetos como o TYPO3 e o WordPress, que oferecem sistemas de gerenciamento de conteúdo (CMS – Content Management System) e capacidades de publicação em blogs (basicamente uma vertente do CMS), o código fonte chegaria a um tamanho absurdo caso cada recurso que as pessoas quisessem fosse incluído (o Wordpress possuía 11.213 plugins até setembro de 2010; o Firefox tem no momento mais de 13.000, número que continua aumentando).

## Por que se preocupar?

Os plugins quase sempre são executados dentro do contexto seguro e do nível de privilégio do aplicativo ao qual estão conectados. Isso significa que um plugin para Firefox (assumindo-se que o Firefox seja executado com sua conta) irá ter acesso a todos os seus arquivos.

O plugin também pode interagir com sua sessão de login, executar processos em segundo plano e fazer praticamente qualquer coisa que sua conta tenha a permissão de fazer, tal como editar o `crontab` ou `.profile` de sua máquina para executar scripts e códigos arbitrários, mesmo quando você não está conectado.

Isso de fato aconteceu em 2008; um plugin do Firefox chamado *Basic Example Plugin for Mozilla* espalhou o trojan [Trojan.PWS.ChromeInject.A](#) para roubar senhas de usuários e detalhes de contas [1]. Mesmo quando não são intencionalmente maliciosos, a dura verdade é que a qualidade do código dos plugins geralmente deixa à desejar se comparada à do projeto principal.

Grandes projetos como o Firefox, TYPO3 e WordPress chamam muita atenção e suporte; em alguns casos, possuem equipes de segurança dedicadas que estão continuamente auditando o código e o trabalho para resolver problemas de segurança com rapidez. Grandes empresas de segurança também têm muito interesse em encontrar falhas nesses programas, pois seus clientes os utilizam. Felizmente, a maioria dessas empresas trabalha para garantir que questões de segurança sejam tratadas de modo a causar pouquíssimo incômodo ao usuário final. Mas projetos de plugins raramente têm esses recursos, pois normalmente um único autor cria e lança o código publicamente.

## TYPO3

O TYPO3 suporta extensões que vão desde plugins de calendários até envio de email, um ótimo editor de texto e vários pacotes de software de fóruns, só para citar alguns exemplos. O cerne do TYPO3 consiste de mais de 6.000 arquivos, dos quais 1.200 mais ou menos são arquivos PHP. Em 2009 (como 2010 ainda não acabou, vou usar o ano passado), houve 21 avisos de segurança com 113 questões a serem resolvidas. Dessa questão, apenas 16 estavam no código do TYPO3 [2]; as outras 97 eram de suas extensões.

Esse número não é tão ruim quanto parece. De acordo com a página de repositório de extensões do TYPO3, o décimo plugin mais popular foi baixado 317 vezes para a versão corrente, o que quer dizer que a maioria dos plugins do TYPO3 foi baixada menos de 300 vezes (logicamente, um plugin pode ser baixado uma só vez e



# 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](http://www.sodic.com.br/canais)

### Consulte políticas especiais:

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

instalado em vários lugares, mas acredito que esses números sejam representativos).

De acordo com os números do *Common Vulnerabilities and Exposures* (CVE – Exposições e Vulnerabilidades Comuns) dos últimos anos, o código do TYPO3 possuía 20 vulnerabilidades e várias de suas extensões possuíam 235 – uma relação aproximadamente parecida com os números de 2009. A mesma história ocorre com o Firefox, o WordPress e praticamente todos os outros softwares que suportam plugins e extensões.

## O kernel Linux

Outro bom exemplo do uso de plugins (ou, nesse caso, módulos) é o kernel Linux. Na maior parte dos sistemas que executam um kernel modificado pelo fabricante, haverá mais de 1.000 módulos (cito como exemplo o CentOS 5.4 que possui 1.251). O tamanho total desses módulos é 96MB, o que quer dizer que seu kernel iria de 2MB para 98MB (sua partição /boot precisaria ter 1 ou 2GB). Para se proteger dos módulos exclusivamente binários, os desenvolvedores do kernel Linux implementaram um sistema que marca o kernel como “maculado” se há um módulo carregado que não possui licença de código aberto. Devido ao fato de o kernel Linux utilizar módulos para a maioria das funções secundárias, é relativamente rápido e fácil atualizar o sistema sem uma reinicialização.

## Soluções em curto prazo

Várias soluções a curto e longo prazo estão disponíveis para lidar com vulnerabilidades. A solução em curto prazo mais óbvia é a redução da área de ataque. O Firefox é um ótimo exemplo disso, pois vários aplicativos silenciosamente instalam plugins (Java, Skype etc.) possivelmente desconhecidos. Extensões bem comportadas como o NoScript ou o AdBlock Plus oferecem a opção de desinstalação; outras menos comportadas como o Java Console não possuem a opção de desinstalação mas normalmente possuem a opção de desativação.

Extensões sem as opções de desinstalar ou desativar, no geral, devem ser evitadas. Mas ao menos no Linux, se há uma extensão rebelde, é possível removê-la manualmente, no diretório `~/.mozilla/firefox/`, entrando em seu diretório pessoal padrão (ele possui um nome aleatório para prevenir que os invasores incluam arquivos nele) e excluindo os diretórios das extensões não desejadas [3].

O único problema é saber qual diretório pertence a qual extensão; elas usam um GUID (uma string muito longa e, esperamos, única) como nome do diretório, tal como essa: `ec8030f7-c20a-464f-9b0e-13a3a9e97384` portanto, vai ser preciso usar um mecanismo de busca de sua escolha para descobrir quais diretórios pertencem a quais plugins. Os mesmos problemas se aplicam a

aplicativos web. A maioria dos plugins e extensões são normalmente bem comportadas, mas, caso contrário, será preciso excluir os arquivos manualmente.

Nem sempre é possível remover plugins que representam ameaça, por isso é preciso executar outras ações para garantir que os plugins baixados são os melhores possíveis. A primeira coisa a se considerar é a idade: de quando é a última versão e qual é a frequência delas? Plugins velhos são normalmente mais perigosos; ajustes de segurança levam algum tempo, se é que eles são atualizados. Além disso, verifique o site do projeto. Se o plugin ou extensão possui um site decente, com informações de contato, isso pode indicar sua qualidade (dica: a falta de informação de contato é um mau sinal).

## Soluções em longo prazo

Uma das melhores soluções em longo prazo (potencialmente) é um projeto relacionado ao WordPress. O WordPress anunciou que iria separar os plugins em dois campos: os plugins “centrais” e o resto. Os plugins centrais seriam os mais populares, que todo mundo usa e, portanto, os que fornecem maior exposição a ataques. Esses plugins centrais (assim se espera) seriam auditados e integrados ao WordPress, resultando em maior qualidade de código e uma instalação e gerenciamento mais fáceis. Infelizmente, parece que não aconteceu muita coisa nesse projeto (suspeito que este seja um caso clássico de “está bom o suficiente”, o que sufoca o esforço em busca de melhorias).

## Conclusão

Plugins e extensões vieram para ficar. Infelizmente, a qualidade do código de muitos deles varia de regular a terrível. Meu conselho é não usar qualquer plugin que não possui atualizações regulares ou não se comporta bem. Por outro lado, certos plugins como o NoScript, o FlashBlock e o AdBlock Plus podem melhorar significativamente a segurança do seu sistema. ■

### Mais informações

- [1] Plugins maliciosos do Firefox: <http://blog.mozilla.com/security/2008/12/08/malicious-firefox-plugin/>
- [2] Segurança TYPO3: <http://typo3.org/teams/security/security-bulletins/>
- [3] Desinstalação de extensões: [http://kb.mozilla.org/Uninstalling\\_extensions/](http://kb.mozilla.org/Uninstalling_extensions/)

---

**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.

---



# 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](http://www.LinuxMagazine.com.br)





*Coluna do Alexandre*

# O valor das coisas simples

*Comandos utilizados diariamente, se bem explorados, podem resolver muitos problemas do dia a dia.*

O dia a dia, por muitas vezes, nos impede de encontrar tempo suficiente para aprender comandos e opções de comandos GNU/Linux e Unix de maneira completa e detalhada. Não faz muito tempo que um aluno questionou, em um treinamento que eu estava ministrando, se o uso do comando `tar` (tipicamente usado para realizar backups compactados) se resumia apenas ao clássicos `tar -cvf ...` ou `tar -xvf ...`, ou seja, criação e extração de arquivos dentro de um pacote `tar`.

Relembrando para criar um arquivo com todo o conteúdo do diretório `/etc`:

```
# mkdir /linuxmagazine ; cd /linuxmagazine
# tar -cvf etc.tar /etc
```

Se a sua intenção é a de fazer um backup em um dispositivo removível de algum diretório, utilize o comando `# tar -cvf /dev/st0 /etc`. Para extrair todos os arquivos de dentro deste backup, execute o comando `# tar -xvf etc.tar`.

Quando necessário, é possível extrair todo o conteúdo de um determinado arquivo `tar` em outro diretório, através do comando `# tar -xvf etc.tar -C /teste`. Para visualizar um arquivo específico dentro desse `tar`, é possível ainda utilizar o comando `# tar -tvf etc.tar`.

Caso a sua necessidade seja a de extrair apenas um único arquivo desse `tar`, execute o comando `# tar -xvf etc.tar etc/ntp.conf`. Para adicionar mais arquivos dentro de um `tar` já existente com `# tar -rvf etc.tar /boot/grub/menu.lst`.

Para incluir arquivos apenas se estes forem mais recentes do que os já existentes dentro de um arquivo `tar` (atualização), execute `# tar -uvf etc.tar /etc`.

É claro que o comando `tar` tem outras opções muito úteis e que podem nos auxiliar em tarefas simples, porém nem sempre usuais. Por exemplo, às vezes realizamos um backup usando o comando `tar` e temos a intenção de incluir quase todos os arquivos, contudo excluir alguns indesejáveis de modo a não ocupar espaço desnecessariamente. Isso poderá ser feito criando um arquivo de texto qualquer onde serão listados os arquivos que não queremos incluir no backup, como por exemplo:

```
# more /linuxmagazine/excl.txt
/etc/passwd
/etc/shadow
/etc/shadow-
/etc/timezone
```

Concluído o arquivo de texto, basta criar o backup de quase todos os arquivos do diretório `/etc`, todavia indicando que não queremos que sejam incluídos os arquivos listados no documento de texto, através do comando `# tar -cvf /linuxmagazine/etc.tar -X excl.txt /etc`.

Uma outra alternativa maravilhosa do `tar` é o seu uso para realizar backup incremental com o auxílio de um arquivo de `snapshot` que possui informações do último backup. Com esta possibilidade, podemos então realizar um backup completo e, depois de um certo tempo, fazendo deste arquivo de snapshot, realizar um backup incremental contendo apenas os arquivos que sofreram alteração desde o último backup (no nosso caso, um backup completo, que também poderia ser um outro backup incremental). No exemplo abaixo, usaremos a opção `-z` para fazer o backup de forma compactada:

(Backup completo):  
`# tar -zcvf /linuxmagazine/etc\_full.tar.gz -g /`  
`linuxmagazine/snapshot\_etc /etc`

(Backup incremental):  
`# tar -zcvf /linuxmagazine/etc\_incr.tar.gz -g /`  
`linuxmagazine/snapshot\_etc /etc`

Sabendo desses conceitos, fica mais fácil criar um backup diferencial, ou seja, um backup com todos os arquivos que sofreram modificação desde o último backup completo:

(Backup diferencial):  
`# find /etc -type f -newer /`  
`linuxmagazine/etc\_full.tar.gz`  
`-print0 | tar -null -zcvf /`  
`linuxmagazine/etc\_diff.tar.gz`  
`-T -`

A opção `-type -f` é necessária para incluir apenas arquivos no backup diferencial (sem isso, seriam incluídos arquivos e diretórios). A opção `-null` em conjunto com a opção `print0` inclui arquivos com espaço no nome. A opção `-T -` usa a saída do comando `find` para criar o arquivo `etc_diff.tar.gz`.

Como o leitor pode perceber, não é fascinante como comandos que utilizamos diariamente, se melhor explorados, podem nos oferecer mais resultados com eficiência? São estes detalhes que me incentivam a buscar soluções simples para pequenos problemas do nosso cotidiano. Até o mês que vem. ■

**Alexandre Borges** ([alex\\_sun@terra.com.br](mailto:alex_sun@terra.com.br), [twitter: @ale\\_sp\\_brazil](http://twitter.com/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.


**ESPECIAL**

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



**MOBILIDADE COM ECONOMIA p.10**  
Ampla 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 plano de discagem.

[WWW.LINUXMAGAZINE.COM.BR](http://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**  
**Webhbt**  
**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.

# → Apple passa a contribuir com o projeto OpenJDK

A Apple vai contribuir, em conjunto com a Oracle, para o projeto OpenJDK. O objetivo é desenvolver aplicações Java de código aberto para o Mac OS X. A decisão também indica uma mudança na estratégia da Apple para o Java, pois, significa que a empresa – com ou sem intenção – respondeu ao apelo dos entusiastas do Java sobre abrir e tornar públicos os componentes do projeto. A notícia surge após a IBM também anunciar sua contribuição com o OpenJDK.

Em outubro, a Apple anunciou uma “despedida silenciosa” para o Java, classificando sua versão de desenvolvimento e ambiente runtime para o Mac OS X 10.6 e 10.5 como “obsoleta”. A empresa não queria mais manter as implementações.

De acordo com o anúncio conjunto das empresas, a Apple vai contribuir com a maioria dos principais componentes, ferramentas e tecnologias necessárias para a implementa-

ção do OpenJDK. O anúncio menciona versões 32 e 64 bits baseadas na máquina virtual Java, bibliotecas de classe, uma pilha de rede e as bases para uma nova interface gráfica.

Além disso, a Apple também tem planos de disponibilizar a versão estável do Java Standard Edition (Java SE 6) para o Mac OS X Snow Leopard e para o futuro Mac OS X Lion. Futuras versões do Java para o sistema operacional da Apple serão lançadas pela Oracle. Explicando a razão da entrega de seus componentes Java para a Oracle, a Apple afirmou que a melhor maneira de seus usuários obterem uma versão segura e estável dos componentes Java, seria diretamente com a Oracle. □

## ► Lançada atualização de segurança para o ProFTPD

Uma falha de segurança foi encontrada no ProFTPD, permitindo ataques de usuários não autenticados à um determinado servidor. O problema é causado por um estouro de buffer na função `pr_netio_telnet_gets()`.

O ProFTPD é capaz de processar sequências TELNET IAC na porta 21; as sequências são capazes de habilitar ou desabilitar algumas opções não suportados pelo protocolo Telnet ou FTP. O estouro de buffer permite que invasores possam escrever e inserir um código malicioso no sistema. Com a atualização para a versão 1.3.3c do ProFTPD, o problema é resolvido.

A atualização também corrige uma vulnerabilidade de passagem de diretório que só pode ser explorada se o módulo `mod_site_misc` estiver carregado. Essa falha pode permitir que invasores com privilégios de escrita possam excluir diretórios ou criar links simbólicos para outros locais do sistema. O módulo não vem carregado por padrão.

Mais informações podem ser encontradas no site do projeto. Os desenvolvedores recomendam que os usuários atualizem o aplicativo o quanto antes. ■

## ► Citrix lança nova versão do XenServer

A Citrix Systems anunciou o lançamento de uma nova versão do Citrix XenServer, com novidades em armazenamento e conectividade que mudam o cenário da virtualização de desktops e servidores para clientes de qualquer porte. O Citrix XenServer é uma versão gratuita de gerenciamento de desktops e computação em nuvem.

O XenServer atingiu um novo marco com a instalação do software em ambientes de produção para a virtualização de servidores em mais de 50 mil empresas em todo o mundo, dentre as quais, mais de 50% estão listadas na Fortune 500. O número de novas ativações do XenServer em ambientes de produção cresce a uma taxa de mais de mil novos servidores ativados por dia. A solução também continua ganhando mercado entre os provedores de nuvem, beneficiados pelo hipervisor Xen – plataforma open source de virtualização mais popular na nuvem. Além do crescimento nos ambientes de servidor e nuvem, o XenServer é agora o hipervisor mais popular para desktops virtuais, hospedando aproximadamente 2,5 milhões de desktops baseados em VDI. ■

## ► Red Hat lança Red Hat Enterprise Linux 6, trazendo inovações

A Red Hat anunciou na primeira quinzena de novembro, o lançamento do Red Hat Enterprise Linux 6, o lançamento do mais recente sistema de plataforma operacional da empresa, definindo o cenário para sistemas operacionais open source na próxima década. Com a solução, a Red Hat estabelece novos padrões para ambientes operacionais corporativos livres. Criado para dar suporte às atuais arquiteturas empresariais, cada vez mais flexíveis e variadas, o produto atende às necessidades para ambientes físicos, virtualizados e implantação em nuvem.

Disponível há cerca de uma década, o Red Hat Enterprise Linux, ganhou reputação por sua performance e confiabilidade e é uma valiosa ferramenta àqueles que operam sistemas. Por incorporar tecnologias desenvolvidas pela Red Hat, seus parceiros e a comunidade de Software Livre, o Red Hat Enterprise Linux 6 possui recursos novos que expandem o produto. Os aperfeiçoamentos passam por melhoria de kernel para gerenciamento de recursos, RAS, desempenho, escalonabilidade, virtualização e economia de energia, além de uma gama de servidores atualizados e aplicações para desktop. Seu design aumenta a agilidade, reduz custos e diminui a complexidade de TI para os usuários

O Red Hat Enterprise Linux 6 é uma boa escolha para usuários que estão buscando migrar de UNIX para Linux e representa uma alternativa vantajosa com relação a sistemas corporativos de servidores. A nova versão oferece inovações para nuvens públicas e privadas. ■



**Você está com a cabeça nas nuvens?  
Nós também.**

**AntiSpam SaaS UNODATA**

BASEADO EM SOFTWARE,  
FILTRO DE ENTRADA E SAÍDA,  
FLEXÍVEL E CUSTOMIZÁVEL,  
CLIENTES 100% SATISFEITOS

**30 DIAS  
GRÁTIS!**

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

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

# ► Intel anuncia novo diretor geral para América Latina

A Intel anunciou recentemente que Steve Long foi contratado como o novo diretor geral para a América Latina. Ele substituirá Jesus Maximoff, que ocupou o cargo durante quase três anos. Maximoff se dedicará a novas oportunidades de negócios na Intel.

Segundo um comunicado emitido pela empresa, Jesus Maximoff e Steve Long trabalharão juntos na transição do cargo até o final de 2010. Long estará sediado em São Paulo, e assume o comando a partir de 2011.

Steve Long é formado em Artes pela Universidade de Tulane em New Orleans, EUA, e possui MBA em Negócios pela Universidade do Texas. Está na Intel há mais de 10 anos e ocupou diversos cargos internacionais na empresa nos Estados Unidos, Brasil e México.

A carreira do executivo na Intel inclui posições em localidades como Califórnia (USA), Hong Kong (China) e Texas (USA), nas áreas de vendas e marketing. Atualmente é responsável pela área de vendas da Intel para contas multinacionais voltadas para as Américas, exceto EUA. ■

## ► Lenovo do Brasil anuncia novo Diretor de Vendas

A Lenovo contratou no mês de novembro Armando Alvarenga de Souza para o cargo de diretor geral de vendas da Lenovo do Brasil. O profissional sênior tem como missão consolidar a liderança da empresa no mercado corporativo. “Assumo o cargo na Lenovo com objetivo de ampliar a posição de liderança no mercado corporativo já conquistada, oferecendo mais suporte para esse crescimento por meio da reformulação do modelo de negócios e alinhamento com a estratégia mundial da empresa”, afirma o diretor, que possui formação em Engenharia Eletrônica, com ênfase em Telecomunicações, pela Escola Politécnica da USP, e MBA em Administração pela mesma Universidade.

Alvarenga conta com mais de 20 anos de experiência na área de Telecomunicações e TI para empresas. Ele conduzia a Siemens Enterprise Communications no Brasil desde sua formação, em 2006. Anteriormente, foi diretor da área Private Networks da Siemens do Brasil. Com vasta experiência internacional, o executivo morou por dois anos em Munique, na Alemanha. ■

## ► Nokia anuncia o fim da Fundação Symbian

A Nokia anunciou no início de novembro que a Fundação Symbian, atualmente a entidade responsável pelo desenvolvimento do sistema operacional para smartphones Symbian, irá deixar de existir. A previsão é de que, em seis meses, a Fundação torne-se apenas um órgão de licenciamento, conforme o vice-presidente da área de smartphones, Jo Harlow, divulgou no blog oficial da empresa.

No entanto, Harlow afirmou que a Nokia irá continuar o desenvolvimento da plataforma: “Agora é a hora de a Nokia conduzir o Symbian ao próximo estágio”.

Muito se tem discutido acerca do futuro do sistema operacional da Nokia, e as especulações aumentaram depois que a Samsung e a Sony Ericsson decidiram deixar de usá-lo, preferindo-o em favor do Android. No entanto, a fabricante insistiu, em um recente comunicado, que os últimos acontecimentos em nada alterarão seu planejamento.

A mudança de postura em relação ao Symbian já era esperada, afirma o instituto de pesquisa CSS Insight. Em julho, Ben Wood, diretor do instituto, já afirmara que a Nokia havia estudado mal o mercado ao tornar open source a sua plataforma. ■

## ► Presidente da Microsoft vende 12% de sua participação na empresa

O presidente-executivo da Microsoft, Steve Ballmer, vendeu 1,3 bilhão de dólares em ações da empresa, reduzindo sua fatia na companhia em cerca de 12 por cento. O executivo comentou que sua primeira venda de ações da Microsoft em sete anos não deve ser considerada como um sinal de desconfiança na maior fabricante mundial de software.

Ballmer afirmou que venderá mais ações até o fim do ano, em uma medida para diversificar seus investimentos, mas a empresa procurou minimizar rumores de que o executivo, no comando da empresa desde 2000, possa estar se preparando para deixar a companhia.

“Ainda que seja uma questão de finanças pessoais, quero deixar claro para evitar confusões.”, disse Ballmer em comunicado divulgado no site da empresa. “Estou animado com nossos novos produtos e o potencial de nossa nova tecnologia para mudar a vida das pessoas e continuo completamente comprometido com a Microsoft e seu sucesso.”

Ballmer, que foi o primeiro gerente de negócios da Microsoft quando entrou para a companhia nos anos 1980, não demonstrou nenhum interesse em deixar a empresa, apesar das críticas de Wall Street sobre o preço da ação da companhia, atualmente de volta ao mesmo patamar de 2002.

De acordo com documentação encaminhada a *Securities and Exchange Commission*, Ballmer vendeu 49,3 milhões de ações da Microsoft nos últimos dias, a preços ao redor de 27 dólares por ação.

Ballmer disse ter planos de vender até 75 milhões de ações até o final do ano. Se ele realmente fizer isso, a venda reduzirá a participação do executivo na empresa em 18 por cento, baseado nas 408 milhões de ações que ele detinha antes das vendas mais recentes.

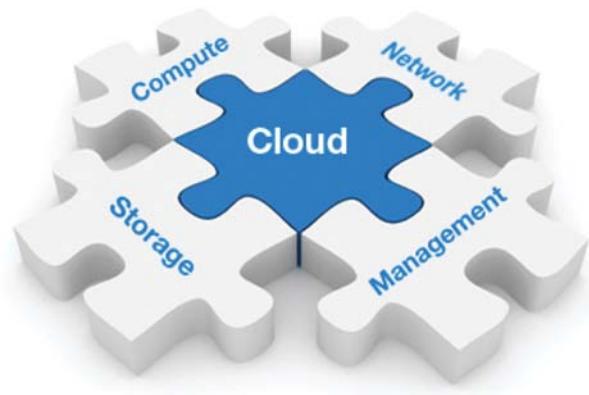
Até novembro, Ballmer ainda mantinha 359 milhões de ações da Microsoft, ou 4,2 por cento da empresa, avaliadas em 9,6 bilhões de dólares. Esse volume torna o executivo o segundo maior acionista da Microsoft, atrás do co-fundador Bill Gates, segundo dados da Thomson-Reuters.

Gates, que detém cerca de 621 milhões de ações, ou aproximadamente 7,2 por cento da empresa, vende ações regularmente em lotes de 1 milhão ou 2 milhões para financiar sua fundação. ■

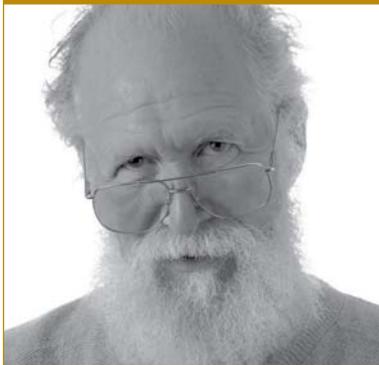
## ► Citrix OpenCloud vence prêmio

A Citrix Systems divulgou que sua solução, Citrix OpenCloud foi vencedora do prêmio PC World 2010 como Melhor Solução de Nuvem da América Latina. O aplicativo foi selecionado por um juri composto por jornalistas.

O Citrix OpenCloud proporciona às empresas e prestadores de serviços uma abordagem pragmática da computação em nuvem que simplifica a migração. Com a plataforma, as empresas podem utilizar as tecnologias de infraestrutura preexistentes, adicionar novas, integrar seus bancos de dados a nuvens externas e provisionar aplicativos, entregando-os aos usuários. Os fornecedores de soluções em nuvem também podem aumentar o alcance dos seus produtos, incorporando suas experiências e melhores práticas ao Citrix OpenCloud e, desta forma, oferecer uma variedade maior de soluções.



“Com os serviços de nuvem se consolidando e se desenvolvendo no mercado latino americano, as empresas estão buscando meios para se beneficiar destes serviços sem arcar com expansão ou custos adicionais de infraestrutura de TI. O Citrix OpenCloud permite ao usuário usufruir de um número crescente de serviços de computação em nuvem públicos, aproveitando a infraestrutura preexistente e sem precisar adotar uma abordagem específica de nuvem”, afirma Enrique Pla, vice-presidente da Citrix para a América Latina. “Ser premiado pela PC World América Latina reforça o nosso compromisso de oferecer poder de escolha aos clientes e nossa visão de entregar a TI como serviço”, completa Pla. ■



Coluna do maddog

# Hardware e cervejas

*Maddog visita o Rio de Janeiro para o evento "Hack and Beer" e conta sobre sua viagem.*

O menininho atrás de mim estava muito animado com sua primeira viagem de avião. Quando o avião começou a decolagem, ele fez uma contagem regressiva para o “lançamento”. Foi bom ver tanto entusiasmo, principalmente porque viagens aéreas se tornaram um “elevador mágico” para mim. As portas se fecham em um lugar e se abrem em outro, mas não estou tão animado com essa viagem, apenas com o destino dela.

Senti uma emoção semelhante à do menino no meu primeiro *Arduino Hack and Beer*. Organizado pelo meu amigo Álvaro Justen, no Rio de Janeiro. Devo admitir que duvidei um pouco que qualquer coisa proveitosa viria de apenas uma noite de *hardware hacking*.

O planejamento e a organização do evento *Hack and Beer* ocorreu há algum tempo. Uma taxa foi solicitada para ajudar a pagar as bebidas, petiscos, refrigerantes e, claro, cerveja. Quatro projetos foram discutidos, e cerca de 20 pessoas apareceram, então aproximadamente quatro ou cinco pessoas trabalharam em cada projeto.

Todos os projetos precisavam de um Arduino [1]. O

seja possível criar novos hardwares derivados de placa-mãe (placas em geral: vídeo, fax, ou novas invenções). A maioria desses novos hardwares tende a ser protótipos de fácil criação, e por isso os usuários podem construir extensões de hardware simples baseados na plataforma. Uma cadeia de desenvolvimento de software permite que sejam criados programas para o Arduino facilmente. Também faz com que sejam testados e armazenados. Uma grande e crescente biblioteca de código-fonte está disponível para a montagem de circuitos elétricos simples (e não tão simples). E o melhor de tudo, esses componentes elétricos e o próprio Arduino são relativamente baratos e reutilizáveis para outros fins.

Depois de distribuir os petiscos, refrigerantes e cervejas, dividimo-nos em quatro grupos. Um grupo era liderado por uma moça que demonstrou a programação básica do Arduino. Outro grupo estava trabalhando na produção de uma interface do Arduino para um semáforo, o que foi difícil, porque a luz conduzida precisava de uma entrada maior do que o Arduino poderia gerar.

Meu grupo estava tentando integrar um sensor que usa som para medir a distância. Alguns circuitos e o software já haviam sido desenvolvidos e publicados para o Arduino, mas o sensor utilizado no programa de teste foi bastante caro, e alguém achou um outro que custava muito menos. O sensor chegou, e meu grupo estava ansioso para continuar o trabalho.

Quando me pediram para ajudar o grupo do sensor em seu projeto, a princípio recusei, pois não sei nada sobre o Arduino; só sei que ele tem pouco espaço de memória. E já fazia mais de 20 anos que eu não mexia com eletrônica. Porém, percebi que o Álvaro estava precisando de ajuda. Muitas pessoas que lá estavam não eram formadas em computação nem em engenharia elétrica, mas sim em história e outras disciplinas gerais

**A maioria desses novos hardwares tende a ser protótipos de fácil criação, e por isso os usuários podem construir extensões de hardware simples baseados na plataforma.**

e apenas queriam vivenciar a experiência de participar desse tipo de atividade.

O grupo carregou o código e conectou o sensor. Infelizmente, ele não funcionou; o programa devolvia distâncias muito grandes o tempo todo. Então, fiquei sabendo sobre o outro sensor e perguntei se eles tinham as especificações dele. Ninguém tinha, e eu sugeri que procurassem na Internet pelo número do sensor para ver se conseguiam localizar as especificações. Tudo foi encontrado online.

O novo sensor possuía três pinos – um para a energia elétrica, outro para o terra e outro para a saída, que emitia um sinal quando o sensor detectava uma onda sonora retornando – e o grupo estava tentando enviar o sinal no pino de saída. Comecei a suspeitar que o funcionamento desse sensor era completamente diferente do sensor usado no código de teste do Arduino, então expliquei que, sem mais especificações desta unidade, não poderíamos determinar o espaço de tempo entre a ativação do sinal e o primeiro pulso emitido. Além disso, não sabíamos por quanto tempo o pulso emitido

estaria presente no pino de saída ou se o Arduino iria conseguir captá-lo. Sugeri um circuito elétrico conhecido como *latch*. Infelizmente, não dispúnhamos das partes necessárias para montar um.

Apesar de o sensor não ter funcionado nessa sessão do *Hack and Beer*, sei que a equipe aprendeu muito com nossos esforços. Outros membros disseram que continuariam tentando: estavam animados com a viagem, não com o destino dela, e essa é a ideia do *Hack and Beer*. ■

### Mais informações

[1] Arduino: <http://www.arduino.cc/>

**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 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 LP1 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





*Coluna do Taurion*

# Quais as soluções para enfrentar o trânsito?

*Um sistema inteligente de transportes resolveria o problema do trânsito caótico das grandes cidades?*

**U**m dos desafios das grandes cidades é o trânsito caótico e um sistema de transporte público ineficiente. Uma pesquisa recente feita pela IBM em 20 cidades do mundo inteiro, mostrou que o tempo de viagem é um dos motivos de insatisfação e stress dos usuários, gerando perdas em produtividade e qualidade de vida.

As seis piores cidades em matéria de trânsito, encontram-se nos países em desenvolvimento. O rápido crescimento econômico desses países não foi acompanhado pela evolução da infraestrutura urbana e o resultado é um trânsito caótico. As soluções tradicionais, como construir mais avenidas e viadutos, está chegando ao seu limite. Temos que buscar soluções novas e inovadoras.

A crescente disseminação da tecnologia está permitindo a convergência entre o mundo digital e físico da infraestrutura urbana. Com isso podemos pensar em um sistema de transporte mais inteligente, conhecido como ITS (*Intelligent Transport Systems*). Seu conceito baseia-se na aplicação de tecnologias inovadoras para coletar mais e melhores dados, analisá-los de forma mais rápida e inteligente e conectá-los através de redes mais eficientes para ações e decisões mais ágeis e eficazes.

Embora as consequências do congestionamento sejam similares, as suas causas e soluções são diferentes entre as cidades do mundo. Por exemplo, em Amsterdam, metade dos cidadãos andam a pé ou de bicicleta. Já em Chicago, quase toda movimentação é feita através de carros particulares.

Mas, chegar a um sistema inteligente de transporte é um processo de evolução gradual, que passa pelo nível de maturidade dos modelos de governança e gestão de transporte das grandes cidades. O modelo chamado *Intelligent Transport Maturity Model* permite situar uma cidade em um determinado nível de maturidade e ajudar a desenhar os próximos passos.

Por exemplo, podemos classificar uma cidade em diversos níveis, do mais baixo onde o planejamento de cada

modalidade de transporte é feito de forma independente, sem coordenação com os demais, até níveis mais avançados.

Na vertente de serviços oferecidos, vemos que nos níveis mais baixos de maturidade não existe a figura do “bilhete único” (modelo aplicado em grandes cidades para integrar os meios de transporte através de um cartão magnético) e portanto cada meio de transporte é pago separadamente. Nos níveis mais avançados chegamos à integração multimodal, onde o mesmo pagamento serve para qualquer modalidade de transporte e as formas de pagamento são variadas, inclusive via celular. Ainda nesse nível, o sistema de transporte oferece serviços completos de informação, que orientam a viagem de forma multimodal, ou seja, indicam qual o melhor meio para se deslocar de um ponto a outro, inclusive com alertas em tempo real de eventuais interrupções ou atrasos nos serviços.

Os passos básicos para implementação de um modelo de transporte inteligente passam pelas seguintes etapas:

- a) Desenvolver uma estratégia abrangente de transporte, que envolva todos os modelos e aspectos econômicos da cidade e que considere a possibilidade de usar tecnologias inovadoras.
- b) Adotar a visão do cidadão usuário do transporte público como um cliente. Com as informações da demanda desses clientes pode-se criar serviços inovadores e inclusive meios para incentivar deslocamentos em outros horários, através de preços variados.
- c) Implementar um sistema de mobilidade urbana integrada, que inclua não apenas o transporte público, mas o particular, como automóveis e bicicletas.
- d) Utilizar um sistema de comunicação e divulgação, que integre a sociedade no processo, também é fundamental para o sucesso do projeto. ■

**Cesar Taurion** ([ctaurion@br.ibm.com](mailto: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>

Sistemas de arquivos distribuídos

# Em busca do melhor

*Para garantir tolerância a falhas, proteção e consistência de dados, bem como replicação segura – entre outros atributos –, a escolha do melhor sistema de arquivos distribuído é imprescindível.*

**por Flávia Jobstraibizer**

Um sistema de arquivos distribuído (SAD), é um tipo de sistema de arquivos no qual todos os dados nele armazenados estão espalhados em hardwares fisicamente diferentes, interconectados através de uma rede. Tais sistemas possuem vários aspectos semelhantes aos dos sistemas de arquivos centralizados, além de operações de manipulação de arquivos, mecanismos de redundância e consistência, entre outros atributos. A vantagem do uso de um SAD, é a possibilidade de montar estratégias de distribuição de carga para melhor desempenho no acesso aos dados, mesmo sob alta demanda.

A escolha da melhor opção de um sistema de arquivos distribuído eficiente, depende da topologia da rede, ou da estratégia de armazenamento de dados.

Nesta edição, você irá conhecer alguns dos principais sistemas de arquivos distribuídos do mercado. O KosmosFS, oriundo do GFS – *Google File System* – e do projeto Hadoop, é um sistema que impressiona por sua simplicidade e pela perfeita manipulação de dados na casa dos gigabytes e terabytes.

Para quem tem a necessidade de um sistema de arquivos de cluster, o OCFS2 – *Oracle Cluster File System* – é a melhor opção. Com bloqueio de arquivos via DLM – *Distributed Lock Manager* –, e configuração inteligente de discos compartilhados, o sistema de arquivos já está presente no kernel Linux padrão desde a versão 2.6.16, e é de fácil utilização.

O já conhecido NFS, sistema de arquivos de rede clássico do Linux, está agora em sua versão 4 (NFSv4), e é robusto e completo. Conheça sua diversidade de protocolos, e entenda como o sistema trabalha em rede e gerencia cadeias de processos.

E para finalizar esta edição recheada de incríveis sistemas de arquivos distribuídos, conheça o OpenAFS, implementação de código aberto do AFS – *Andrew File System*. Seguro e escalável, o sistema funciona por meio de células AFS e volumes de dados específicos. Embora pouco utilizado, o sistema surpreende por sua facilidade de implementação e sua ampla gama de recursos e opções de configuração. Boa leitura! ■



## Matérias de capa

O sistema que veio do Kosmos	30
Cluster compartilhado	35
Armazenamento com segurança	42
Seguro e escalonável	49

# O sistema que veio do Kosmos

Sistemas de arquivos distribuídos manipulam facilmente arquivos de tamanhos nas faixas dos gigabytes e terabytes. O sistema de arquivos Kosmos impressiona seus concorrentes.

por Tim Schürmann

Programas de computador modernos lidam com volumes cada vez maiores de dados. Enquanto aplicativos de busca de dados gostam de vassourar montanhas de informações, os mecanismos de busca da Internet constantemente arrebanham novas informações. Os usuários que acessam tais dados regularmente costumam encontrar arquivos de vários gigabytes ou mais.

Sistemas de arquivos抗igos logo chegam ao seu limite de espaço com esse tipo de dados a essa taxa de transferência. Consequentemente, as empresas que administram grandes volumes de dados precisam de uma solução alternativa para o acesso rápido e seguro às informações. O armazenamento redundante de dados é útil; afinal, quem quer perder dados valiosos obtidos em dias de processamento por causa de um erro de disco banal?

Sistemas de arquivos distribuídos preenchem esses requisitos. Um sistema de arquivos distribuído divide os dados em partes gerenciáveis e armazena os pedaços em *clusters* de computadores escalonáveis. Ao virtualizar o armazenamento em cluster, o sistema de arquivos, em seguida, faz os aplicativos acreditarem que estão lidando com um enorme disco rígido.

## No espaço

O sistema de arquivos *Kosmos* (KFS) [1] é algo novo e promissor nesse campo. A Kosmix Corporation desenvolveu o KFS e liberou o código-fonte sob a licença Apache. A primeira versão, alfa 0.1, foi lançada em setembro de 2007. A relativa juventude do KFS aparece na configuração do sistema de arquivos: o KFS necessita de uma versão Linux de 64 bits. Se possível, a versão do Linux e da distribuição devem ser idênticas em

todos os computadores envolvidos no armazenamento de dados.

O KFS enfrenta alguns competidores de renome, incluindo o sistema de arquivos do Google (GFS), utilizado pela empresa como fundamentos de seu motor de busca, e o projeto HDFS [2] da Hadoop. Os desenvolvedores do KFS emprestaram grande parte da estrutura e funcionalidade do Google, mas tiraram uma série de limitações. O KFS – como o GFS – está otimizado para os cenários em que muitos arquivos grandes são criados uma vez, mas lidos muitas vezes [3].

## Apresentação da tripulação

O sistema de arquivos Kosmos é dividido em três camadas:

- Um ou vários servidores de *chunk* (blocos de dados) que armazenam os dados em seus próprios discos rígidos;

- ▶ Um metaservidor que monitora os servidores de chunk;
- ▶ Um aplicativo que rapidamente elimina arquivos grandes.

O KFS, portanto, funciona de modo bastante similar a um banco de dados que fica entre um programa de computador e o sistema de arquivos tradicional (**figura 1**).

## Em blocos

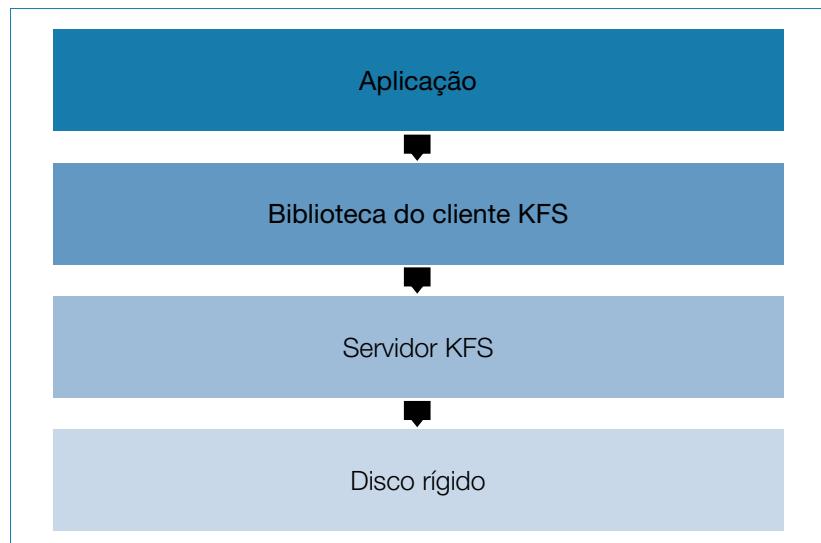
O KFS primeiro divide um arquivo em blocos de 64 MB cada, que são simples de manipular. O sistema de arquivos distribui uniformemente esses pedaços entre todos os servidores conectados, apropriadamente denominados como servidores de chunk. Os servidores armazenam os blocos em arquivos normais que pertencem aos sistemas operacionais do *host*.

Se os servidores de chunk começam a apresentar esgotamento de sua capacidade de armazenamento, o administrador pode simplesmente adicionar um novo computador ao cluster. O KFS ajusta automaticamente o nó de armazenamento, o que mantém todo o sistema escalonável e ajuda a manter o ritmo sincronizado com o aumento da demanda por armazenamento.

O KFS minimiza erros de hardware, armazenando os blocos de cada arquivo de forma redundante em múltiplos servidores de chunk; normalmente, existem três instâncias de cada arquivo armazenado.

Essa rede de segurança permite aos administradores usar computadores baratos como repositórios de dados confiáveis. O Google FS prova que isso funciona todos os dias. Se um disco ou um servidor falhar, basta trocá-lo por um novo. O KFS detecta automaticamente a substituição e integra o recém-chegado ao cluster.

Como outra medida preventiva contra a perda de dados, cada



**Figura 1** O sistema de arquivos Kosmos reside entre o hardware existente e o aplicativo, assim como um banco de dados. A biblioteca cliente cuida do acesso ao sistema de arquivos virtual.

bloco tem um número de versão e um código de verificação (*checksum*). O KFS avalia o checksum em cada operação de leitura. Em caso de irregularidade, o sistema de arquivos distribuídos exclui o bloco de informação com defeito e o substitui imediatamente com uma cópia intacta (re-replicação).

Os números de versão ajudam a identificar chunks obsoletos: se uma conexão de Internet ruim temporariamente separa um servidor do cluster, é possível identificar chunks obsoletos rapidamente, quando a conexão for restabelecida e a variante mais recente for recuperada de outros servidores do cluster.

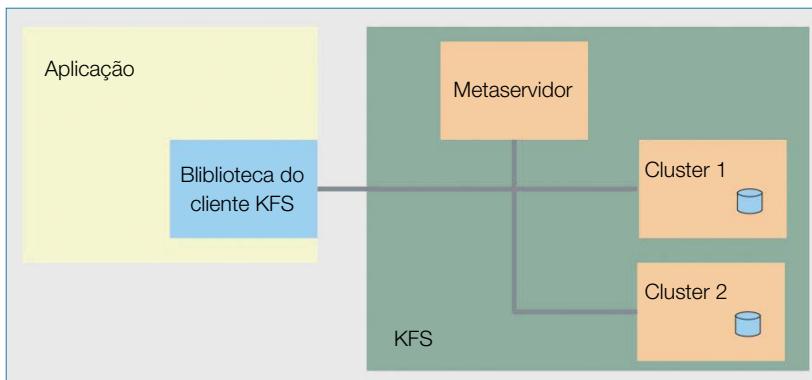
### Quadro 1: Caixa de ferramentas

A biblioteca cliente fornece aos aplicativos um acesso conveniente aos recursos do sistema de arquivos, mas para verificar o conteúdo de um diretório seria preciso uma ferramenta de programação. O pacote KFS tem um shell especial para remover a necessidade de programação extra. O shell oferece ferramentas Unix populares, incluindo `ls`, `cp` e `mv`. Graças ao shell, os usuários podem navegar pela árvore do KFS normalmente. Para iniciar o shell, é preciso executar um script no diretório `scripts`:

```
python kfsshell.py -f
Konfigurationsdatei.cfg -b
~/kfs-0.1.1/build/bin/KfsPing
```

O `KfsPing` é uma ferramenta avançada para `ping` que fornece um serviço útil de monitoramento de servidores KFS. Digitar `KfsPing-h` mostra a ajuda da ferramenta. Outras ferramentas úteis estão localizadas no diretório `build/bin/tools`.

Se a ideia de comandos especiais não agrada, a alternativa no Linux é o suporte FUSE (*Filesystem in userspace*), um módulo de kernel que migra um driver de sistema de arquivos para o modo de usuário. O FUSE permite aos usuários montar o KFS como uma partição de disco rígido normal e, em seguida, utilizar a gama completa de ferramentas Linux.



**Figura 2** Um aplicativo que quer acessar um arquivo recorre à biblioteca do cliente. A biblioteca faz uma busca no metaservidor para descobrir em qual cluster de servidores o arquivo reside e, em seguida, recupera o arquivo dos servidores.

## Metaservidor

Infelizmente, os servidores de chunks não lembram quais partes de quais arquivos são armazenadas em qual servidor. Por essa razão, um servidor de metadados (ou *metaservidor*, para abreviar) é usado para monitorar um número de servidores de chunk (o sistema de arquivos do Google se refere a esses metaservidores como *masters*). Como o nome sugere, os metaservidores armazenam os metadados, incluindo detalhes de qual servidor tem qual parte de um arquivo, o tamanho do arquivo correspondente e os nomes e informações sobre os processos que estão acessando cada arquivo.

Em intervalos regulares, o metaservidor verifica a capacidade dos servidores de chunks que lhe são atribuídos. Se necessário, o metaservidor irá migrar partes de um servidor com uma carga pesada para uma máquina de menor movimento (reequilíbrio). Isso optimiza o uso das capacidades disponíveis, melhorando, assim, o desempenho em geral.

## Clientes

Os aplicativos utilizam a biblioteca do cliente para acessar essa infraestrutura (**figura 2**). A biblioteca inclui uma API completa de sistema de arquivos que permite aos clientes armazenar grandes arquivos no KFS, manipular e ler todos os arquivos existentes normalmente.

Em contraste com o HDFS, seu concorrente, o KFS suporta a gravação em posições arbitrárias de um arquivo ou dados anexos a arquivos existentes.

Infelizmente, a biblioteca do cliente é a única porta para o sistema de arquivos distribuído, com exceção de algumas ferramentas mínimas (**quadro 1**). Por conseguinte, não há como escapar da modificação de seus próprios programas, e a escolha de linguagens de programação é restrita a C++ ou Python. Programadores Java podem usar a interface nativa JNI. Em uma jogada inteligente, os

desenvolvedores do KFS adicionaram uma API para o sistema de arquivos HDFS, concorrente do KFS. Assim, programas escritos para o HDFS podem ser portados facilmente para o KFS.

## Início

O Kosmos FS é fornecido sob a forma de um arquivo de código-fonte que só pode ser usado em um sistema de 64 bits. Fora isso, o Kosmos é bastante frugal em suas exigências: além de `CMake`, são necessárias apenas as bibliotecas `Log4cpp` e `Boost`. Depois de cumprir os requisitos, basta descompactar e abrir o arquivo `Cmake-Lists.txt`.

Por padrão, o compilador irá construir os programas e bibliotecas KFS com informações de depuração. Se preferir não fazer a depuração, altere o valor entre aspas que vem depois do parâmetro `CMAKE_BUILD_TYPE` de `Debug` para `Release`. Se precisar de suporte à biblioteca FUSE, descomente a linha `# set (Fuse_LIBRARY_DIR "")` e adicione o caminho entre as aspas.

O administrador deve inserir uma série de comandos para compilar e instalar o KFS. Para começar, mude para o diretório do código-fonte do KFS, que é `~/kfs-0.1.1` neste exemplo. Quando chegar lá, digite os seguintes comandos:

```
mkdir build
cd build
cmake ~/kfs-0.1.1
gmake
gmake install
```

O último comando sugere uma instalação do sistema, mas o que realmente acontece é que os programas criados na etapa anterior são transferidos para `~/kfs-0.1.1/build/bin` e as bibliotecas correspondentes para `~/kfs-0.1.1/build/lib` ou `~/kfs-0.1.1/build/lib-static`.

Se precisar de uma interface Java, é possível ir até o diretório do KFS

### Listagem 1: Configurando o Kosmos FS

```
01 [metaserver]
02 node: 192.168.1.100
03 rundir: /home/tim/kfs/➥
metaserver
04 baseport: 20000
05 [chunkserver1]
06 node: 192.168.1.101
07 rundir: /home/tim/kfs/chunk1
08 baseport: 30000
09 space: 30 G
10 [chunkserver2]
11 node: 192.168.1.102
12 rundir: /home/tim/kfs/chunk2
13 baseport: 30000
14 space: 18000 M
```

em `~/kfs-0.1.1`, e iniciar a interface através do comando `ant jar`. Se tudo der certo, o arquivo `kfs.jar` deve estar presente no subdiretório de compilação. Esse pacote contém tudo que é preciso para desenvolver programas em Java que usam o KFS.

A interface Python é um pouco mais complexa. Comece mudando o diretório para `~/kfs-0.1.1/src/cc/access`, abra o arquivo `kfs_setup.py` em um editor e modifique os caminhos de inclusão. Em seguida, dê o comando de compilação `kfs_setup.py python ~/kfs-0.1.1/build/lib`. Isso cria o arquivo `kfs.so` no diretório de compilação, que pode então ser integrado ao ambiente Python através da instrução `python kfs_setup.py ~/kfs-0.1.1/build/lib/ install`.

## Iniciar o KFS

A próxima etapa distribui os arquivos binários entre os metaservidores e os servidores de chunk. Um script Python no diretório `~/kfs-0.1.1/scripts/` cuida disso, criando um pacote de programas personalizados para cada servidor e garantindo a instalação em conjunto com o terminal SSH.

Para permitir que isso aconteça, todos os seus servidores devem executar o mesmo ambiente Linux, ou pelo menos as distribuições não devem ser muito diferentes. Configurar o SSH com pares de chaves elimina a necessidade de digitar várias senhas.

## Topologia

A única coisa que falta agora é o arquivo de configuração que informa ao script quais computadores da rede desempenharão qual tarefa. A **listagem 1** mostra um exemplo de configuração.

O arquivo tem uma seção separada para cada servidor envolvido, encabeçada pelo nome do servidor entre colchetes. A exigência mínima é uma seção `[metaserver]`.

Na sequência existe uma seção para cada servidor de chunk, que normalmente assume as formas de `[chunkserver1]` até `[chunkserverN]`. O cluster do KFS nesse exemplo compreende um metaservidor e dois servidores de cluster.

O parâmetro `node` é seguido pelo nome do endereço IP para o servidor. `rundir` é seguido pelo diretório em que os binários serão armazenados (no exemplo da **listagem 1**, esse é o diretório `home` da conta do usuário `tim` em cada servidor). A palavra-chave `baseport` especifica a porta TCP que o servidor usará para se comunicar com os outros nós.

Os nomes dos computadores não precisam ser diferentes. Na verdade, o Kosmos FS permite executar todos os servidores em uma única máquina – e que pode ser `localhost` – mas em

casos como este, é preciso atribuir portas TCP exclusivas para o seu metaservidor e os servidores do cluster.

Cada servidor de chunk tem uma opção `space`, que especifica a quantidade de espaço em disco que o servidor vai usar para salvar os dados. No exemplo, o primeiro servidor de chunk oferece 30 GB, o segundo um pouco menos, 18.000 MB. Arquivos de configuração de exemplo estão disponíveis no diretório `conf`.

## Central de comando

Agora que o arquivo de configuração está concluído, o próximo passo é alterar o diretório para os scripts e habilitar o seguinte:

```
python kfssetup.py -f configuration_file.cfg -b ../build/bin
```

### Listagem 2: Programa para armazenamento de dados no KFS

```
01 ...
02 #include "libkfsClient/KsfClient.h"
03
04 using namespace KFS; // Espaço de nomes (namespace do KFS):
05
06 int main(int argc, char **argv)
07 {
08     string serverHost= "localhost";
09     int port = 20000;
10
11     KfsClient *gKfsClient
12
13     // Fornecer acesso ao sistema de arquivos:
14     gKfsClient = KfsClient:: Instance();
15     gKfsClient->Init (serverHost, port);
16
17     // Criar subdiretório:
18     gKfsClient->Mkdirs("testdir");
19
20     // Abrir arquivo "fd":
21     int fd = gKfsClient->Create(testdir/foo.1");
22
23     //Write junk:
24     int numBytes=2048
25     char *buffer=new char[numBytes];
26     gKfsClient->Write(fd, buffer, numBytes);
27
28     // Atualizar atualizações:
29     gKfsClient->Sync(fd);
30
31     // Fechar arquivo:
32     gKfsClient->Close(fd);
33 }
```

Graças ao arquivo de configuração, todos os servidores e o SSH podem ser iniciados centralmente a partir da máquina atual:

```
python kfslaunch.py -f
configuration_file.cfg -start
```

Para desligar o sistema, utilize:

```
python kfslaunch.py -f
configuration_file.cfg --stop
```

Especificar o arquivo de configuração é importante e permite aos usuários o gerenciamento de diferentes clusters KFS a partir de um único console.

Agora que os servidores estão funcionando, os usuários podem começar a mover dados para o enorme sistema de arquivos novo usando o shell ou através da API. Um exemplo simples de um programa C++ que armazena seus dados no KFS é exibido na [listagem 2](#).

Infelizmente, os arquivos de cabeçalho estão escondidos nas profundezas do código-fonte no diretório `src/cc`. Isto também se aplica às bibliotecas, que estão localizados em `build/lib`:

```
g++ test.cpp -I
~/kfs-0.1.1/src/cc -L
~/kfs-0.1.1/build/lib
-lkfsClient -lkfsIO
-lkfsCommon
```

Antes de executar o programa, o parâmetro `LD_LIBRARY_PATH` tem de ser definido:

```
export LD_LIBRARY_PATH = ↵
~/kfs-0.1.1/build
```

Para poupar ao sistema o trabalho de procurar as bibliotecas dinâmicas, é possível “linkar” os próprios programas em modo estático, que está localizada em `~/kfs-`

`0.1.1/build/lib-static`. Para lidar com grandes volumes de dados, um aplicativo KFS simplesmente abre um novo arquivo através da biblioteca do cliente.

## Buffers

Em primeiro lugar, a biblioteca armazena as operações de escrita, de entrada e espera que a memória cache reservada para isso seja preenchida ou que o aplicativo emita um comando `flush` antes de enviar os dados para os servidores de chunk.

Imediatamente depois que os dados chegam, eles se tornam disponíveis para outras operações.

Além dos dados de saída, a biblioteca cliente também armazena quaisquer metadados que são solicitados por 30 segundos. Isso ajuda a evitar conexões desnecessárias ao servidor.

Se um cliente está sendo executado em um servidor de chunks, ele recupera os dados localmente ao invés de ocupar toda a largura de banda de rede. Se um servidor de chunks de repente falha durante uma operação de leitura, a biblioteca do cliente passa automaticamente para outro servidor de chunks. Tudo isso é completamente transparente para o aplicativo.

## Conclusão

O Kosmos FS é uma alternativa interessante ao Google FS e ao HDFS, mas ainda está em uma etapa intermediária de desenvolvimento. Atualmente, um ponto fraco é o metaservidor. Eles precisam ser capazes de fornecer metadados rapidamente. Afinal, para ser capaz de processar o arquivo, um cliente precisa saber em qual nó o arquivo necessário está armazenado. Se o metaservidor falhar completamente, os arquivos nos servidores de chunks que ele gerencia também ficarão inacessíveis.

O metaservidor adicionaicionalmente cuida da distribuição da carga, por isso é responsável pelo desempenho da rede KFS que gerencia. Infelizmente, não há atualmente nenhum plano de replicação de metadados, em contraste com o esquema usado pelos servidores de chunk. Os administradores precisam cuidar disso manualmente e fazer backup dos dados regularmente.

Outra questão é a falta de controles de acesso. Atualmente, os usuários podem armazenar informações no sistema de arquivos distribuído e ler todos os dados armazenados lá. Por esta razão, o KFS só deve ser implantado em ambientes de teste até que uma versão mais madura seja lançada. ■

## Mais informações

- [1] Sistema de arquivos Kosmos: <http://kosmosfs.sourceforge.net/>
- [2] HDFS e o projeto Hadoop: <http://lucene.apache.org/hadoop/>
- [3] Trabalho sobre o sistema de arquivos do Google (GSF), no qual o KFS se baseia: <http://research.google.com/pubs/papers.html>

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lhm.com.br/article/4453>



Sistema de arquivos de cluster

# Cluster compartilhado

O OCFS2, que já está presente no kernel Linux básico desde a versão 2.6.16 é anterior ao GFS2, sistema de arquivos mais popular. Apesar de não ser trivial sob o capô, o OCFS2 é de fácil utilização.

por Udo Seidel

CAPA

**S**empre que dois ou mais computadores precisam acessar o mesmo conjunto de dados, sistemas Linux e Unix terão várias abordagens concorrentes ([quadro 1](#)). Neste artigo, vamos examinar o OCFS2 – *Oracle Cluster File System*, sistema de arquivos em cluster de disco compartilhado [\[1\]](#). Como o nome sugere, este sistema de arquivos é principalmente indicado para configurações de cluster com vários servidores.

Antes de configurar um sistema de arquivos em cluster baseado em discos compartilhados, é preciso levar em conta alguns itens primordiais. Primeiro, o administrador precisa estabelecer a estrutura básica de um cluster, inclusive estipulando os computadores que pertencem ao cluster, como acessá-lo via TCP/IP e seu nome. No caso do OCFS2, um arquivo ASCII simples já é suficiente ([listagem 1](#)).

A segunda tarefa é controlar e ordenar o acesso aos dados com o uso de bloqueio de arquivos para evitar situações de conflito. No caso do OCFS2, o DLM – *Distributed Lock Manager* evita inconsistências no sistema de arquivos. Inicializar o cluster OCFS2 abre o DLM automaticamente, assim, não é preciso configura-lo separadamente. No entanto, o melhor bloqueio de arquivos é inútil se o computador escrevendo no sistema de arquivos não está funcionando muito bem. A única maneira de impedir que computadores escrevam é adotar o uso de *fencing*. O OCFS2 é bastante simplista em sua abordagem e só usa o auto-fencing. Se um nó perceber que não está mais claramente integrado ao cluster, ele gera um erro do tipo *kernel panic* e se isola. Assim como a DLM, o auto-fencing no OCFS2 não exige uma configuração separada. Uma vez que a configuração do cluster está completa e foi distribuída

para todos os nós, o grosso do trabalho é feito por um OCFS2 funcional.

As coisas são aparentemente muito simples até aqui: inicie o cluster, crie o OCFS2 – se necessário –, monte o sistema de arquivos, e pronto.

## Primeiros passos

Como mencionamos, o OCFS2 é um sistema de arquivos em cluster baseado em discos compartilhados. A gama de tecnologias de discos compartilhados vai do caro SAN até o *Fibre Channel*, e do popular iSCSI até o barato DRBD [\[2\]](#). Neste artigo, vamos utilizar iSCSI e NDAS – *Network Direct Attached Storage*. O segundo ingrediente na configuração do OCFS2 são os computadores com sistema operacional compatível com OCFS2. As melhores opções são o Oracle Enterprise Linux, o SUSE Linux Enterprise Server, o openSUSE, o Red Hat Enterprise Linux (RHEL) e o Fedora.

## Quadro 1: Sistemas de arquivos compartilhados

A família de sistemas de arquivos compartilhados é um grupo bastante diversificado. Por definição, todos eles compartilham a capacidade de conceder acesso simultâneo a determinados dados entre vários computadores. As diferenças estão na maneira de implementar esses requisitos. De um lado estão os sistemas de arquivos em rede, onde o representante Linux/Unix mais popular é o NFS – *Network File System* [3]. O NFS está disponível para quase todos os sistemas operacionais existentes e apenas pede que o sistema operacional forneça uma pilha TCP/IP. A instalação também é bastante simples. O sistema de arquivos AFS – *Andrew File System* – é um outro sistema de arquivos em rede que está disponível em uma implementação gratuita, o OpenAFS [4], sobre o qual falaremos à página 49 desta edição.

Do outro lado, estão os sistemas de arquivos de cluster. Antes que os computadores possam acessar dados distribuídos, primeiro é necessário entrar no cluster. A configuração requer infraestruturas adicionais, tais como placas adicionais de I/O, um software de cluster e, é claro, uma configuração adequada. Sistemas de arquivos em cluster também são classificados pela forma como armazenam os dados. Aqueles baseados em discos compartilhados permitem que vários computadores leiam e escrevam na mesma mídia. O I/O é feito via do Fibre Channel (“SAN clássico”) ou TCP/IP (iSCSI). Os representantes mais populares no Linux são o OCFS2 e o GFS2 – *Global File System* [5].

Sistemas de arquivos de clusters paralelos são uma invenção mais recente. Eles distribuem dados pelos computadores no cluster por meio da distribuição de arquivos entre os nós de armazenamento. O Lustre [6] e o Ceph [7] são exemplos populares dessa tecnologia.

O conjunto de aplicativos de software para o OCFS2 compreende os pacotes `ocfs2-tools`, `ocfs2console` e os módulos do kernel `ocfs2-uname-r`. Digite o comando `ocfs2console` para abrir uma interface gráfica onde é possível criar a configuração do cluster e distribuí-lo entre os nós envolvidos (**figura 1**). No entanto, é possível fazer a mesma tarefa através do editor de texto `vi` e o comando `scp`. A **tabela 1**

lista as ações que a interface gráfica suporta e as ferramentas de linha de comando equivalentes. Depois de criar a configuração do cluster, o comando `/etc/init.d/o2cb` abre o subsistema (**listagem 2**).

O script de inicialização carrega módulos do kernel e define alguns padrões para o `heartbeat` e o `fencing`. Uma vez que o OCFS2 está sendo executado, o administrador

pode criar o sistema de arquivos do cluster. No caso mais simples, é possível usar `mkfs.ocfs2 devicefile` (**listagem 3**) para isso. O manual do `mkfs.ocfs` fornece uma lista completa de opções. As mais importantes são mostradas na **tabela 2**.

Depois de ter criado o sistema de arquivos, é preciso montá-lo. O comando `mount` funciona como nos sistemas de arquivos sem clusteres (**figura 2**). Ao montar e desmontar volumes OCFS2, um pequeno atraso é esperado: durante a montagem, a máquina de execução precisa se registrar no DLM. De forma semelhante, o DLM resolve os bloqueios existentes ou os gerencia nos demais sistemas em caso de `umount`. A documentação indica várias opções que podem ser usadas para a operação de montagem. Se o OCFS2 detectar um erro na estrutura de dados, ele irá para o padrão de somente leitura. Em determinadas situações, uma reinicialização da máquina pode resolver o problema. A opção de montagem `errors=panic` cuida disso. Outra opção interessante é `commit=seconds`. O valor padrão é 5, o que significa que o OCFS2 grava os dados no disco a cada cinco segundos. Se ocorrer uma falha, um sistema de arquivos consistente pode estar garantido – graças ao journaling (método que o sistema operacional utiliza para gravar logs antes de gravar efetivamente os dados no disco) – e apenas o trabalho dos últimos cinco segundos será perdido. A opção de montagem que especifica a forma como os dados são tratados para registro no journaling também é importante. A versão mais recente permite que o OCFS2 escreva todos os dados no disco antes de atualizar o journal.

Administradores de sistemas OCFS2 inexperientes podem ficar imaginando por que o volume OCFS2 não está disponível após a reinicialização, apesar de existir uma

### Listagem 1: Arquivo /etc/ocfs2/cluster.conf

```

01 node:
02 ip_port = 7777
03 ip_address = 192.168.0.1
04 number = 0
05 name = node0
06 cluster = ocfs2
07 node:
08 ip_port = 7777
09 ip_address = 192.168.0.2
10 number = 1
11 name = node1
12 cluster = ocfs2
13 cluster:
14 -node_count = 2

```

entrada no arquivo `/etc/fstab`. O script de inicialização que vem com a distribuição, `/etc/init.d/ocfs2`, faz a montagem OCFS2 resistente à reinicializações. Uma vez ativado, esse script busca entradas OCFS2 em `/etc/fstab` e integra esses sistemas de arquivos.

Assim como ocorre com o `ext3/4`, o administrador pode modificar algumas das propriedades do sistema de arquivos depois de montar o sistema de arquivos sem destruir os dados. A ferramenta `tunefs.ocfs2` ajuda muito neste sentido. Se o cluster cresce inesperadamente e são necessários mais computadores acessando o OCFS2 ao mesmo tempo, um valor muito pequeno para a opção `N` em `mkfs.ocfs2` pode se tornar um problema. A ferramenta `tunefs.ocfs2` permite alterar esses valores rapidamente. A mesma coisa se aplica ao tamanho do journal (**listagem 4**).

Além disso, é possível usar essa ferramenta para modificar o rótulo do sistema de arquivos e ativar ou desativar determinados recursos (**listagem 5**). Infelizmente, a página do manual não diz quais alterações são permitidas dinamicamente e quais não são. Assim, é possível encontrar uma mensagem como: *Trylock failedhou ao abrir o dispositivo /dev/sdal* ao tentar executar alguns comandos no OCFS2.

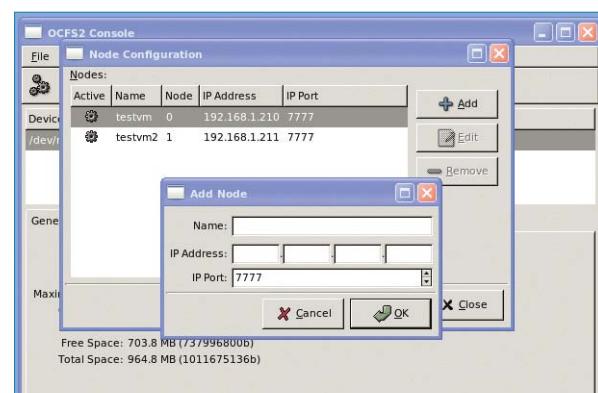
## Mais detalhes

Como dissemos, não é preciso pré-configurar o `heartbeat` ou o `fencing` do cluster. Quando a pilha do cluster é inicializada, os valores padrão são definidos para ambos. No entanto, é possível modificar os padrões para atender às suas necessidades. A abordagem mais fácil é através do script `/etc/init.d/o2cb/configure`, que solicita os valores necessários – por exemplo, quando o cluster OCFS2 considera um nó ou conexão de rede como parada. Ao mesmo tempo, é possível

especificar quando a pilha do cluster deve tentar restaurar a conexão e quando ela deve enviar um pacote `keep-alive`.

Com exceção do `timeout` do `heartbeat`, todos esses valores são informados em milissegundos. No entanto, para o `timeout` do `heartbeat`, é preciso um pouco de matemática para determinar quando o cluster deve considerar que um computador caiu. O valor representa o número de interações de dois segundos mais

um para o `heartbeat`. O valor padrão de 31 é, portanto, equivalente a 60 segundos. Em redes maiores é preciso aumentar todos estes valores para evitar alarmes falsos.



**Figura 1** Configuração de cluster com a ferramenta gráfica `ocfs2console`.

**Tabela 1: Diretórios em um repositório**

Função do sistema de arquivos	Menu na interface gráfica	Ferramenta em linha de comando
Montar	Mount	<code>mount.ocfs2</code>
Desmontar	Unmount	<code>umount</code>
Criar	Format	<code>mkfs.ocfs2</code>
Verificar	Check	<code>fsck.ocfs2</code>
Reparar	Repair	<code>fsck.ocfs2</code>
Alterar nome	Change Label	<code>tunefs.ocfs2</code>
Número máximo de nós	Edit Node Slot Count	<code>tunefs.ocfs2</code>

## Listagem 2: Inicializar o subsistema OCFS2

```

01 # /etc/init.d/o2cb online
02 Loading filesystem "configfs": OK
03 Mounting configfs filesystem at /sys/kernel/config: OK
04 Loading filesystem "ocfs2_dlmfs": OK
05 Mounting ocfs2_dlmfs filesystem at /dlm: OK
06 Starting O2CB cluster ocfs2: OK
07 #
08 # /etc/init.d/o2cb status
09 Driver for "configfs": Loaded
10 Filesystem "configfs": Mounted
11 Driver for "ocfs2_dlmfs": Loaded
12 Filesystem "ocfs2_dlmfs": Mounted
13 Checking O2CB cluster ocfs2: Online
14 Heartbeat dead threshold = 31
15 Network idle timeout: 30000
16 Network keepalive delay: 2000
17 Network reconnect delay: 2000
18 Checking O2CB heartbeat: Not active

```

Se OCFS2 se depara com um erro crítico, ele muda o sistema de arquivos para o modo somente leitura e gera um erro do tipo *kernel oops*, ou até mesmo um *kernel panic*.

No uso em produção, provavelmente vai ser preciso corrigir esse problema, sem análise de erros em profundidade (isto é, reiniciar o nó do cluster). Para que isso aconte-

ça, é preciso modificar o sistema operacional para que ele reinicie automaticamente no caso de um erro de kernel ([figura 3](#)). O melhor método para isso no Linux é alterar o sistema de arquivos em `/proc` para mudanças temporárias, ou então o `sysctl` se for preciso mudar algumas configurações para sobreviver a uma reinicialização.

Assim como qualquer outro sistema de arquivos, o OCFS2 tem alguns limites internos que precisam ser levados em consideração na concepção de armazenamento. O número de subdiretórios em um diretório é restrito a 32.000. O OCFS2 armazena os dados em clusters entre 4 e 1.024 KB. Como o número de endereços de cluster é restrito a 2<sup>32</sup>, o tamanho máximo do arquivo é 4 PB. Este limite é mais ou menos irrelevante, porque outra restrição – a utilização de journaling JBD – limita o tamanho máximo do sistema de arquivos OCFS2 a 16 TB, o que pode se referir a um máximo de 2<sup>32</sup> blocos de 4 KB.

Um cluster OCFS2 ativo usa vários processos para lidar com seu trabalho ([listagem 6](#)). Tarefas relacionadas com o DLM são manipuladas pelos processos `dlm_thread`, `dlm_reco_thread` e `dlm_wq`. Os processos `ocfs2cmt`, `ocfs2dc`, `ocfs2_wq` e `ocfs2rec` são responsáveis pelo acesso ao sistema de arquivos. Já os processos `o2net` e `o2hb-XXXXXXXXXX` lidam com as comunicações de clusters e os heartbeats.

Todos esses processos são iniciados e parados por scripts `init` próprios para o conjunto de clusters e o OCFS2.

O OCFS2 mantém seus arquivos de gerenciamento no diretório

```
# time mount -L data /cluster/
real    0m7.011s
user    0m0.000s
sys     0m0.008s
# █
```

**Figura 2** O processo de montagem do OCFS2.

### Listagem 3: OCFS2 otimizado para uso em servidores de emails

```
01 # mkfs.ocfs2 -T mail -L data /dev/sda1
02 mkfs.ocfs2 1.4.2
03 Cluster stack: classic o2cb
04 Filesystem Type of mail
05 Filesystem label=data
06 Block size=2048 (bits=11)
07 Cluster size=4096 (bits=12)
08 Volume size=1011675136 (246991 clusters) (493982 blocks) ↗
16 cluster groups (tail covers 8911 clusters, rest cover ↗
15872 clusters)
09 Journal size=67108864
10 Initial number of node slots: 2
11 Creating bitmaps: done
12 Initializing superblock: done
13 Writing system files: done
14 Writing superblock: done
15 Writing backup superblock: 0 block(s)
16 Formatting Journals: done
17 Formatting slot map: done
18 Writing lost+found: done
19 mkfs.ocfs2 successful
```

### Tabela 2: Opções importantes do `mkfs.ocfs2`

Opção	Finalidade
b	Tamanho do bloco
C	Tamanho do cluster
L	Label
N	Número máximo de computadores com acesso simultâneo
J	Opções de journal
T	Tipo do sistema de arquivos (otimização para vários arquivos pequenos ou alguns grandes)

### Listagem 4: Manutenção com o `tunefs.ocfs2`

```
01 # tunefs.ocfs2 -Q "NumSlots = %N\n" /dev/sda1
02 NumSlots = 2
03 # tunefs.ocfs2 -N 4 /dev/sda1
04 # tunefs.ocfs2 -Q "NumSlots = %N\n" /dev/sda1
05 NumSlots = 4
06 #
07 # tunefs.ocfs2 -Q "Label = %V\n" /dev/sda1
08 Label = data
09 # tunefs.ocfs2 -L oldata /dev/sda1
10 # tunefs.ocfs2 -Q "Label = %V\n" /dev/sda1
11 Label= oldata
```

de sistema de arquivos, que é invisível para os comandos normais como o `ls`. O comando `debugfs .ocfs2` deixa o diretório do sistema visível (**figura 4**). Os objetos no diretório do sistema são divididos em dois grupos: arquivos global e locais (ou seja, específico do nó). O primeiro desses grupos inclui `global_inode_alloc`, `slot_map`, `heartbeat` e `global_bitmap`. Eles têm acesso a cada nó do cluster e as inconsistências são evitadas por um mecanismo de trava. Os únicos programas que acessam `global_inode_alloc` são os que criam e ajustam o sistema de arquivos.

## Planejamento

Quando se planeja instalar o OCFS2, é preciso saber qual versão será usada na nova máquina. Embora o sistema de arquivos em si – isto é, a estrutura na mídia – seja compatível, operações mistas com o OCFS2 v1.2 e o OCFS2 v1.4 não são suportadas. O protocolo de rede é culpado por isso. Os desenvolvedores habilitaram uma *tag* na versão ativa do protocolo para que as futuras versões do OCFS2 sejam compatíveis através da pilha de rede. Isso acarreta a incompatibilidade com a versão 1.2. Por outro lado, os administradores têm um certo grau de flexibilidade na montagem de mídia OCFS2. Computadores com o OCFS2 v1.4 vão entender a estrutura de dados da versão 1.2 e montá-los sem nenhum problema. Isso também funciona ao contrário: se o volume OCFS2 v1.4 não usar os recursos mais recentes presentes na versão, é possível usar um computador com OCFS2 v1.2 para acessar os dados.

## Depuração

Um sistema de arquivos comum tem uma série de problemas em potencial e o grande grau de complexidade de um sistema de arquivos

## Listagem 5: Recursos para habilitar/desabilitar o OCFS2

```
01 # tuneefs.ocfs2 -Q "Incompatible: %H\n" /dev/sda1
02 Incompatibel: sparse inline-data
03 # tuneefs.ocfs2 --fs-features=nosparse /dev/sda1
04 # tuneefs.ocfs2 -Q "Incompatible: %H\n" /dev/sda1
05 Incompatibel: inline-data
06 # tuneefs.ocfs2 --fs-features=noinline-data /dev/sda1
07 # tuneefs.ocfs2 -Q "Incompatible: %H\n" /dev/sda1
08 Incompatibel: None
09 #
10 # tuneefs.ocfs2 --fs-features=sparse,inline-data /dev/sda1
11 # tuneefs.ocfs2 -Q "Incompatible: %H\n" /dev/sda1
12 Incompatibel: sparse inline-data
13 #
```

```
# echo 1 > /proc/sys/kernel/panic_on_oops
# echo 20 > /proc/sys/kernel/panic
#
#
# echo "kernel.panic_on_oops = 1" >> /etc/sysctl.conf
# echo "kernel.panic = 20" >> /etc/sysctl.conf
#
# █
```

**Figura 3** Reinicialização automática após 20 segundos, para erros no kernel.

## Listagem 6: Processos OCFS2

```
01 # ps -ef|egrep '[d]lm|[o]cf|[o]2'
02 root 3460 7 0 20:07 ? 00:00:00 [user_dlm]
03 root 3467 7 0 20:07 ? 00:00:00 [o2net]
04 root 3965 7 0 20:24 ? 00:00:00 [ocfs2_wq]
05 root 7921 7 0 22:40 ? 00:00:00 [o2hb-BD5A574EC8]
06 root 7935 7 0 22:40 ? 00:00:00 [ocfs2dc]
07 root 7936 7 0 22:40 ? 00:00:00 [dlm_thread]
08 root 7937 7 0 22:40 ? 00:00:00 [dlm_reco_thread]
09 root 7938 7 0 22:40 ? 00:00:00 [dlm_wq]
10 root 7940 7 0 22:40 ? 00:00:00 [ocfs2cmt]
```

## História

O OCFS2 é um sistema bastante jovem. Como o “2” no nome sugere, a versão atual está melhorada. A Oracle desenvolveu o antecessor, o OCFS, para uso em *Real Application Clusters*, voltado para bancos de dados Oracle. O novo OCFS2 é projetado para atender as exigências de um sistema maduro capaz de armazenar dados arbitrários. Compatibilidade POSIX e o típico – e necessário – desempenho exigido para bancos de dados são outros critérios. Após dois anos de desenvolvimento, foi lançada a versão 1.0 do OCFS2, mas ele foi incluído no kernel básico (2.6.16) apenas um ano depois. A versão 1.2 tornou-se mais generalizada, com um grande suporte para várias distribuições Linux Enterprise. O OCFS2 está disponível para os principais sistemas operacionais do mundo Linux há algum tempo. Isso se aplica às variantes comerciais, tais como SLES, RHEL, ou Oracle EL, e para os sistemas gratuitos Debian, Fedora e openSUSE. Dependendo da versão do kernel, os usuários podem utilizar a versão 1.4, que foi lançada em 2008, ou a versão 1.2, que é dois anos mais velha.

em cluster não ajuda. Do ponto de vista do OCFS2, as coisas podem dar errado em três camadas diferentes – a estrutura do sistema de arquivos no disco, a configuração

de cluster ou a infraestrutura do cluster – ou mesmo uma combinação dos três. A infraestrutura do cluster inclui a pilha de rede para os heartbeats, comunicações de

cluster e, possivelmente, acesso à mídia. Problemas com o *Fibre Channel* – FC e o iSCSI também pertencem a este grupo.

Para problemas com a infraestrutura do cluster, é possível solucionar como se se tratasse de uma rede comum, FC ou iSCSI. Problemas também podem ocorrer se a configuração do cluster não for idêntica em todos os nós. Usando o editor `vi`, o comando `scp` e a sequência `md5sum`, é possível verificar e resolver o problema. A alternativa – assumindo-se que a infraestrutura de cluster está instalada e funcionando – é sincronizar a configuração do cluster em todos os seus computadores, atualizando a configuração com o `ocfs2console`.

Deixar o volume OCFS2 problemático offline pode ajudar – isto é, desmontá-lo e reiniciar o serviço de cluster em todos os seus computadores usando o comando `/etc/init.d/o2cb/restart`. É possível até mesmo mudar o sistema de arquivos para uma espécie de modo de usuário único com `tunefs.ocfs2`.

Para isso, é preciso mudar o tipo de montagem de cluster para local. Após fazer isso, só um único computador pode montar o sistema, e ele não precisa da pilha de cluster para fazê-lo. Em todas essas ações, é preciso estar ciente de que o sistema de arquivos pode ser montado por mais de um computador. Algumas ações que envolvem, por exemplo, `tunefs.ocfs2`, não irão funcionar se outro computador acessar o sistema de arquivos ao mesmo tempo.

O exemplo da [listagem 7](#) mostra o usuário tentando modificar o rótulo do sistema. Esse processo falha, embora o sistema esteja *offline* (no computador). Nesse caso, o `mounted.ocfs2` vai ajudar: ele verifica o cabeçalho OCFS2 para identificar o computador que está online com o sistema de arquivos. Os dados mais

```
debugfs: ls -l //
  8      drwxr-xr-x   6  0  0  2048 11-Apr-2010 20:19 .
  8      drwxr-xr-x   6  0  0  2048 11-Apr-2010 20:19 ..
  9      -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 bad_blocks
 10     -rw-r--r--   1  0  0  411792 11-Apr-2010 20:19 global_inode_alloc
 11     -rw-r--r--   1  0  0  4096 11-Apr-2010 20:19 slot_map
 12     -rw-r--r--   1  0  0  524288 11-Apr-2010 20:19 heartbeat
 13     -rw-r--r--   1  0  0  1011675136 11-Apr-2010 20:19 global_bitmap
 14     -rw-r--r--   2  0  0  2048 11-Apr-2010 20:19 orphan_dir:0000
 15     -rw-r--r--   2  0  0  2048 11-Apr-2010 20:19 orphan_dir:0001
 16     -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 extent_alloc:0000
 17     -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 extent_alloc:0001
 18     -rw-r--r--   1  0  0  4194304 11-Apr-2010 20:19 inode_alloc:0000
 19     -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 inode_alloc:0001
 20     -rw-r--r--   1  0  0  67108864 11-Apr-2010 20:19 journal:0000
 21     -rw-r--r--   1  0  0  67108864 11-Apr-2010 20:19 journal:0001
 22     -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 local_alloc:0000
 23     -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 local_alloc:0001
 24     -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 truncate_log:0000
 25     -rw-r--r--   1  0  0  0 11-Apr-2010 20:19 truncate_log:0001
 26     drwxr-xr-x   2  0  0  2048 11-Apr-2010 20:49 orphan_dir:0002
 27     drwxr-xr-x   2  0  0  2048 11-Apr-2010 20:49 orphan_dir:0003
 28     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 extent_alloc:0002
 29     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 extent_alloc:0003
 30     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 inode_alloc:0002
 31     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 inode_alloc:0003
 32     -rw-r--r--   1  0  0  67108864 11-Apr-2010 20:49 journal:0002
 33     -rw-r--r--   1  0  0  67108864 11-Apr-2010 20:49 journal:0003
 34     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 local_alloc:0002
 35     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 local_alloc:0003
 36     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 truncate_log:0002
 37     -rw-r--r--   1  0  0  0 11-Apr-2010 20:49 truncate_log:0003
debugfs: 
```

**Figura 4** Os metadados do OCFS2 são armazenados em arquivos invisíveis ao comando `ls`. Eles podem ser listados com o comando `debugfs.ocfs2`.

## Opções do OCFS2

Os administradores de sistemas irão encontrar basicamente duas versões do OCFS2: a versão 1.2 ou a 1.4. Com relação à estrutura de dados no disco, as duas versões são compatíveis, porém, isso significa ter que passar sem os recursos mais recentes da versão 1.4. A documentação enumera 10 diferenças significativas entre as versões 1.2 e 1.4. A [tabela 3](#) relaciona as mais interessantes delas. Não importa qual versão será escolhida, mas algumas coisas exigem atenção. O `mkfs.ocfs2` fornecido pela versão 1.4 habilita automaticamente todos os novos recursos, efetivamente impedindo que máquinas com o OCFS v1.2 acessem o sistema de arquivos. Para mudar isso, use o `tunefs.ocfs2` para desativar as novas funções ([listagem 8](#)). Uma abordagem mais simples é criar o sistema de arquivos com a opção `--fs-feature-level=max-compat`, assim, o `tunefs.ocfs2` ajudará o administrador a migrar da versão 1.2 para a 1.4 sem problemas.

**Tabela 3: Novos recursos do OCFS2 versão 1.4**

Recurso	Descrição
Modo de journal ordenado	O OCFS2 escreve os dados antes dos metadados
Alocação flexível	O OCFS2 suporta arquivos <code>sparse</code> – isto é, lacunas nos arquivos. Além disso, a pré-alocação de <code>extents</code> é possível
Dados inline	O OCFS2 armazena os dados de pequenos arquivos diretamente no inode e não em extents
Clustered flock()	A chamada de sistema <code>flock()</code> possui capacidade de trabalhar ou funcionar em modo cluster

importantes da estrutura do sistema de arquivos estão contidos no superbloco. Assim como outros sistemas de arquivos Linux, o OCFS2 cria cópias de backup do superbloco, no entanto, a abordagem usada pelos desenvolvedores do OCFS2 é um pouco incomum.

O OCFS2 cria um máximo de seis cópias em *offsets* não-configuráveis: 1, 4, 16, 64 e 256 GB e 1 TB. Nem é preciso dizer que volumes OCFS2 menores do que 1 GB não têm uma cópia do superbloco. Para ser justo, o `mkfs.ocfs2` mostra isso quando o sistema de arquivos é gerado.

Um efeito colateral desse backup de superblocos estático é que é possível fazer referência a eles pelos números durante uma verificação no sistema de arquivos. O exemplo da [listagem 8](#) mostra um superbloco primário danificado que está impedindo a montagem e o funcionamento do `fsck.ocfs2` simples. O primeiro backup torna possível a restauração.

## Conclusão

No geral, é fácil configurar um cluster OCFS2. O software está disponível em várias distribuições Linux. O OCFS2 funciona muito bem com iSCSI e Fibre Channel, por isso a parte do hardware não é muito difícil. A configuração de um conjunto de cluster é uma tarefa bastante simples que pode ser feita com ferramentas simples como o editor `vi`.

Embora o OCFS2 não inclua tecnologias sofisticadas de fencing quando comparado com outros sistemas de arquivos de cluster, o fencing não é necessário em muitas áreas. A falta de um gerenciador de volumes com capacidade de cluster facilita a imersão no mundo do OCFS2. Já que o OCFS2 é mais simples e menos complexo que outros sistemas de arquivos de cluster, vale a pena investigá-lo. ■

## Listagem 7: Depuração com mounted.ocfs2

```
01 # grep -i ocfs /proc/mounts |grep -v dlm
02 # hostname
03 testvm2.seidelnet.de
04 # tunefs.ocfs2 -L olldata /dev/sda1
05 tunefs.ocfs2: Trylock failed while opening device "/dev/
06 sda1"
07 # mounted.ocfs2 -f
08 Device FS Nodes
09 /dev/sda1 ocfs2 testvm
10 #
```

## Listagem 8: Restauração de superblocos OCFS2 corrompidos

```
01 # mount /dev/sda1 /cluster/
02 mount: you must specify the filesystem type
03 # fsck.ocfs2 /dev/sda1
04 fsck.ocfs2: Bad magic number in superblock while opening ↵
"/dev/sda1"
05 # fsck.ocfs2 -r1 /dev/sda1
06 [RECOVER_BACKUP_SUPERBLOCK] Recover superblock
07 information from backup block#262144? <n> y
08 Checking OCFS2 filesystem in /dev/sda1:
09 label: backup
10 uuid: 31 18 de 29 69 f3 4d 95 a0 99 a723 ab 27 f5 04
11 number of blocks: 367486
12 bytes per block: 4096
13 number of clusters: 367486
14 bytes per cluster: 4096
15 max slots: 2
16 /dev/sda1 is clean. It will be checked after 20 ↵
additional mounts.
```

## Mais informações

- [1] OCFS2: <http://oss.oracle.com/projects/ocfs2/>
- [2] DRBD: <http://www.drbd.org/>
- [3] First NFS RFC: <http://tools.ietf.org/html/rfc1094/>
- [4] OpenAFS: <http://www.openafs.org/>
- [5] GFS: <http://sources.redhat.com/cluster/gfs/>
- [6] Lustre: <http://wiki.lustre.org/>
- [7] Ceph: <http://ceph.newdream.net/>

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lnm.com.br/article/4454>



NFS e segurança

CAPA

# Armazenamento com segurança

O NFS é o sistema de arquivos de rede clássico do Linux. Este artigo apresenta o NFSv4 e suas funções de segurança.

por Thorsten Scherf



Chris Quirinell-Brock - sxc.hu

A ideia por trás do NFS é relativamente simples: quando diversos computadores trabalham em rede, é interessante designar um deles como o servidor de arquivos. Ele ocupa o lugar do armazenamento central para os clientes, que precisam apenas montá-lo num diretório local. Isto permite que os dados importantes sejam armazenados todos juntos e com maior segurança. O benefício para os clientes é ter de buscar em menos locais e, para o administrador, poder concentrar as atividades de backup do servidor de arquivos em um único local. Os usuários, na melhor das hipóteses (isto é, total disponibilidade do servidor de arquivos), nem sequer perceberão que estarão trabalhando com dados remotos.

## Perto e longe

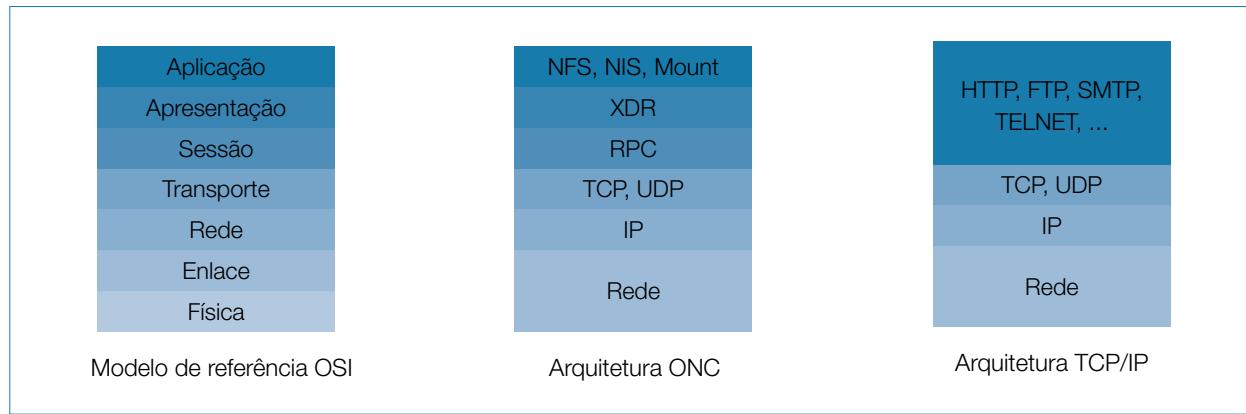
No uso do NFS, os usuários não notam qualquer diferença entre arquivos armazenados localmente e aqueles

acessados via NFS. Por trás dos panos, no entanto, há uma importante diferença: arquivos armazenados localmente, que residem em blocos gerenciados por um sistema de arquivos, precisam ser encontrados pelos programas por meio de *inodes*. Essas estruturas armazenam, além dos blocos de dados, informações sobre cada arquivo, como seu número único, o tamanho do arquivo, permissões de acesso e *timestamps* (data e hora). Tais informações podem ser acessadas por meio do comando `stat <nome_do_arquivo>`.

Porém, a operação em arquivos remotos é realizada pelo servidor, em nome do cliente. O computador remoto (cliente) acessa o arquivo desejado no servidor por meio de um manipulador de arquivo recebido do servidor, sob demanda. Juntamente com o manipulador, é possível efetuar qualquer uma das 18 operações oferecidas como parte do serviço de um servidor NFS.

## Diversidade de protocolos

Quando a Sun apresentou o NFS ao mercado em 1984, ela publicou também uma grande coleção de documentos relacionados, sob o nome de ONC – *Open Network Computing*. A figura 1 mostra a arquitetura do ONC em comparação com outros modelos, que dependem apenas do TCP/IP. No modelo ONC, o NFS está junto a outros protocolos da camada de aplicação. Isto inclui o protocolo para bloquear arquivos com NLM – *Network Lock Manager* e NSM – *Network Status Monitor*. A tarefa do protocolo XDR – *External Data Representation* está uma camada abaixo destes, realizando a conversão dos dados para um formato uniforme antes da transmissão. Isto permite o processamento dos dados independente no hardware e no sistema operacional. Novamente, uma camada mais profunda é o



**Figura 1** No modelo do ONC, o sistema de arquivos de rede localiza-se na camada de aplicação (camada 7 OSI) e o XDR fica na camada 6. O modelo TCP/IP clássico unifica as camadas 5 a 7.

protocolo RPC – *Remote Procedure Call* [1]. Com o uso do RPC, funções de outros programas em computadores remotos podem acessar dados remotos.

## Serviços

Todo programa que deseja utilizar as funções via RPC precisa se registrar em um serviço especial, o *Portmapper*. O Portmapper funciona como intermediário: ele coleta as ofertas de serviços – incluindo informações de logs e portas dinâmicas para contato no banco de dados – e os retorna aos clientes quando é solicitado. A figura 2 ilustra esse processo.

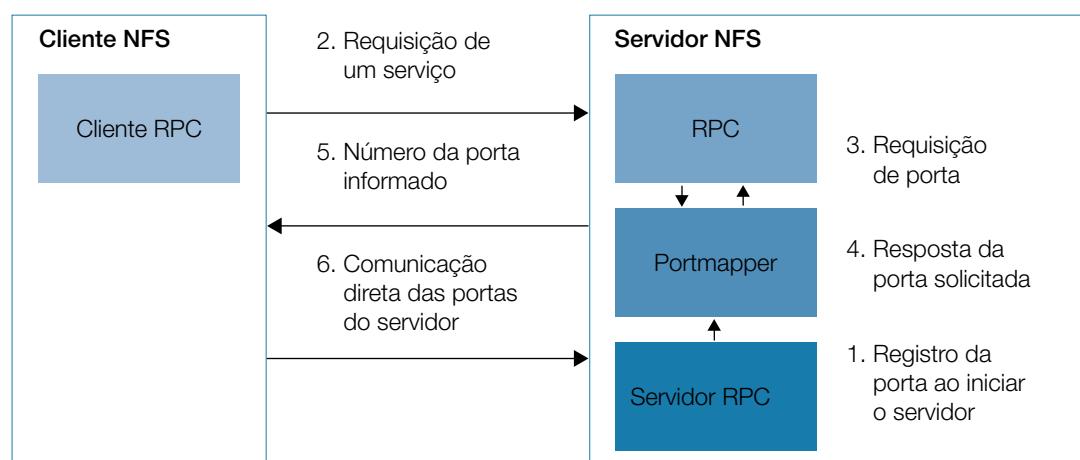
Principalmente as versões mais antigas do *portmapper* podem facilmente expor problemas de segurança. As mais recentes ao menos se comprometem a reduzir esse incômodo, respondendo somente na rede local. Esta configuração, definitivamente, é aconselhável. As entradas usam o formato *portmap: hosts* no arquivo */etc/hosts.deny* e */etc/hosts.allow*. Para saber quais programas são de conhecimento do *portmapper*, use o comando *rpcinfo -p*.

## Trabalho em equipe

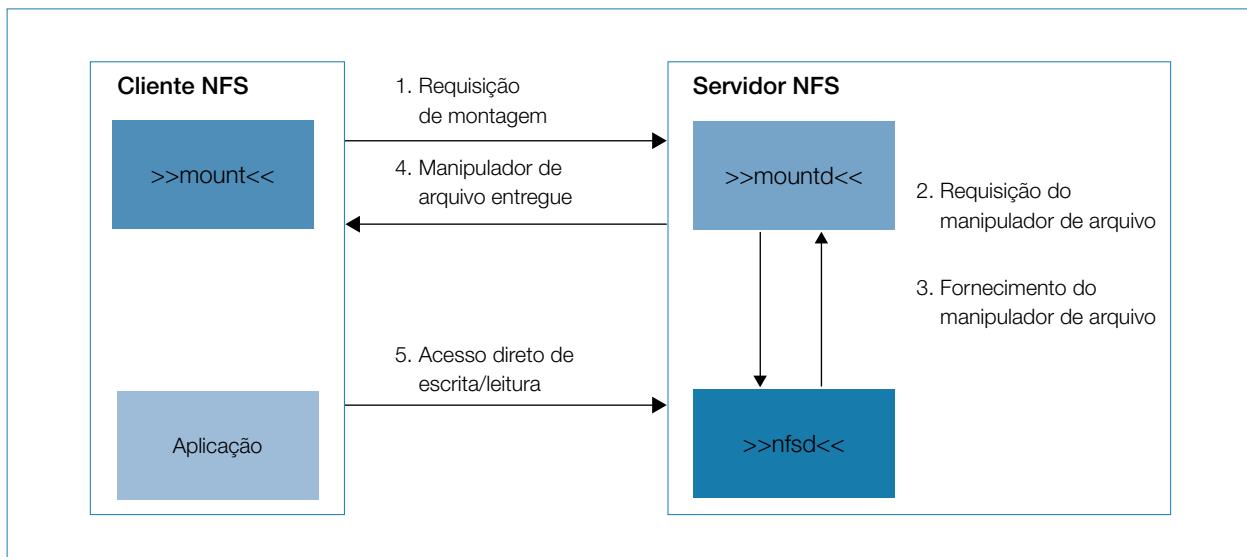
O trabalho do servidor NFS geralmente é realizado em conjunto pelo *mountd* e pelo *nfsd*. O primeiro

*daemon* verifica as requisições de montagem dos clientes com relação à sua possibilidade, e o último essencialmente inicia várias *threads* de kernel que tomam para si as operações do NFS. Opcionalmente, há suporte ao *daemon rquotad*. Ele monitora os níveis de uso do disco por usuário. Normalmente, os scripts de inicialização *nfs* ou *nfsserver* já carregam esses serviços. Dependendo da distribuição, a versão do NFS e do kernel pode ter dois *daemons* para bloquear – *lockd* e *statd* – que são iniciados separadamente.

Para verificar se todos os serviços estão funcionando corretamente,



**Figura 2** O portmapper atua como contato entre o servidor RPC e o cliente. O cliente pede a porta pela qual pode se conectar diretamente ao servidor.



**Figura 3** No pedido de montagem, o cliente recebe um manipulador de arquivo, que é enviado ao daemon NFS juntamente com as operações (como leitura e gravação).

confira a saída dos comandos `ps -A | grep rpc` e `ps -A | grep nfs`.

Nas distribuições atuais, o *daemon* NFS é parte do kernel. A saída do comando `lsmod | grep nfs` deve conter os seguintes módulos para que o servidor NFS funcione:

nfsd	196624	9
exportfs	4992	1 nfsd

lockd	60008	2 nfsd
nfs_acl	3584	1 nfsd
sunrpc	130364	9 ↵
		nfsd,lockd,nfs_acl

Além do `nfsd` na forma de um módulo de kernel, há também uma versão executada completamente no espaço do usuário. Seu desempenho é muito pior do que o do módulo do

kernel e não segue as determinações do *Network Status Manager* – NSM e do *Network Lock Manager* – NLM, nem permite arquivos maiores que 2 GB.

## Serviços

O importador de dados do NFS pode conter uma lista de clientes – além do caminho local – e precisa ser exportado pelo servidor para ser acessado. As configurações para tal estão no arquivo `/etc/exports`, e são lidas pelo `mountd` e pelo `nfsd`. Com o comando `exportfs`, também é possível exportar diretórios temporariamente através do comando `exportfs -o ro, sync server1.example.com /var/ftp/pub`. Uma execução subsequente de `exportfs -u` inverte os compartilhamentos: `exportfs -u server1.example.com:/var/ftp/pub`.

Os compartilhamentos ativos no servidor NFS são exibidos pelo comando `showmount`. No caso do computador Tiffy, o comando `showmount -e tiffy` retornaria:

```
Export list for tiffy: /var/ftp ↵
/pub/rhel4-es 192.168.0.0/255.255.255.0 ↵
5.255.0.
```

O `showmount` de fato exibe os diretórios exportados e os clientes capazes

### Listagem 1: Arquivo /etc/idmapd.conf

```
01 [General]
02
03 Verbosity = 0
04 Pipefs-Directory = /var/lib/nfs/rpc_pipefs
05 Domain = example.com
06
07 [Mapping]
08
09 Nobody-User = nfsnobody
10 Nobody-Group = nfsnobody
```

### Listagem 2: Arquivo /etc/exports para NFSv4

```
01 # NFSv4
02 /documentos gss/krb5(sync,rw,fsid=0,insecure,no_subtree_check,↪
anonuid=65534,anongid=65534)
03
04 # NFS3
05 /documentos 192.168.0.0.0/255.255.255.0(sync,rw,nohide,insecure,↪
no_subtree_check,anonuid=65534,anongid=65534,no_root_squash)
```

## Quadro 1: Opções de montagem

- ▶ **rw, ro:** permissões de leitura e escrita ou apenas escrita. É importante que os direitos sejam mais restritivos, isto é, um compartilhamento somente-leitura no servidor não deve ser aberto para gravação localmente; da mesma forma, um compartilhamento só deve receber permissão de escrita se também a tiver localmente.
- ▶ **fg:** cada processo de montagem gera uma mensagem de erro em caso de falha, e o processo é executado em primeiro plano.
- ▶ **bg:** em caso de falhas na operação de montagem, ela será tentada novamente em segundo plano até ter sucesso ou o **rsize** ser alcançado.
- ▶ **retrans=número:** número de tentativas de montagem. O valor padrão é 5.
- ▶ **hard:** caso um programa trave durante o acesso a um diretório NFS, o servidor é reiniciado. Após o reinício, o programa prossegue em seu processamento. Um programa travado somente pode ser interrompido se a opção **intr** for especificada.
- ▶ **soft:** caso o servidor não responda durante um período especificado, o kernel gera um erro e os processos em espera no servidor são informados. O intervalo de tempo entre as tentativas pode ser definido com o parâmetro **timeo=segundos**.
- ▶ **ntr, nointr:** permite ou proíbe que uma ação suspensa de um cliente seja executada por meio de uma combinação de teclas.
- ▶ **remount:** desmontar um diretório e remontá-lo imediatamente. Costuma ser usado para testar novas configurações.
- ▶ **suid, nosuid:** bits SUID podem ou não ter acesso ao sistema de arquivos montado.
- ▶ **retry=número:** número de tentativas de montagem sem sucesso (o padrão é 10000) até o sistema desistir da montagem.
- ▶ **wsize=tamanho:** define o tamanho de bloco em bytes ao escrever via NFS. O padrão é 1024, mas deve ser alterado para 8192.
- ▶ **rsize=tamanho:** define o tamanho de bloco em bytes ao ler via NFS. O padrão é 1024, mas deve ser alterado para 8192.
- ▶ **timeo=número:** intervalo entre repetições, em décimos de segundo.
- ▶ **proto=protocolo:** especifica o protocolo (UDP ou TCP).

de acessá-los, mas não oferece um panorama das opções de exportação. Estas são encontradas no servidor, no arquivo `/var/lib/nfs/etab`:

```
/var/ftp/pub/rhel4-es
192.168.0.0/255.255.255.0(ro, sync, wdelay, hide, nocrossmnt, secure,
root_squash,no_all_squash,subtree_check,secure_locks,anonuid=-2,anongid=-2)
```

## Números em vez de nomes

O gerenciamento interno de usuários em sistemas Linux não se baseia em nomes de usuários ou grupos, mas em IDs. Se um arquivo em um servidor NFS pertencer ao usuário *tscherf* com UID 500 e possuir permissão de leitura e gravação, e

esse arquivo for importado por um cliente remoto, o usuário do cliente remoto que possuir UID 500 terá os mesmos direitos que o usuário *tscherf* sobre o arquivo. Para tornar esse problema, defina um sistema de gerenciamento de usuários centralizado, como o LDAP ou NIS. Para o usuário *root*, no entanto, não é esta a solução.

Uma solução é o chamado *squashing*. A opção `root_squash` nas configurações de `exports` significa que qualquer acesso de usuário *root* remoto será feito, localmente, sob o usuário *nobody* ou *nfsnobody*. Com a opção `all_squash`, todas as requisições de qualquer usuário remoto serão realizadas localmente como *nobody* ou *nfsnobody*. Quando um cliente

## Quadro 2: Como funciona o Kerberos

A [figura 5](#) mostra o funcionamento do Kerberos. O cliente estabelece uma conexão com um KDC – *Key Distribution Center*. Isto é feito de forma transparente para o usuário por meio do programa de login ou com uso do `krb5`. O KDC é composto por duas partes: um servidor de autenticação (*Authentication Server*, ou AS) e um *Ticket Granting Server* (TGS). O servidor de autenticação recebe a requisição do cliente e verifica seu espaço de nome (*Realm*) em busca do nome de usuário fornecido (*User-Principal*). Se o principal estiver no banco de dados do Kerberos, o AS cria uma chave de sessão aleatória e um chamado *Ticket Granting Ticket* (TGT). O TGT contém várias informações que incluem o nome e o IP do cliente, um período de validade, uma marca de hora e a nova chave de sessão recém-gerada.

## Quadro 3: TGT

O TGT – *Ticket Granting Ticket* é criptografado com uma chave que somente o AS e o TGS conhecem. Juntamente com a chave de sessão recém-gerada, o cliente recebe este ticket: evidentemente não em texto puro, mas criptografado com uma chave derivada da senha do cliente. Após o cliente receber a resposta do AS (TGT criptografado e chave de sessão), é pedida a senha ao usuário. Isto converte a senha do Kerberos numa chave DES. Este procedimento também é usado para decodificar os TGTs recém-recebidos. O cliente armazena o TGT em seu cache de credenciais e apaga da memória a senha digitada. Usando o TGT, o usuário utiliza a validade do ticket para provar sua identidade, mas ainda sem usar uma senha para se autenticar.

acessa um arquivo compartilhado, toda uma cadeia de procedimentos é executada no segundo plano.

## Cadeia de processos

Em seguida, o cliente precisa requisitar acesso ao servidor NFS para determinar quais portas permitem acessar o `mountd` e o `nfsd`. Estas informações são obtidas com o `portmapper`. Se ele desejar editar o arquivo de forma exclusiva, também serão necessários os endereços do `lockd` e do `statd`.

Na etapa seguinte, o cliente utiliza os mesmos números de porta requisitados, agora para se conectar diretamente ao `mountd` no servidor. Esta ação consulta o arquivo `/var/lib/nfs/etab` para verificar se o diretório pedido está exportado e se o cliente pode acessá-lo. Se ambos os testes forem positivos, o `mountd` recebe do `nfsd` um manipulador de arquivo que permite acesso ao arquivo requisitado pelo cliente. O manipulador envia o `mountd` de volta ao cliente requisitante. Agora, ele já pode li-

dar diretamente com as instruções enviadas ao `nfsd` e enviar pedidos para ler, gravar ou apagar dados. O processo completo é mostrado na **figura 3**. O comando `mount` é usado para integrar o diretório ao sistema de arquivos local. Um exemplo seria:

`mount -t nfs -o ro tiffy:/var/ftp/pub/rhel4-es/ /mnt/daten/`

Para isso, o ponto de montagem local precisa existir. Uma lista dos diretórios exportados pelo servidor pode ser visualizada pelo cliente com o comando `showmount -w`.

Para montar automaticamente um sistema de arquivos NFS remoto, é preciso informá-lo no arquivo `/etc/fstab`. Uma outra possibilidade é usar o `automount`. Ele inicia o processo de montagem assim que o ponto de montagem local é acessado. Sua configuração se localiza no arquivo `/etc/auto.master`, assim como em `/etc/auto.misc`. Os parâmetros de montagem possíveis estão no **quadro 1**.

## Direitos exclusivos

Em um sistema de arquivos distribuí-

do, múltiplos clientes podem acessar simultaneamente o mesmo arquivo. Em geral, é interessante evitar essas ações problemáticas por arquivo ou por partes dele. No Linux, esse objetivo é coberto pelo kernel – na camada de chamada de sistema `fcntl()` (*File Control*, ou controle de arquivo).

Se um cliente desejar acesso exclusivo a um arquivo, deve enviar esse pedido ao kernel. Se o arquivo a ser bloqueado for localizado num compartilhamento NFS, o kernel repassa o pedido ao *Network Lock Manager* (NLM, `rpc.lockd`). Deste ponto, o pedido segue para o `lockd` do servidor NFS, que o processa e envia o resultado de volta ao NLM do cliente. Com isso, o kernel finalmente pode terminar o processamento desse pedido. A condição para que isso tudo funcione é que o NLM esteja em execução tanto no cliente quanto no servidor.

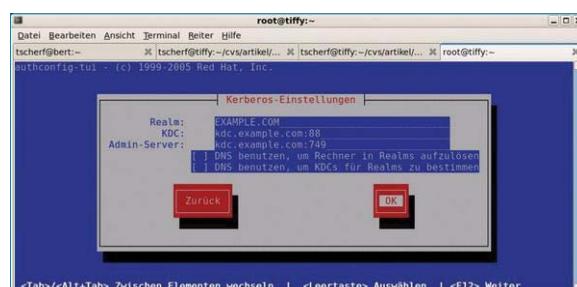
Quando o cliente ou o servidor é reiniciado, o *Network Status manager* (NSM, `rpc.statd`) entra em ação. Caso o `lockd` do servidor tenha bloqueado algum arquivo, essa informação será repassada ao NSM e o diretório `/var/lib/nfs/sm` receberá o nome do cliente. No lado cliente, será informado o nome do servidor que realizou o bloqueio. Novamente, o responsável por isso é o NSM do cliente.

Agora, se um cliente cair, o *Network Status Monitor* do servidor será contactado e a informação encaminhada ao NLM. Isto acende a luz vermelha. Se o servidor cair, ocorre o mesmo no outro sentido. Os clientes serão informados e, após o servidor reiniciar, poderão refazer e atualizar seus pedidos de bloqueio. Se nenhum pedido de atualização for feito, os bloqueios抗igos serão liberados.

Um problema é o uso de bloqueios de arquivos em ambientes de cluster. Como as informações de bloqueio são armazenadas em arquivos locais e estes não são copiados em casos de *failover*, os bloqueios ficam indisponíveis.

## NFSv4

Na versão 4 [2], o NFS suporta, além da autenticação `AUTH_SYS` com base unicamente em dados de UID/GID, a autenticação via Kerberos `RPCSEC_GSS`.



**Figura 4** A ferramenta authconfig-tui permite adicionar as informações necessárias para a autenticação.

[3]. O resultado é não apenas uma autenticação segura dos clientes que acessam o servidor, mas também a criptografia e a proteção de integridade dos dados transmitidos. Em geral, o NFS4 utiliza a autenticação com Kerberos juntamente com LDAP para gerenciamento centralizado de usuários. Este artigo pressupõe, portanto, a existência da administração centralizada de usuários com LDAP no servidor. Para mais informações sobre o Kerberos, confira o [quadro 2](#).

## Configuração do servidor

Para que o servidor LDAP consiga autenticar seus usuários via Kerberos, é preciso preencher alguns critérios. O primeiro é ter um principal Kerberos no servidor LDAP; o jeito mais fácil é por meio de um arquivo `kadmin.local` no servidor LDAP. Com isso, pode-se adicionar um principal com `add_principal -randkey ldap /ldap.example.com` e armazená-lo no arquivo `/etc/openldap/ldap.keytab` com `ktadd -k /etc/openldap/ldap.keytab 1dap@ldap.example.com`.

Para o servidor LDAP saber onde encontrar o arquivo de `keytab` na inicialização do sistema, basta informar isso no arquivo `/etc/sysconfig/ldap`. Inclua nele a diretiva `export KRB5_KT_NAME=/etc/open-ldap/ldap.keytab`. Após uma reinicialização do servidor, a autenticação por LDAP já deve ser possível. A forma mais fácil de testar isso é com a ferramenta `ldapsearch`. O cliente se autenticará automaticamente usando o protocolo Kerberos.

Para utilizar o NFS com autenticação por Kerberos, ative em `/etc/sysconfig/nfs` a variável `SECURE_NFS`:

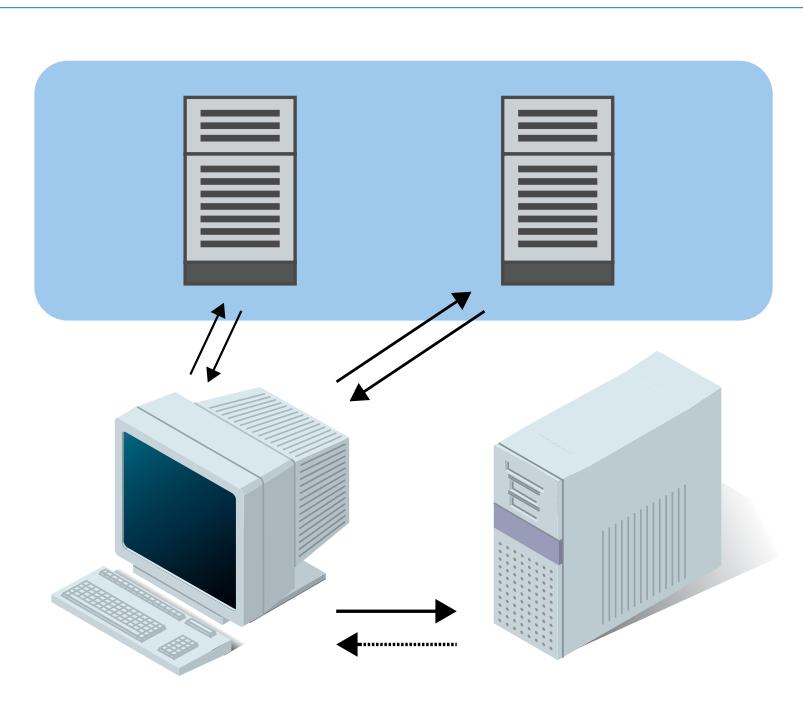
```
# Esta linha deve ser "yes" se você utilizar RPCSEC_GSS_KRB5
# (auth=krb5,krb5i, ou krb5p)
SECURE_NFS="yes"
```

## Quadro 4: Tickets de serviço

A estação verifica a autenticidade do usuário com o TGT. Porém, se ele desejar acessar algum outro serviço de rede, como NFS, precisará pedir novamente um ticket ao KDC, desta vez do TGS. Este ticket de serviço (ST – Service Ticket) é responsável por exatamente um serviço – aquele para o qual foi pedido. Uma requisição de ticket de serviço é muito mais complexa: o cliente envia uma requisição para o TGS. Esta requisição inclui o nome do serviço que o cliente deseja acessar, chama um autenticador e armazena o TGT. O autenticador consiste de: nome do cliente, seu endereço IP e informações de hora (hora atual do cliente).

O TGT é criptografado com o autenticador e, juntos, são enviados ao TGS. O autenticador é criptografado juntamente com a chave da sessão enviada pelo TGT. O TGS decodifica o autenticador e o endereço do TGT e compara seu conteúdo, o IP do cliente requisitante e a hora atual. Se tudo se encaixar, o KDC gera uma nova chave de sessão, que o cliente e o servidor envolvido (neste caso, o servidor NFS) usarão no futuro. A chave desta sessão é parte dos tickets de serviço, que agora são emitidos pelo TFS e criptografados (com a chave de sessão do TGT) para o cliente requisitante. E assim o jogo recomeça.

O cliente recebe o ticket de serviço e o entrega ao servidor desejado (NFS) para continuar provando sua identidade. Além do ticket de serviço, é gerado um novo autenticador, e ambos são enviados ao servidor. Se todas as informações do ticket de serviço e do autenticador coincidirem, o cliente é classificado como real e aceito, sem precisar informar novamente um nome de usuário e uma senha para se autenticar. O autenticador protege contra o *sniffing* de rede, interceptações de tickets de serviço e servidores forjados. Este procedimento é chamado de *replay attack*. Para ocorrer sem problemas, todos os sistemas participantes precisam ter a mesma hora definida. Isto é fácil de proporcionar por meio do *Network Time Protocol*.



**Figura 5** Funcionamento do Kerberos.

```
# Esta entrada define o número de processos do servidor NFS. 8 é o padrão
RPCNFSDCOUNT=8
```

Dependendo da distribuição, o nome da variável pode mudar um pouco. A próxima etapa é atualizar o sistema para ter sempre a biblioteca mais recente (atualmente, `libgssapi_krb5.so`). Geralmente, este valor já está corretamente informado no arquivo `/etc/gssapi_mech.conf`. No arquivo `/etc/idmapd.conf`, configure o mapeamento entre UIDs e nomes de usuários. Esse serviço também precisa estar em execução no cliente, assim como no servidor. O arquivo de configuração é mostrado na **listagem 1**.

No arquivo `/etc(exports`, informe os compartilhamentos normalmente. A **listagem 2** mostra um exemplo.

Na primeira linha encontram-se todos os usuários do Kerberos autenticados que têm permissão para acessar o compartilhamento. A segunda linha também permite que clientes NFSv3 accessem o compartilhamento.

## Cientes

Cada cliente precisa de um principal. Isto é feito pelo administrador com a chamada a `kadmin.local` no cliente e o comando `add_principal -randkey host/client.example.com`. Em seguida ele grava no arquivo de `keytab` com `ktadd -k host/client.example.com`. Se os clientes NFS já estiverem configurados para usar o LDAP para autenticação, basta usar o `authconfig-tui` para fornecer as informações do Kerberos. A **figura 4** mostra uma entrada correspondente.

Se o cliente não estiver configurado para autenticação por LDAP, isto também pode ser feito pelo `authconfig-tui`. Em seguida, inicie (como `root`) o `daemon` com o comando `/etc/init.d/rpcgssd start`.

Agora, com o comando `mount`, já é possível montar os compartilhamentos

## Quadro 5: Servidor Kerberos

O servidor Kerberos contém o banco de dados propriamente dito no qual os *principals* (contas principais) são armazenados. Esse servidor precisa ser especialmente protegido e não deve oferecer outros serviços. Existem *principals* para usuários e para serviços baseados em Kerberos e também para hosts. Um *principal* é assim: `primary/instance@REALM`, onde o parâmetro `instance` é opcional e usado somente para agrupamentos. Por exemplo, um *principal* de usuário pode ser assim: `thorsten/admin@example.com`. Um exemplo de servidor NFS: `nfs/nfs.example.com@example.com`. O *realm* guarda todos os *principals* de uma área e o corresponde ao nome de domínio DNS, escrito em letras maiúsculas. Com os *principals*, o servidor armazena as senhas dos usuários e serviços no banco de dados do Kerberos.

O servidor é relativamente fácil de configurar: no arquivo `/etc krb5.conf` deve ser fornecido o `realm`. O comando `create_kdb5_util` gera o banco de dados propriamente dito no diretório `/var/kerberos/krb5kdc`. A administração do banco de dados pode ser feita tanto localmente pela ferramenta `kadmin.local` quanto remotamente com o `kadmin`. Para isto, o serviço do Kadmin precisa estar ativo no KDC, e é necessário existir um *principal* administrador no arquivo `/var/kerberos/krb5kdc/kadm5.ac1`. Se uma das ferramentas de administração for usada, é possível usar o `add_principal` para adicionar um novo *principal* ao banco de dados – por exemplo, `add_principal -pw password thorsten`. Para um serviço ou uma estação seria semelhante a: `add_principal -randkey nfs/nfs.example.com`. As senhas do *principal* do serviço precisam, evidentemente, ser conhecidas nos servidores apropriados. Isto é feito por meio do serviço de senhas, com uso do seguinte comando para extraí-las do banco de dados do Kerberos: `ktadd -k /etc/krb5.keytab nfs/nfs.example.com`. Com isso, o arquivo `/etc/krb5.keytab` já pode ser copiado com segurança para o computador do serviço, por exemplo, via SSH. Após iniciar o KDC usando o comando `service kdb5kdc start`, a autenticação já estará pronta para o Kerberos.

dos servidores. No caso do NFSv4, é preciso informar o tipo de sistema de arquivos `nfs4` e a autenticação `krb5` (em vez de `sys`) como em: `root@tiffy ~]# mount -t nfs4 -o sec=krb5 nfs. example.com/export /mnt/nfs.`

Em caso de problemas, verifique novamente no arquivo `/etc/sys-`

`config/nfs` se a autenticação com Kerberos está mesmo ativada. Além disso, quando for necessário verificar a integridade dos dados transmitidos, informe a opção de montagem `sec=krb5i`. A opção `sec=krb5p` ainda criptografa os dados que devem ser transmitidos. ■

## Mais informações

- [1] RFC 1050: <http://www.faqs.org/rfcs/rfc1050.html>
- [2] RFC do NFSv4: <http://www.faqs.org/rfcs/rfc3550.html>
- [3] RFC do RPCSEC\_GSS: <http://www.faqs.org/rfcs/rfc2204.html>

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lhm.com.br/article/4457>

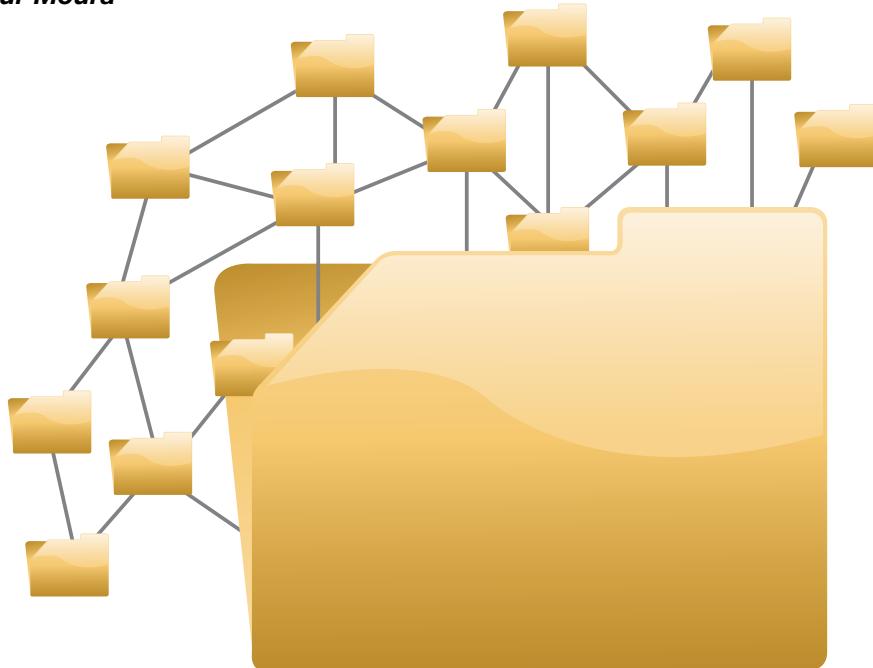


Eficiência em sistema de arquivos

# Seguro e escalonável

Repleto de funções, o OpenAFS surpreende pela segurança e escalabilidade.

por Eduardo Moura e Artur Moura



**O**penAFS [1] é uma implementação de código aberto do AFS – *Andrew File System*, um sistema de arquivos desenvolvido pela Universidade Carnegie Mellon, como parte de um projeto de computação distribuída nos anos 80. Muitos dos conceitos que o AFS implementava nos anos 80, foram incorporados à versão 4 de outro famoso sistema de arquivos de rede, o NFS. Além dessa famosa influência o AFS também tem seus genes presentes no Coda [2], outro sistema de arquivos distribuídos que vem ganhando espaço no palco das corporações.

## Características

O OpenAFS é um sistema de arquivos projetado para ser seguro e escalonável. Existem implementações de *células AFS* (aglomerado

de informações independentes) com mais 50.000 clientes. Em nossas instalações temos casos de perfis móveis com mais de 10GB que funcionam com um desempenho incomparável.

Além do desempenho, o sistema de arquivos permite que uma célula seja atendida por mais de um servidor e que um cache seja criado para o conteúdo mais usado diretamente na estação de trabalho, permitindo que o usuário continue trabalhando em caso de uma falha de rede. Todas as operações em arquivos são feitas nas cópias locais; quando o arquivo é fechado somente suas partes modificadas são enviadas para o servidor, aliviando a carga de rede.

Uma das principais características do OpenAFS é o *volume*, um conjunto de arquivos e subdiretórios (e algumas vezes links para outros volumes AFS), que são criados pelos ad-

ministradores e montados em algum ponto da célula. Após sua criação, os usuários podem criar diretórios e arquivos normalmente sem se preocupar com a localização física deste volume. Os administradores da célula podem mover o volume para outro disco, ou mesmo para outro servidor da célula sem afetar os usuários, que podem continuar utilizando os seus arquivos durante a movimentação.

Outra função do OpenAFS são os clones somente de leitura, que permitem que arquivos populares – como binários de programas, por exemplo –, sejam alocados em volumes replicados em vários servidores. Desta forma, a carga de trabalho da célula é distribuída e os arquivos estão sempre disponíveis (se um volume falhar, a célula fornece à estação o endereço da próxima cópia disponível).

No quesito segurança, o OpenAFS implementa o Kerberos 5 combinado com uma lista de controle de acesso (ACL, na sigla em inglês) que possui 7 permissões distintas (administrar, apagar, inserir, travar, procurar, ler e escrever) contra as 3 permissões tradicionais do Unix (ler, escrever e executar). Além da ACL, o OpenAFS utiliza o conceito de autenticação mútua onde clientes e servidores da célula identificam-se um ao outro antes de trocar informações.

## Como fazer

Nesse artigo vamos ensinar como criar dois servidores AFS para uma célula (um servidor principal e uma cópia *read-only*) e como acessar os arquivos da célula.

O OpenAFS é bastante dependente da estrutura de nomes da rede (DNS); sendo assim, utilizaremos o arquivo `hosts` para simplificar o processo. Os dois servidores terão os seguintes nomes:

**1** `srv1.afs.local` - 172.20.200.85  
**2** `srv2.afs.local` - 172.20.200.84

e devem ser inseridos no arquivo `/etc/hosts` conforme o exemplo abaixo:

```
172.20.200.85 srv1 srv1.afs.local
172.20.200.84 srv2 srv2.afs.local
```

Para instalar o OpenAFS em sua distribuição Linux é necessário obter os módulos do kernel, os binários e o restante dos componentes via web. Para saber qual é a versão do seu kernel, use o comando `# uname -r`, que irá retornar algo como a string: `2.6.18-194.26.1.el5`.

De posse da versão do kernel, você pode obter os pacotes .RPM adequados com o comando `wget`. Selecione a versão adequada, e aguarde a conclusão do download. Para instalar o pacote, utilize o comando:

```
# rpm -ivh openafs*.rpm dkms
openafs-1.4.12-e15.1.1.x86_64.rpm
```

## Configuração da partição Linux

Para instalar o servidor AFS é necessária a alocação de uma partição lógica dedicada para armazenar os volumes AFS. Crie um diretório chamado `/vicepa/`, que será o ponto de montagem da partição que armazenará os volumes AFS.

Adicione no arquivo `/etc/fstab` a partição criada, apontando para o ponto de montagem `/vicepa`, através da entrada `/dev/sdb1 /vicepa ext2 defaults 0 2`. Caso não exista a partição, crie-a utilizando o comando `mkfs`, desta forma: `mkfs -v /dev/sdb1`. Depois de concluída a formatação, monte todas as partições com o comando `mount -a`.

## Servidor BOS

O servidor BOS – *Basic OverSeer Server*, gerencia os processos de todos os servidores AFS. Quando executado pela primeira vez, o servidor irá criar os links simbólicos para os arquivos `/usr/vice/etc/ThisCell` e `/usr/vice/etc/CellServDB` que correspondem a arquivos localizados no diretório `/usr/afs/etc`. Neste ponto, é importante iniciar o servidor BOS com a flag `-noauth` que o iniciará sem necessidade de autenticação.

Verifique se o servidor BOS criou os links simbólicos que correspondem ao diretório `/usr/afs/etc`. Se algum dos arquivos `/usr/vice/etc/ThisCell` ou `/usr/vice/etc/CellServDB` não existir ou seus links simbólicos não tenham sido criados, crie-os, conforme indicado pelos comandos abaixo.

```
# cd /usr/vice/etc
# ln -s /usr/afs/etc/ThisCell
# ln -s /usr/afs/etc/CellServDB
# ln -s /usr/afs/etc/CellServDB CellServDB.dist
```

## Definição do nome da célula

A célula é o domínio administrativo do AFS, onde é definido como as máquinas clientes são configuradas e quanto espaço será reservado para cada usuário. Vamos utilizar o comando `bos setcellname` para definir o nome da célula (nesse caso, `afs.local`). O comando criará dois arquivos: `/usr/afs/etc/ThisCell`, que define a célula a qual a máquina pertence e `/usr/afs/etc/CellServDB`, arquivo de banco de dados que define as células existentes e seus respectivos servidores.

Adicione os binários do OpenAFS ao caminho do sistema, desta forma:

```
# export PATH=$PATH:/usr/afs/bin.
```

Em seguida, adicione o nome da célula: `bos setcellname srv1.afs.local afs.local -noauth`, e verifique com o comando `bos listhosts` se a máquina na qual estamos instalando o AFS está registrada, com `bos listhosts srv1.afs.local -noauth`.

O retorno será algo parecido com:

```
Cell name is afs.local
Host 1 is srv1.afs.local
```

## Processo do servidor de banco de dados

Vamos utilizar neste momento, o comando `bos create` para criar as três entradas dos processos do servidor de banco de dados, que é composto por três processos: `buserver`, `ptserver` e `vlserver`. Tais processos servem para controlar o servidor de backup, sua segurança e seu localizador de volumes, respectivamente.

Em primeiro lugar, deve ser criado o processo do servidor de backup, através do comando `bos create`:

```
# bos create srv1.afs.local
buserver simple /usr/afs/bin/
buserver -noauth.
```

Na sequência, crie o processo do servidor de proteção, com o mesmo comando:

```
# bos create srv1.afs.local ➔
ptserver simple /usr/afs/bin/ ➔
ptserver -noauth.
```

Em último lugar, crie o processo do servidor de volume com o comando:

```
# bos create srv1.afs.local ➔
vlserver simple /usr/afs/bin/ ➔
vlserver -noauth.
```

O processo `kaserver` é responsável pela autenticação, que se dá através de um token (chave de acesso do servidor Kerberos). Use o já conhecido comando `bos create` para criar o processo `kaserver` no servidor de banco de dados. O diretório corrente é `/usr/afs/bin`, sendo assim, o comando deve ser executado desta forma:

```
# ./bos create srv1.afs.local ➔
kaserver simple /usr/afs/bin/ ➔
kaserver -cell afs.local -noauth
```

Agora é chegada a hora de configurar o processo de autenticação, para que somente pessoas autorizadas tenham acesso à célula, utilizando o mesmo servidor Kerberos mencionado anteriormente. Em primeiro lugar, inicie o *prompt* interativo do `kasser-ver`, como ilustrado a seguir:

```
# kas -cell afs.local -noauth
ka>
```

Crie agora dois usuários, `afs` e `admin`, que são obrigatórios, lembrando que a senha deve conter seis dígitos. Em nosso exemplo, será utilizada a senha `senhaafs`.

```
ka> create afs
initial_password: senhaafs
Verifying, please re-enter ➔
initial_password: senhaafs
ka> create admin
```

```
initial_password: senhaafs
Verifying, please re-enter ➔
initial_password: senhaafs
```

Atribua permissões de administrador ao usuário `admin` e verifique se estas permissões foram corretamente atribuídas.

```
ka> setfields admin -flags ➔
admin
ka> examine admin
User data for admin (ADMIN) . . .
```

Saia do prompt e use o comando `bos adduser` para adicionar o usuário `admin` ao arquivo `/usr/afs/etc/UserList`. Essa ação proporciona permissão ao usuário `admin` para poder usar os comandos `bos` e `vos`: `./bos adduser srv1.afs.local admin -cell afs.local -noauth`.

Utilize o comando `bos addkey` para definir a chave de criptografia do servidor AFS no arquivo `/usr/afs/etc/KeyFile`. Lembre-se de utilizar a mesma senha neste processo.

```
# ./bos addkey srv1.afs.local ➔
-kvno 0 -cell afs.local -noauth
Input key: senhaafs
Retype input key: senhaafs
```

## Inicialização dos processos

Nesta etapa do processo, vamos adicionar o usuário `admin` ao banco de dados de proteção. O servidor de banco de dados de proteção define quem tem acesso a arquivos e pastas dentro da célula, mapeando usuários do Kerberos com os usuários existentes no AFS.

Utilize o comando `pts createuser` para criar uma entrada para o usuário `admin:pts createuser -name admin -id 1 -noauth`. User `admin` has id 1. Em seguida, torne o usuário `admin` membro do grupo `system:administrators`, desta forma: `./pts adduser admin system:administrators -noauth`. Com

o comando `bos restart` munido da flag `-all`, reinicie o processo de banco de dados utilizando a nova chave de encriptação: `./bos restart srv1.afs.local -all -noauth`.

Agora é necessário iniciar o processo do servidor de arquivos, e para isso, é necessário criar primeiramente, o processo `fs` através do comando `bos create`:

```
# ./bos create srv1.afs.local ➔
fs fs /usr/afs/bin/fileserver ➔
/usr/afs/bin/volserver /usr/afs ➔
/bin/salvager -noauth
```

Em seguida, verifique se o processo inicializou corretamente, com `./bos status srv1.afs.local fs -long -noauth`. E crie o primeiro volume AFS, que será chamado de `root.afs`:

```
# ./vos create srv1.afs.local ➔
/vicepa root.afs -noauth
```

É importante iniciar o primeiro processo do servidor de atualização (o processo `upserver`), que irá distribuir o conteúdo do diretório dessa máquina para os outros servidores da célula. Esse processo irá começar a funcionar quando for instalada a outra parte do servidor de atualização.

Para isso, crie o processo `upserver`, usando o seguinte comando:

```
# ./bos create srv1.afs.local ➔
upserver simple "/usr/afs/bin/" ➔
upserver -crypt /usr/afs/etc ➔
-clear /usr/afs/bin" -noauth.
```

## Membros da célula

Todos os clientes AFS tem uma cópia do arquivo `/usr/vice/etc/ThisCell`, que define a de qual célula a máquina faz parte. Esse arquivo, que foi criado no diretório `/usr/afs/etc` é usado somente em máquinas servidoras. É importante neste ponto,

## Listagem 1: Inicialização do OpenAFS

```
01 # OpenAFS Client Configuration
02 AFSD_ARGS="-stat 2500 -daemons 4 -volumes 100"
03
04 # OpenAFS Server Configuration
05 BOSSERVER_ARGS=
```

definir os membros da célula. Vá até o diretório `/usr/vice/etc` e remova o link simbólico criado inicialmente:

```
# cd /usr/vice/etc
# rm ThisCell
```

Crie em seguida, uma cópia do arquivo `/usr/afs/etc/ThisCell` na pasta corrente, com: `cp /usr/afs/etc/ThisCell ThisCell`

O arquivo `CellServDB` contém todas as células e seus respectivos servidores. Remova também o link simbólico deste arquivo, criado anteriormente e apague os arquivos `CellServDB` e `CellServDB.dist` que foram criados. Copie o arquivo presente em `/usr/afs/etc/CellServDB` em dois novos arquivos, `CellServDB` e `CellServDB.dist`.

```
# rm CellServDB CellServDB.dist
# cp /usr/afs/etc/CellServDB CellServDB
# cp /usr/afs/etc/CellServDB CellServDB.dist
```

O conteúdo arquivo deverá ficar assim:

```
>afs.local #Cell name
IP      #srv1.afs.local
```

## Configuração de inicialização

Edito o arquivo `/etc/sysconfig/openafs` pra que ele fique parecido com o exemplo da **Listagem 1**. Para re inicializar o servidor, utilize o comando `bos shutdown`, conforme ilustrado a seguir:

```
# bos shutdown srv1.afs.local
-wait
# shutdown -r now
```

## Configuração das ACLs do AFS

As células AFS serão sempre encontradas abaixo do diretório `/afs`. Sendo assim, devemos dar permissão de leitura pra qualquer usuário do sistema operacional que estiver no grupo `users`. Após a reinicialização da máquina, acesse a célula `afs` com o usuário `admin: klog admin Password`: senhaafs.

Depois, configure as permissões necessárias e crie o volume da célula com os comandos apresentados na **Listagem 2**.

Com o comando `vos addsite`, é hora de habilitar a replicação dos volumes `root.afs` e `root.cell`, pois essa ação será necessária para a replicação que ocorrerá no servidor adicional que será criado logo a seguir.

```
# vos addsite srv1.afs.local /vicepa root.afs
# vos addsite srv1.afs.local /vicepa root.cell
# vos release root.afs
# vos release root.cell
```

## Instalação de um servidor adicional

Para instalar um servidor adicional que manterá uma cópia somente leitura das entradas dos volumes do servidor `srv1.afs.local`, basta seguir os seguintes passos:

**1** Efetue a instalação do primeiro servidor, como mencionamos no início do artigo;

**2** Inicialize o servidor BOS. Copie o conteúdo da pasta `/usr/afs/etc` do servidor `srv1.afs.local` usando o comando `scp`, desta forma: `# scp srv1.afs.local:/usr/afs/etc/* /usr/afs/etc/`. Vá até o diretório `/usr/afs/bin` que contém o binário do servidor `bosserver` e inicialize-o com a flag `-noauth`, da mesma maneira que foi efetuado no primeiro servidor instalado.

```
# cd /usr/afs/bin
# ./bosserver -noauth &
```

**3** Inicialize a outra parte do servidor de atualização:

```
# bos create srv2.afs.local
upclientetc simple "/usr/afs/bin/upclient srv1.afs.local"
-t 300 "/usr/afs/etc" -cell afs.local -noauth
```

Crie também o processo `upclient-bin` que aceitará atualização do processo `upserver` que está no servidor principal:

```
# bos create srv2.afs.local
upclientbin simple "/usr/afs/bin/upclient srv1.afs.local"
-t 300 -clear "/usr/afs/bin" -cell afs.local -noauth
```

**4** Inicialize o processo `fs`, que contém três componentes: o `File Server`, o `Volume Server`, e o `Salvager`:

```
# bos create srv2.afs.local fs
fs /usr/afs/bin/fileserver /usr/afs/bin/volserver /usr/afs/bin/salvager -cell afs.local -noauth
```

**5** Crie o processo de autenticação:

```
# bos create srv2.afs.local
```

```
# kaserver simple /usr/afs/bin →
/kaserver -noauth
```

- 6** Crie o arquivo `/usr/vice/etc/CellServDB`. Utilize algum programa de transferência de arquivos, como o `scp` para copiar o arquivo `CellServDB` do servidor `srv1.afs.local`:

```
# scp srv1.afs.local:/usr/vice →
/etc/CellServDB /usr/vice/etc/
```

- 7** Entre no diretório `/usr/vice/etc` e crie uma cópia do arquivo `ThisCell`, que está presente originalmente no diretório `/usr/afs/etc`.

```
# cd /usr/vice/etc
# rm ThisCell
# cp /usr/afs/etc/ThisCell →
ThisCell
```

- 8** Desligue o servidor AFS com o comando `bos shutdown` e reinicie-o com o comando `shutdown -r now`.

## Servidor de banco de dados

Neste processo, será instalado o processo do servidor de banco de dados, cujos processos foram criados anteriormente.

- 1 Logue-se no servidor `srv1.afs.local` e obtenha um token(chave de acesso ao AFS), para obter acesso às permissões administrativas.
- 2 Utilize o comando `bos addhost` para adicionar um novo servidor ao arquivo `/usr/afs/etc/CellServDB`, através do comando `bos addhost srv1.afs.local srv2.afs.local`.

Será necessário esperar em média cinco minutos para que o servidor de atualização distribua o novo arquivo `CellServDB` entre as máquinas.

## Listagem 2: Permissões e criação do volume da célula

```
01 # fs setacl /afs system:anyuser r
02 # vos create srv1.afs.local /vicepa root.cell
03 # fs mkmount /afs/afs.local root.cell
04 # fs setacl /afs/afs.local system:anyuser r
05 # fs mkmount /afs/.afs.local root.cell -rw
```

- 3** Verifique depois se o servidor `srv2.afs.local` foi adicionado à lista: `bos listhosts srv1.afs.local`.

- 4** Inicialize o servidor de backup: `bos create srv2.afs.local buserver simple/usr/afs/bin/buserver`.
- 5** Inicialize o servidor de proteção (o processo `ptserver`): `# bos create srv2.afs.local ptserver simple /usr/afs/bin/ptserver`.

- 6** Em seguida, inicialize o localizador de volume (o processo `vlserver`): `# bos create srv2.afs.local vlserver simple /usr/afs/bin/vlserver`.

- 7** Reinicialize todos os servidores através do comando `bos restart`,

começando pelo servidor com IP menor:

```
# bos restart srv2.afs. →
local kaserver buserver ptserver →
vlserver
# bos restart srv1.afs. →
local kaserver buserver ptserver →
vlserver
```

A partir deste momento, você possui instalados e em operação os dois servidores AFS. Para testar se está tudo funcionando, basta efetuar o login nos servidores com o comando `klog` e acessar o conteúdo das células. ■

## Sobre o autor

**Eduardo Moura** ([eduardo.moura@telway.com.br](mailto:eduardo.moura@telway.com.br)) é CEO da Telway, entusiasta de open source e especialista em gestão de TI.

**Artur Moura** ([artur.moura@telway.com.br](mailto:artur.moura@telway.com.br)) é analista técnico sênior da Telway, experiente profissional em software livre e integração multi-plataforma.

## Mais informações

[1] AFS: <http://www.openafs.org/>

[2] Sistema de arquivos Coda: <http://www.coda.cs.cmu.edu/>

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lhm.com.br/article/4460>



Controle de múltiplos sistemas

# Plataformas conectadas

As muitas abordagens para gerenciar computadores remotamente incluem o VNC, o Nomachine e o SSH. O Synergy é uma ferramenta útil que conecta vários computadores para criar um ambiente de desktop virtual.

por Florian Effenberger

**S**ynergy é um software livre que permite que você facilmente compartilhe um único mouse e um único teclado entre vários computadores com diferentes sistemas operacionais, sem necessidade de hardware especial. Tudo que você precisa é uma conexão de rede ativa. É destinado a administradores de redes e sistemas que possuem vários computadores interligados, onde cada sistema utiliza seus próprios recursos.

## Listagem 1: Configuração do Synergy

```

01 # Definição de telas
02 section: screens
03 ubuntu:
04 vista:
05 end
06 # Nomes alternativos
07 section: aliases
08 # ubuntu -> desktop
09 ubuntu:
10 desktop
11 # vista -> notebook
12 vista:
13 notebook
14 end
15 # Arranjo da tela
16 section: left
17 # vista: right of ubuntu
18 ubuntu:
19 right = vista
20 # ubuntu: left of vista
21 vista:
22 left = ubuntu
23 end

```

Para operar o Synergy são necessários pelo menos dois computadores, cada um com seu próprio sistema operacional, monitor e placa de rede. O software suporta desde o Windows 95 até o Windows 7, o Mac OS X desde a versão 10.2 e o Linux com o servidor X atual. Pacotes específicos para Windows e Mac OS X estão disponíveis na página do Synergy [1]. Um arquivo RPM está disponível para Linux e pode ser instalado na maioria das distribuições populares, com ferramentas como o Alien [2], se necessário. Algumas distribuições oferecem pacotes de instalação pré-compilados, como por exemplo, o Ubuntu que contém o pacote Synergy disponível através da Central de Programas do Ubuntu.

## Teste

Nosso ambiente de testes dispõe de um computador executando Ubuntu e um pequeno notebook executando o Windows Vista. Para evitar a constante alternância entre os teclados, será implantado o Synergy. Um usuário com nível administrativo irá trabalhar principalmente no computador principal, que possui o sistema Ubuntu. Usando termos do Synergy, esse é o chamado *sistema de controle*, já que esse administrador irá utilizar o teclado e o mouse dessa máquina principal. Os outros dispositivos (nesse caso, o notebook) são os clientes.

## Configuração

Antes de começar a usar o Synergy, será preciso configurá-lo, editando o arquivo de texto `/etc/synergy.conf` ou `~/.synergy.conf`. A unidade elementar é uma tela com uma posição definida precisamente: cada computador pertence a um grupo, servidor ou cliente – assim como o arranjo de displays na configuração de um computador com vários monitores. Para cada computador, é preciso acessar o arquivo de configuração com o nome da tela, seus alias, e sua posição em relação a outros dispositivos – em ambas as direções. A **listagem 1** contém um exemplo com comentários sobre o caso de teste. O site do Synergy documenta ainda várias opções adicionais.

Todas as opções no arquivo de configuração devem estar em letras minúsculas. Além disso, certifique-se de utilizar as quebras de linha corretas, porque o Synergy é exigente com relação a isso e não usará o arquivo se estiverem erradas. Depois de concluir todo esse trabalho, é possível iniciar o servidor Synergy no Ubuntu com os privilégios de um usuário normal, digitando simplesmente o comando `synergys`. O parâmetro `-f` irá impedir que o Synergy desapareça em segundo plano.

O *QuickSynergy* [3], interface gráfica para o Synergy, oferece uma

abordagem ainda mais conveniente para a configuração. No Ubuntu, baixe o pacote da Central de Programas do Ubuntu e abra-o através do menu *Aplicativos/Ferramentas de sistema/QuickSynergy* após a instalação.

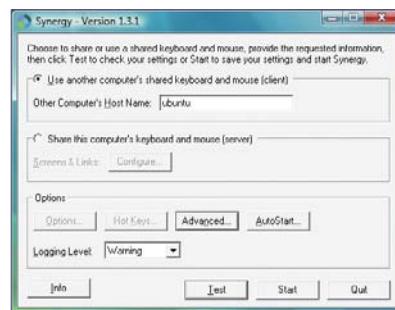
Amáquina cliente executando Windows Vista, que se pretende controlar remotamente com o sistema Ubuntu, é ainda mais fácil de configurar. Após a instalação do Synergy, é possível abri-lo diretamente através do menu *Iniciar*. A tela que será exibida é limpa e de fácil entendimento (**figura 1**). Para abrir uma conexão com o servidor, selecione a opção *Use another computer's shared keyboard and mouse (client)* e digite o nome do computador ao qual deseja se conectar. Os usuários avançados também podem configurar extras como *Logging Level*, *AutoStart* e detalhes de rede.

## Conectando as telas

Depois de configurar todos os clientes, é possível simplesmente executar *synergyc server IP* (ou clicar em *Start* no Windows) para combinar as telas. A coisa toda é espetacular no início, e é possível continuar a trabalhar em cada sistema de forma normal com bom desempenho.

No entanto, se mover o mouse sobre o servidor além da borda direita da tela do Ubuntu, o cursor do mouse será exibido no cliente com Windows Vista como em um único computador com vários monitores, mas aqui, ele se move entre dois computadores com diferentes plataformas. Entradas de teclado também chegam ao cliente enquanto o foco está em sua tela (ou seja, o cursor do mouse é exibido lá). Mas, isso não é tudo – o Synergy também coordena a área de transferência entre os dois sistemas.

Segundo os desenvolvedores, o Synergy identifica automaticamente o conjunto de caracteres correto e converte as quebras de linha entre os sistemas operacionais, o que é perfeito para copiar longos blocos de texto e



**Figura 1** O Synergy como cliente no Windows Vista.

arquivos de configuração. Pressionar a tecla *Scroll* desativa temporariamente o Synergy, se necessário. No arquivo de configuração, é possível definir uma série de opções adicionais. Entre outras coisas, o Synergy pode mapear as teclas entre o servidor e o cliente, configurar áreas específicas da tela quando não se quer alternar entre as telas e executar certas ações em uma tecla.

O Synergy atrapalha algumas funções, no entanto. Em nossos testes, a ferramenta não conseguiu sincronizar protetores de tela e falhou no bloqueio de todas as telas de forma centralizada. Outro problema, é que, de acordo com o site do Synergy, a variante do programa para o Mac OS X, em particular, não é tão madura quanto as versões para Linux e Win-

## Quadro 1: Nota sobre segurança

Os autores do Synergy informam no site que ele não oferece nenhum tipo de segurança no que tange autenticação e criptografia [4]. Por segurança, pode ser bom usar um túnel SSH [5] para criptografar os seus dados.

dows. Sobre questões de segurança, confira o **quadro 1** para mais detalhes.

## Conclusão

O Synergy oferece uma abordagem interessante para controlar vários computadores de forma centralizada, sem investir em hardware adicional. Em contraste com as abordagens antigas, cada sistema mantém seu próprio monitor. O programa é muito útil para os proprietários de vários computadores e que desejam interagir entre eles. E a área de transferência cruzada entre sistemas operacionais é realmente conveniente, o que elimina a necessidade de copiar arquivos de texto. Um item na minha lista de desejos do Synergy, no entanto, é uma configuração mais fácil no Linux. ■

## Mais informações

- [1] Site do Synergy: <http://synergy-foss.org/>
- [2] Alien: <http://kitenet.net/~joey/code/alien/>
- [3] QuickSynergy: <http://code.google.com/p/quicksynergy/>
- [4] Notas sobre Segurança: <http://synergy-foss.org/pm/projects/synergy/wiki/UserFAQ#Q-How-secure-is-the-application>
- [5] Tunelamento com SSH: <http://www.revsys.com/writings/quicktips/ssh-unneel.html>

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lnm.com.br/article/4452>



Gerenciamento de rede

TUTORIAL

# Gerenciamento ágil

*Conforme sua rede cresce, o gerenciamento manual do sistema torna-se moroso e fica impraticável. Conheça o Spacewalk, uma ferramenta de código aberto que elimina o trabalho pesado do gerenciamento de rede.*

por Thorsten Scherf



Enzo Forciniti - sxc.hu

Spacewalk [1] é o derivado de código aberto do popular *Red Hat Network Satellite Server*. A Red Hat publicou o código-fonte do servidor no verão de 2008, e a comunidade já disponibilizou a versão 1.0. As tarefas principais do aplicativo incluem uma provisão de pacotes RPM de software, gerenciamento de arquivos de configuração, e árvores de apoio, tornando possível

a instalação de sistemas *bare-metal* (sistemas completamente restauráveis a partir de um backup). A abordagem utilizada pelo Spacewalk é simples: antes de um sistema acessar os recursos do Spacewalk, ele primeiro tem que se registrar no servidor. Os registros podem ser baseados em uma combinação de nome de usuário/senha ou uma chave de ativação que é pré-gerada pelo servidor Spacewalk.

Depois do registro, o sistema aparece na interface gráfica web do servidor.

Se o servidor tiver mais recursos, é possível atribuí-los ao sistema nesse momento. Os recursos incluem pacotes de software ou arquivos de configuração que são normalmente organizados em canais.

Um sistema sempre tem exatamente um canal base com subcanais opcionais. O canal base contém o sistema operacional baseado em um pacote RPM, como o *Red Hat Enterprise Linux*, o *Fedora* ou o *CentOS*. Os subcanais contêm pacotes de software adicionais que são independentes do sistema operacional, como o *Red Hat Cluster Suite* ou o *389 Directory Server*.

O Spacewalk pode clonar os canais existentes e criar novos canais a partir do zero. Esta característica lhe dá o controle total da pilha de software fornecido através do Spacewalk.

## Listagem 1: Configuração do listener Oracle

```

01 cat >> /etc/tnsnames.ora << 'EOF'
02 XE =
03 (DESCRIPTION =
03 (ADDRESS_LIST =
04 (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)
05 (PORT = 1521))
06 )
07 (CONNECT_DATA =
08 (SERVICE_NAME = xe)
09 )
10 )
11 EOF

```

Canais de configuração ajudam a distribuir os arquivos de configuração dos pacotes de software. O Spacewalk também mantém as versões mais antigas dos arquivos para que seja possível reverter para uma versão anterior a qualquer momento em caso de necessidade.

Os pacotes de software ou arquivos de configuração podem ser instalados através do sistema de destino ou centralmente na interface web do Spacewalk. Para evitar gastar muito tempo com a instalação de um grande número de sistemas, é possível atribuir sistemas a grupos lógicos e a instalação de um recurso a um grupo. Por exemplo, pode fazer sentido conferir todos seus servidores web para um grupo servidor [www](#) no Spacewalk. Quando uma nova versão do software de servidor web é lançada, basta dizer ao Spacewalk para aplicar a atualização ao grupo, atualizando automaticamente todos os sistemas pertencentes a este grupo.

Para a instalação, os sistemas clientes consultam o servidor em intervalos predefinidos (cerca de quatro horas por padrão) para ver se novas ações foram definidas desde a última versão. Se assim for, o Spacewalk executa essas ações. O sistema cliente e o servidor Spacewalk comunicam-se sempre usando o protocolo Jabber. Quaisquer novas ações definidas são imediatamente executadas no cliente pelo Spacewalk.

## Controle da base

A comunicação é sempre feita a partir do cliente para o servidor, o que é importante no que diz respeito às regras de firewall. Uma lista das portas de rede que precisam ser habilitadas pode ser encontrada online [\[2\]](#). Além do pacote de software ou instalação do arquivo de configuração, as ações também podem executar comandos arbitrários nos sistemas individuais através do servidor Spacewalk. Por exemplo, depois de criar um novo arquivo de

configuração para os servidores web e distribuí-lo aos sistemas, será preciso reiniciar o processo do servidor para analisar as novas instruções de configuração. Em vez de fazer login em cada sistema ou usar um *loop for*, basta emitir o comando de reiniciar centralmente no servidor Spacewalk.

A instalação de novos sistemas também é bastante simples. O Spacewalk possui os arquivos de instalação necessários em forma de árvores *kickstart*. O candidato à instalação utiliza um meio de inicialização como um CD, um pendrive USB ou uma placa de rede com capacidade PXE para contatar o servidor. O programa de instalação *First Stage*, que é parte da mídia de instalação, define qual servidor irá cuidar da instalação.

As etapas de instalação restantes são feitas pelo programa de instalação *Second-Stage*, localizado no servidor Spacewalk, que é transferido para o sistema do cliente quando a instalação é iniciada. Se quiser automatizar a instalação completamente, defina a localização do arquivo *kickstart* na mídia de inicialização. O arquivo *kickstart* é uma espécie de arquivo de resposta que descreve as propriedades do candidato à instalação, tais como particionamento, software, linguagem e configurações de firewall. Logicamente, é possí-

vel criar um arquivo de kickstart no servidor Spacewalk e apenas incluir um link para o arquivo na mídia de inicialização. O Spacewalk pode gerenciar qualquer distribuição baseada em RPM. Ainda há a opção de operar sistemas clientes através de várias organizações. Usando a interface web, o administrador cria diversas organizações e atribui certo número de direitos ao sistema para elas. Os direitos estão vinculados aos certificados que o Spacewalk gera automaticamente durante a instalação. É possível adicionar usuários às organizações.

Se um cliente é registrado com uma conta de usuário de uma organização específica, o sistema assume essa organização. Quando os usuários da organização se conectam ao servidor Spacewalk, verão apenas os sistemas em sua própria organização. Esse recurso é útil quando é necessário gerenciar vários departamentos e é preferível gerir os sistemas dos departamentos individuais separadamente. Basta atribuí-los a diferentes organizações, que, naturalmente, precisam ser criadas com antecedência.

## Instalação

O Spacewalk pode ser instalado no Red Hat Enterprise Linux (RHEL) [\[3\]](#), Fedora [\[4\]](#), ou CentOS [\[3\]](#).

### Listagem 2: Criação do usuário Spacewalker

```
01 sqlplus 'sys@xe as sysdba'
02 SQL> create user spacewalk identified by spacewalk ➔
default tablespace users;
03 SQL> grant dba to spacewalk;
04 SQL> quit
```

### Listagem 3: Ajuste do Oracle

```
01 sqlplus spacewalk/spacewalk@xe
02 SQL> alter system set processes = 400 scope=spfile;
03 SQL> alter system set "_optimizer_filter_pred_pullup" ➔
=false scope=spfile;
04 SQL> alter system set "_optimizer_cost_based_ ➔
transformation"=off scope=spfile;
05 SQL> quit
```

## Listagem 4: Arquivo de resposta

```

01 admin-email = root@localhost
02 ssl-set-org = Tuxgeek Org
03 ssl-set-org-unit = Tuxgeek OU
04 ssl-set-city = Essen
05 ssl-set-state = NRW
06 ssl-set-country = DE
07 ssl-password = spacewalk
08 ssl-set-email = root@localhost
09 ssl-config-sslhost = Y
10 db-backend=oracle
11 db-user=spacewalk
12 db-password=spacewalk
13 db-sid=xe
14 db-host=localhost
15 db-port=1521
16 db-protocol=TCP
17 enable-tftp=Y

```

Repare que o Spacewalk precisa do Java na versão 1.6.0 ou superior, para funcionar corretamente. É possível usar o OpenJDK para isso; o Fedora já vem com ele. Administradores do RHEL ou CentOS podem obter o pacote através do repositório de software adicional EPEL – *Extra Packages for Enterprise Linux*.

Além do pacote Java, um banco de dados Oracle 10g também é necessário para instalar o Spacewalk. O Oracle XE fornece uma versão gratuita de seu banco de dados. Os desenvolvedores estão trabalhando duro para implementar o suporte de um banco de dados de código aberto após terem identificado o PostgreSQL como a

melhor alternativa para o Oracle. Até o momento, é difícil dizer quando o suporte oficial ao PostgreSQL estará disponível, mas é bom verificar o cronograma de desenvolvimento do Spacewalk [5] ou listas de discussão [6] regularmente.

## Oracle XE

Após instalar o RPM do repositório de sua distribuição, o primeiro passo é instalar o Oracle Express, que pode ser baixado gratuitamente que [7]. É preciso a versão 10.2.0.1. Além do banco de dados, também é preciso instalar o `oracle-instantclient-basic` e o `oracle-instantclient-sqlplus`, que podem ser instalados com o Yum, desta forma:

```

yum localinstall --nogpgcheck →
oracle-xe-univ*.rpm →
oracle-instantclient-basic*.rpm →
oracle-instantclient-sqlplus*.rpm

```

Antes de configurar o banco de dados, certifique-se de que seu *hostname* aponta para o endereço IP correto no arquivo `/etc/hosts`, de modo a evitar problemas com a configuração do *Oracle Listener* mais tarde. Use os seguintes parâmetros para a configuração:

```

HTTP port for Oracle Application
Express: 9055
Database listener port: 1521
Password for SYS/SYSTEM: Password
Start at boot: y

```

A porta HTTP padrão para o aplicativo Oracle Express é a porta 8080 e que já está ocupada pelo servidor de aplicativos Tomcat. Então, é preciso escolher uma porta alternativa para evitar conflitos. Para se comunicar-se com o banco de dados, será preciso configurar o processo que o monitora no arquivo `/etc/tnsnames.ora` ([listagem 1](#)).

Agora só é preciso fazer algumas alterações no banco de dados. Para fazer isso, conecte-se a ele com o `sqlplus` e crie um usuário `spacewalk`, para o qual seja possível atribuir uma senha ([listagem 2](#)).

A configuração padrão do Oracle Express suporta um máximo para 40 conexões simultâneas, o que não é suficiente para as operações do Spacewalk. As instruções na [listagem 3](#) alteram o limite máximo de 400 conexões. Agora é preciso reiniciar o banco de dados, com o comando `/sbin/service oraclexe`.

## Instalação do Spacewalk

O próximo passo é instalar o servidor Spacewalk. Para isso, é preciso incluir o repositório Spacewalk como

The screenshot shows the 'Create Software Channel' page. On the left, there's a sidebar with links: Software Channels, Package Search, Manage Software Channels, and Manage Software Packages. The main area has tabs: Details (selected) and Basic Channel Details. A note says: 'Create or edit software channels from this page. If the parent channel is set to 'none', the channel is a base channel. Otherwise, the channel is a child of the specified channel.' Below that, it says: 'Channel name and label are required. They each must be at least 6 characters in length. Labels must begin with a letter, contain only lowercase letters, hyphens ('-'), periods ('.'), underscores ('\_'), and numerals. Channel name may also contain spaces and forward slashes ('/').' Another note says: 'Channel summary is also required.' The form fields are: Channel Name\*, Channel Label\*, Parent Channel: None, Parent Channel Architecture: IA-32, Yum Repository Checksum Type: sha1 (with a tip: 'Tip: sha1 offers the widest compatibility with clients. sha-256 offers higher security, but is compatible only with newer clients: Fedora 11 and newer, or Enterprise Linux 6 and newer.'), Channel Summary\*, and Channel Description:.

**Figura 1** A abordagem mais simples para configurar um canal de software é usando a interface gráfica web.

descrito anteriormente. É preciso um arquivo `spacewalk.repo` que aponta para o repositório adequado em `/etc/yum.repos.d/`. O seguinte comando inicia a instalação: `yum install spacewalk-oracle`.

Como esse pacote depende de todos os outros pacotes do Spacewalk; o gerenciador de pacotes irá baixar e instalar automaticamente todas as dependências. Depois, é possível configurar o aplicativo de forma interativa com a ferramenta de configuração ou com o uso de um arquivo de resposta ([listagem 4](#)).

Passe o arquivo para a ferramenta de configuração da seguinte forma:

```
spacewalk-setup --disconnected →
--answer-file=answerfile
```

A configuração pode levar algum tempo para terminar, pois o processo configura as tabelas do banco de dados. A ferramenta de configuração. Em seguida, inicia todos os serviços necessários. É possível reiniciar manualmente usando a ferramenta `/usr/sbin/rhn-satellite`. Para configurar o sistema, inicie a interface web do Spacewalk através da sua URL: <http://spacewalk.server.tld>. Além das informações de contato, também é possível definir a senha do administrador do Spacewalk nesse momento.

## Canais de software

A próxima etapa é a criação de um canal de software inicial para os sistemas clientes. Quando um cliente é registrado, é preciso especificar exatamente um canal base para ele, canal este que será utilizado para recuperar os pacotes do sistema operacional e suas atualizações. Claro que é possível configurar subcanais para o canal base e atribuir os subcanais a determinados clientes, conforme necessário. Após fazer isso, é possível usar os subcanais para distribuir mais pacotes RPM para

The screenshot shows the 'Active Users' page in the Spacewalk interface. On the left, there's a sidebar with 'User List' and 'Active' selected. The main area has a header 'Active Users' with a question mark icon. Below it is a search bar with 'Filter by Username:' and a 'Go' button. To the right of the search bar are buttons for 'create new user' and '1 - 1 of 1'. A table lists one user: 'satadmin' (Real Name: Scherf, Thorsten, Roles: Satellite Administrator, Organization Administrator), with a 'Last Sign In' timestamp of '6/2/10 8:38:41 PM CEST'. At the bottom are 'Download CSV' and copyright information: 'Copyright © 2002-10 Red Hat, Inc. All rights reserved. Privacy statement Legal statement redhat.com Spacewalk release 1.0'.

**Figura 2** Atribuição de diferentes privilégios a usuários individuais no servidor Spacewalk.

os sistemas. Os pacotes podem ser seus próprios aplicativos ou RPMs de outros repositórios.

A abordagem mais fácil para a criação de um canal de software é utilizar a interface web (*Channels/Manage Software Channels/Create – figura 1*). Graças à API Spacewalk, também é possível fazer um script para realizar esse processo [\[8\]](#). Chame o script da seguinte maneira:

```
create_channel.py --label=fedora →
-12-i386
--name "Fedora 12 32-bit"
--summary "32-bit Fedora 12 →
channel"
```

No script, é preciso fornecer o *Fully Qualified Domain Name* (FQDN) para o servidor Spacewalk e a conta do usuário para a criação de canais, assim como a conta do administrador Spacewalk criada anteriormente. A aba *Users* também dá a opção de criar mais usuários com privilégios específicos ([figura 2](#)).

O canal configurado agora deve estar visível na aba *Channels* da interface web, mas não terá nenhum pacote de software. Embora seja possível enviar pacotes de software para o servidor de várias maneiras, o método

escolhido vai depender se os pacotes estarem disponíveis localmente (por exemplo, em DVD) ou da preferência por sincronizar um repositório Yum remoto com o servidor Spacewalk. Se preferir o *upload* local, é possível usar a ferramenta `rhnpush`, que é iniciada da seguinte forma:

```
rhnpush -v --channel=fedora →
13-i386
--server=http://localhost/APP →
--dir=/path/to/the/packages
```

Para sincronizar o servidor Spacewalk com um repositório remoto de software, basta especificar a URL para este repositório nas propriedades do canal de software na interface web (*Channels/Manage Software Channels/Fedora 12 32-bit*). A sincronização pode demorar um pouco para acontecer. Outra opção aqui é a ferramenta de linha de comando `spacewalk-repo-sync`, que baixa os pacotes a partir de um repositório Yum para seu próprio servidor Spacewalk.

Para manter o servidor atualizado, é possível usar o `cron` para executar um script [\[9\]](#) em intervalos regulares. Esse script irá checar suas fontes de software configuradas e automaticamente baixar qualquer pacote novo.

## Listagem 5: Configuração GPG para RPM

```
01 cat .rpmmacros
02 %_signature gpg
03 %_gpg_name Thorsten Scherf <tscherf@redhat.com>
```

**Create Activation Key**

**Activation Key Details**

Systems registered with this activation key will inherit the settings listed below.

**Description:** Mailserver

**Key:** 1-mailserver

**Usage:**

**Base Channels:** Fedora 12 i386

**Add-On Entitlements:**  Monitoring,  Provisioning,  Virtualization,  Virtualization Platform

**Figura 3** Vários recursos podem estar ligados à chave de registro. Sistemas que utilizam a chave têm acesso a recursos associados.

Essa abordagem elimina a necessidade de sincronização manual.

Aliás, é possível usar o método discutido aqui para criar subcanais também. Note que os pacotes RPM feitos por você devem ser assinados digitalmente. Tanto o servidor Spacewalk quanto o aplicativo cliente Yum irão rejeitar pacotes não assinados por padrão.

Embora seja possível desativar esse recurso, é melhor trabalhar com as assinaturas digitais por razões de segurança. O comando `rpm --resign RPM package` irá assinar o pacote; é preciso ter as chaves GPG disponíveis localmente para a ferramenta RPM. O arquivo `~/.rpmmacros` dá o nome e a localização da chave ([listagem 5](#)).

Para permitir que os sistemas clientes verifiquem os pacotes assinados com essa chave, é preciso depositar a chave pública no servidor Spacewalk, de preferência em `/var/www/html/pub`, diretório que qualquer cliente pode acessar. O seguinte comando exporta a chave pública do GPG:

```
gpg --armor --export tscherf@redhat.com > /var/www/html/pub/rpm-gpg-key
```

Para permitir que os sistemas clientes existentes accessem os pacotes de software que acabaram de ser enviados, é preciso registrá-los com o servidor Spacewalk. Comece instalando o *Spacewalk Client Repository* RPM

Updates	Errata	Packages	Configs	System	Base Channel	Entitlement
0	0	0	0	fedora.tuxgeek.de	Fedora 12 i386	Management, Provisioning

**Figura 4** Após completar o registro, o sistema aparece na interface web do servidor Spacewalk.

nos clientes. Os sistemas Fedora 12 há um RPM adequado em [\[10\]](#), assim como para o RHEL5 e o CentOS5 [\[11\]](#). No RHEL e no CentOS, também é preciso instalar o RPM para o repositório EPEL [\[12\]](#), porque, caso contrário, as dependências da ferramenta cliente podem não ser resolvidas problema corretamente. O seguinte comando instala o arquivo Yum em um sistema Fedora 12 de 32 bits:

```
rpm -Uvh http://spacewalk.redhat.com/ yum/1.0/Fedora/12/i386/spacewalk-client-repo-1.0-2.fc12.noarch.rpm
```

Agora, use o Yum para instalar as ferramentas do cliente:

```
yum install rhn-client-tools rhn-check rhn-setup rhnsd m2crypto yum-rhn-plugin
```

A abordagem mais fácil para registrar um sistema no servidor é executar a ferramenta `rhnreg_ks`, que espera uma chave de registro. É preciso criar a chave antes no servidor Spacewalk (*Systems/Activation Key/Create Key*). Quando uma chave é criada, é possível ligar vários recursos a ela, como o canal de software do Fedora 12 recém-criado aqui, ou vários canais de configuração, caso alguns tiverem sido criados ([figura 3](#)). Além disso, é possível atribuir grupos de sistema para a chave. Os sistemas que usam essa chave para registro têm acesso aos recursos associados. Para isso, especifique a chave criada durante o processo de registro:

```
rhnreg_ks --serverUrl= http://spacewalk.server.tld/ XMLRPC --activationkey=key
```

Se tudo funcionou corretamente, o sistema estará na aba *Systems* da interface web do servidor. Um exame nas propriedades do sistema

também deve mostrar o canal de software configurado. A abordagem mais fácil de verificar se o acesso ao canal está funcionando é instalar um pacote de canal. Se isso não funcionar, é possível que o sistema cliente não esteja usando o certificado CA do servidor Spacewalk. O certificado é armazenado em <http://spacewalk.server.tld/pub/> no servidor e deve ser armazenado em `/usr/share/rhn` no lado do cliente. O arquivo `/etc/sysconfig/rhn/up2date` precisa de uma referência ao certificado.

Como antes, é preciso digitar o nome do servidor Spacewalk. Só é necessário executar essas etapas em sistemas já instalados. Qualquer sistema instalado do zero através do servidor Spacewalk é registrado automaticamente no servidor como parte do processo de instalação e pode, assim, acessar imediatamente o servidor ([figura 4](#)).

## Instalação kickstart

Para automatizar a instalação de novos sistemas cliente, duas informações sobre o servidor Spacewalk são necessárias: uma delas é um arquivo *kickstart* com detalhes de como instalar o novo sistema, incluindo o particionamento, a seleção de software e outras configurações que precisavam ser fornecidas no caso de uma instalação manual. A maneira mais fácil de criar um arquivo *kickstart* é selecionar *Systems/Kickstart/Profiles* na interface web.

Depois de verificar a descrição dos perfis existentes, é possível criar um novo perfil. A distribuição *kickstart* deve ser especificada como parte do arquivo de perfil. Com isso, não queremos dizer que os arquivos RPM que pertencem à distribuição que desejamos instalar, como o Fedora 12, mas sim os arquivos básicos de instalação, como a ferramenta Anaconda, por exemplo.

Os repositórios de software sincronizados anteriormente não irão fornecer por padrão uma distribuição *kickstart*,

**Figura 5** As propriedades do sistema são uma bela opção para realizar uma variedade de tarefas administrativas em um sistema através do servidor Spacewalk.

e isso significa que teremos que criar a distribuição no servidor Spacewalk. Novamente, navegue até *Systems/Kickstart/Distributions* na interface web e aponte para os arquivos necessários. A maneira mais fácil de fornecer os arquivos é montar uma instalação de CD/DVD da sua distribuição preferida através do dispositivo *loopback*:

```
mount -o loop ➔
/var/iso-images/ ➔
Fedora-23-i386-DVD.iso ➔
/var/distro-trees/Fedora-12
```

Quando uma distribuição Fedora 12 *kickstart* é criada, basta apontar o

servidor Spacewalk para o diretório `/var/distro-trees/Fedora-12`. Se tudo der certo, apenas aponte para a distribuição criada quando o arquivo *kickstart* for criado. Quando um sistema cliente é instalado a partir do zero, ele irá automaticamente pegar os arquivos dessa fonte.

Embora haja uma série de maneiras de se instalar um sistema Fedora 12 do zero, o método mais fácil é apontar todas as solicitações de cliente PXE dos seus clientes para o servidor Spacewalk com o comando `next-server`. Graças à integração do Cobbler [\[13\]](#), o servidor Spacewalk possui um servidor interno *TFTP* e lista todos os perfis de

```
#!/usr/bin/perl
use Frontier::Client;
my $HOST = 'satellite.example.com';
my $user = 'username';
my $pass = 'password';

my $client = new Frontier::Client(url => "http://$HOST/rpc/api");
my $session = $client->call('auth.login', $user, $pass);

my $systems = $client->call('system.listUserSystems', $session);
foreach my $system (@$systems) {
    print $system->{name} . "\n";
}
$client->call('auth.logout', $session);
```

**Figura 6** Uma interface XMLRPC abre uma grande seleção de funções de servidores Spacewalk através da API programável.

*kickstart* disponíveis. Para confirmar, basta digitar `cobbler profile list` na linha de comando. Quando iniciar um sistema cliente através de uma placa de rede com suporte a PXE, automaticamente será exibida uma lista dos perfis de *kickstart* existentes. Para instalar o cliente, basta selecionar o perfil desejado na lista. O cliente é automaticamente registrado no servidor Spacewalk. Os sistemas existentes podem ser reinstalados facilmente usando os comandos:

```
koan --replace-self →
--server=Spacewalk-Server →
--profile=Kickstart-Profile
```

Isso cria uma entrada no menu `bootloader` do sistema e seleciona automaticamente a entrada quando o sistema for reinicializado.

## Gerenciamento do sistema

Todos os sistemas registrados no servidor Spacewalk obtém seus pacotes de software a partir dessa fonte, sem precisar acessar repositórios externos. Esse método não só melhora sua segurança, mas também economiza largura de banda de rede. Com um sistema registrado, é possível personalizar várias definições na seção *System Properties* (**figura 5**).

Por exemplo, é possível atribuir um novo software ou canais de configuração, comparar o software instalado com perfis em outros sistemas, ou criar snapshots para backup que podem ser usados novamente mais tarde. Além disso, é possível instalar um novo software ou distribuir arquivos de configuração a partir de um local centralizado.

Graças à capacidade de atribuir sistemas registrados para os grupos, é possível apontar e clicar para fazer isso para um grande número de sistemas. O serviço `rhnrd` nos sistemas, consulta o servidor Spacewalk em

intervalos predefinidos para verificar novas ações, tais como instalações de software. Quando o sistema encontra uma ação, ele a executa. Se o serviço `osad` estiver habilitado no sistema, é possível até mesmo executar ações imediatamente, sem aguardar o intervalo de sondagem. O cliente e o servidor, então, usam o protocolo Jabber para realizar uma troca contínua de informações.

Finalmente, não esqueça a API Spacewalk, que está disponível em <http://meuservidor/rhn/apidoc/index.jsp> no servidor instalado. Essa ferramenta dá acesso a uma infinidade de funções que não estão disponíveis na interface web.

A API pode ser acessada usando `XMLRPC`, que é perfeito para seus scripts Perl ou Python. Um script Python [[8](#)]

para a criação de um canal de software serve como um exemplo de acesso ao servidor Spacewalk via da API (**figura 6**).

## Conclusão

O Spacewalk é uma ferramenta muito poderosa para o gerenciamento de instalações em larga escala de ambientes Linux. Ele facilita muitas tarefas diárias, tais como a instalação de atualizações de software ou o upload de arquivos de configuração. Os recursos avançados, como a clonagem de canal, tornam possível instalar qualquer software através de um processo com garantia de qualidade, antes de liberá-lo para uso em ambientes de produção. E, graças à disponibilidade de uma API de fácil compreensão, muitas tarefas podem ser automatizadas com o uso de scripts. ■

## Mais informações

- [1] Site do projeto Spacewalk: <https://fedorahosted.org/spacewalk/>
- [2] Portas de rede Spacewalk: <http://magazine.redhat.com/2008/09/30/tips-and-tricks-what-tcpip-ports-are-required-to-be-open-on-an-rhn-satellite-proxy-or-client-system/>
- [3] Repositório RPM RHEL5 e CentOS5 do Servidor Spacewalk: <http://spacewalk.redhat.com/yum/1.0/RHEL/5/i386/spacewalk-repo-1.0-2.el5.noarch.rpm>
- [4] Repositório RPM Fedora12 do Servidor Spacewalk: <http://spacewalk.redhat.com/yum/1.0/Fedora/12/i386/spacewalk-repo-1.0-2.fc12.noarch.rpm>
- [5] Roteiro do Spacewalk: <http://fedorahosted.org/spacewalk/roadmap/>
- [6] Grupo de discussão do Spacewalk: <http://www.redhat.com/spacewalk/communicate.html#lists/>
- [7] Oracle XE: <http://www.oracle.com/technology/software/products/database/xe/htdocs/102xelinst.html>
- [8] Script API Spacewalk para criar um canal de software: [http://fedorahosted.org/spacewalk/attachment/wiki/UploadFedoraContent/create\\_channel.py](http://fedorahosted.org/spacewalk/attachment/wiki/UploadFedoraContent/create_channel.py)

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lrm.com.br/article/4467>



# 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](http://www.lpi-brasil.org)  
[treinamentos@vectory.com.br](mailto:treinamentos@vectory.com.br)  
Tel (11) 3675-2600

# VoIP com Asterisk – parte II



O sistema telefônico ultrapassado, presente até pouco tempo, é cada vez mais substituído por tecnologias VoIP. Afinal, o que é cobrado em cobranças: cada novo recurso ativado requer uma nova ativação e um novo pagamento. É hora de mudar.

**adicado ao pagamento mensal. É hora de mudar. É hora de criar sua própria central voIP.**

**por Stefan Wintermeyer**

Na edição 72 da **Linux Magazine**, apresentamos as tendências do mercado VoIP, instruções sobre instalação, configuração, planos de discagem e telefones SIP. Nesta segunda parte do tutorial, vamos abordar a padronização de planos de discagem e contextos. Mão à obra!

## Economia com padrões

Se o plano de discagem parece desnecessariamente longo, com ao menos uma linha para cada número

### Listagem 1: sip show user 2000

```

01 * Name      : 2000
02 Secret    : <Set>
03 MD5Secret : <Not set>
04 Context   : meus-telefones
05 Language  :
06 AMA flags : Unknown
07 Transfer mode: open
08 MaxCallBRL : 384 kbps
09 CallingPres : Presentation
10 Allowed, Not Screened
11 Call limit  : 0
12 Callgroup   :
13 Pickupgroup :
14 Callerid    : "" <>
15 ACL        : No
16 Codec Order : (none)
17 Auto-Framing: No

```

chamado, não se apavore. O plano de discagem pode usar expressões regulares. Infelizmente, os desenvolvedores optaram por reinventar a roda: não é possível aplicar os padrões já conhecidos de expressões regulares. As linhas:

```

exten => 2000,1,Dial(SIP/2000)
exten => 2001,1,Dial(SIP/2001)

```

podem ser substituídas por uma única e condensada linha: `exten => _200X,1,Dial(SIP/${EXTEN})`. Esse padrão conseguiria, inclusive, efetuar chamadas para as extensões de 2003 até 2009. Todo padrão começa com um traço baixo, ou *underline* ("\_"). A extensão `exten => 200X,1,Dial(SIP/${EXTEN})` é, para o Asterisk, absolutamente lógica e correta, mas tem resultados inesperados por não incluir o underline antes do número.

O Asterisk aceita que alguém chame o número 200X, pois ele seria válido para telefones SIP (já que estes também podem usar letras). A variável  `${EXTEN}` sempre contém a extensão chamada, não o padrão – “2001” no caso da extensão “\_2001”. O conceito de variáveis será explicado em outra parte do tuto-

rial. Conheça alguns dos padrões comuns do Asterisk:

- ▶ `[ABC]`: números A, B e C. O padrão `_3[235]` equivale aos números 32, 33 e 35.
- ▶ `[A-B]`: números de A até B. O padrão `_3[2-5]` aceita os números 32, 33, 34 e 35.
- ▶ `X`: qualquer número. O padrão `_3X` coincide com os números 30, 31, 32, 33, 34, 35, 36, 37, 38 e 39.
- ▶ `..`: um ou mais números quaisquer. O padrão `_3.` aceita todos os números iniciados em 3, como 30, 32, 345 e 302303.

O padrão `_` pode causar problemas se for usado, pois o Asterisk 1.4 o interpreta diferentemente do Asterisk 1.2, e emite um alerta. Portanto, evite-o. É melhor usar como padrão para qualquer número o `_X..`

## Dispositivos e caller-ID

No arquivo `sip.conf`, é possível configurar todos os dispositivos SIP que devem receber e efetuar chamadas. Também pode ser um servidor SIP de uma operadora VoIP que encami-

nha chamadas para telefones fixos ou vice e versa. Ao usar a opção `-c` para iniciar o Asterisk, é possível usar, na linha de comando do programa, o comando `sip show users` para listar todos os usuários SIP. Para visualizar todas as informações de um usuário, como o ramal 2000 apresentado em nos nossos exemplos, use o comando `sip show user 2000` e veja um resultado semelhante à **listagem 1**.

## Conhecidos ou anônimos

Como nosso exemplo define somente os mínimos parâmetros necessários para as contas, não há muito para ver. São importantes: o nome do usuário, o ramal (que no nosso exemplo é **2000**), e seu contexto. O nome do usuário não precisa ser uma letra. É possível chamá-lo de “Pedro” e conectar-se diretamente a ele, no plano de discagem, com a linha:

```
[outros]
[meus-telefones]
exten => 2000,1,Dial(SIP/Pedro)
```

O usuário SIP usado não tem qualquer relação com as informações passadas no *callerid*. A **listagem 2** mostra um exemplo. Após o próximo `sip reload`, será exibido para cada telefone SIP o caller-ID, assim como o destinatário.

É possível que, uma vez ou outra, um participante deseje chamar um anônimo, que se registrou no Asterisk sem informar o caller-ID. É possível permitir esse recurso com uma expansão do plano de discagem. Pode-se usar o caller-ID não apenas no arquivo `sip.conf`, mas também com a função `CALLERID(all)` no plano de discagem.

A **listagem 3** demonstra um plano de discagem que, sempre que alguém chama um dos 88 números regis-

dos, torna a chamada anônima. O *caller-ID Anonymous <anonymous>* é definido pela RFC 2543 justamente com esse propósito, e todos os provedores SIP devem implementá-la corretamente. O **:4** na **linha 10** permite que o Asterisk corte os quatro primeiros dígitos da variável  `${EXTEN}`.

## Enxergar tudo em contexto

O conceito de contextos do Asterisk é a maior dificuldade de todo iniciante no Asterisk. O plano de discagem, no arquivo `extensions.conf`, é dividido em seções chamadas de contexto. Elas sempre começam com colchetes. Na **listagem 3**, há dois contextos: `[outros]` e `[meus-telefones]`. Isso é refletido no `sip.conf`, que atribui um contexto a cada telefone.

Os contextos são o principal do fluxo de chamadas. Quando o telefone **2000** chama um número, o Asterisk primeiro busca no arquivo `sip.conf` a qual contexto o usuário pertence. Em seguida, o Asterisk

## Listagem 2: sip.conf

```
01 [general]
02 port = 5060
03 bindaddr = 0.0.0.0
04 context = outros
05
06 [2000]
07 type=friend
08 context=meus-telefones
09 secret=1234
10 host=dynamic
11 callerid=Hans Meier <2000>
12
13 [2001]
14 type=friend
15 context=meus-telefones
16 secret=1234
17 host=dynamic
18 callerid=Uwe Klein <2001>
```

busca esse contexto no arquivo `extensions.conf`. Se houver qualquer erro de digitação em um dos dois arquivos, nenhuma chamada ocorrerá. Se o contexto existir, o Asterisk buscará a extensão apropriada para o número digitado pelo usuário **2000**, para que o programa consiga prosseguir nas ações a serem tomadas. Quando um sistema

## Listagem 3: 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/${EXTEN})
09 exten => _88200[1-2],1,Set(CALLERID(all)=Anonymous <anonymous>)
10 exten => _88200[1-2],n,Dial(SIP/${EXTEN}:4)
```

## Listagem 4: 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/${EXTEN})
09
10 exten => 23,1,NoOp(23 sem padrao)
11 exten => _2X,1,NoOp(${EXTEN} com padrao)
```

Asterisk não funciona conforme esperado, em 90% dos casos a falha está neste processo. Portanto, verifique sempre a digitação dos nomes dos contextos.

Em planos de discagem grandes, é comum múltiplas expressões regulares se aplicarem a uma mesma

chamada. Portanto, o Asterisk busca sempre fazer o melhor e buscar a extensão da forma mais correta. Para isso, a aplicação `NoOp()` funciona muito bem. Ela imprime na linha de comando interna do Asterisk o conteúdo passado a ela, desde que o Asterisk se encontre

pelo menos no nível `verbose 3` (`core set verbose 3`).

Digite no arquivo `extensions.conf` o plano de discagem da **listagem 4**. Em seguida, chame a partir do telefone de número `2000` o número `23` e veja no Asterisk o resultado `23 sem padrao`, informando que o `23` foi selecionado sem um padrão específico, pois coincidiu somente com o `_2X`. Felizmente, o Asterisk oferece o comando `dialplan show`, que permite testar números de destino do plano de discagem. A **listagem 5** executa de uma única vez, com `23@meus-telefones`, a chamada na extensão específica.

## Listagem 5: Testes com dialplan show

```
01 big-island*CLI> dialplan show 23@meus-telefones
02 [ Context 'meus-telefones' created by 'pbx_config' ]
03   '23' =>  1. NoOp(23 sem padrao)          [pbx_config]
04   '_2X' =>  1. NoOp(${EXTEN} com padrao)    [pbx_config]
05
06 -= 2 extensions (2 priorities) in 1 context. =-
07
08
09 big-island*CLI> dialplan show 24@meus-telefones
10 [ Context 'meus-telefones' created by 'pbx_config' ]
11   '_2X' =>  1. NoOp(${EXTEN} com padrao)    [pbx_config]
12
13 -= 1 extension (1 priority) in 1 context. =-
```

## Listagem 6: sip.conf

```
01 [general]
02 port = 5060
03 bindaddr = 0.0.0.0
04 context = outros
05
06 ; Conta SIP do provedor VoIP
07 register => 0223XXXXXX:senha@TXL93.axxesocom/0223XXXXXX
08
09 [axxesocom_saida]
10 type=friend
11 host=TXL93.axxesocom
12 fromuser=0223XXXXXX
13 username=0223XXXXXX
14 secret=senha
15 fromdomain=TXL93.axxesocom
16 context=do-provedor-sip
17 canreinvite=yes
18 qualify=yes
19 insecure=very
20 nat=no
21 dtmfmode=info
22
23 [2000]
24 type=friend
25 context=meus-telefones
26 secret=1234
27 host=dynamic
28
29 [2001]
30 type=friend
31 context=meus-telefones
32 secret=1234
33 host=dynamic
```

## Telefonemas via provedor

Chamar telefones externos é uma necessidade óbvia quando se usa um sistema telefônico via VoIP. A conexão via ISDN será tratada num artigo posterior. Tudo começa com a seleção de um provedor SIP. A qualidade dos principais provedores esteve sujeita a certa flutuação nos últimos anos.

Felizmente, a situação melhorou constantemente nos últimos meses. Mesmo assim, ainda não é possível dizer sem equívocos que um provedor é melhor que o outro. Compare os preços e ofertas de serviços dos diferentes provedores SIP e experimente tantos quantos conseguir. O exemplo a seguir utiliza as configurações necessárias para o provedor alemão Axxeso [\[1\]](#).

Até aqui, o Asterisk sempre funcionou como servidor. Os telefones SIP se registraram nele e o utilizaram para chamar outros telefones SIP também registrados. Para fazer chamadas por meio de operadoras SIP, o Asterisk precisa se registrar nos servidores de sua(s) operadora(s) como um cliente. A **listagem 6** mostra um arquivo `sip.conf` correspondente.

A armadilha do Asterisk é a necessidade de incluir a instrução `register` na seção `[general]` do arquivo `sip.conf` em vez de em cada seção de um provedor. Se a linha `register` estiver fora da seção `[general]`, o Asterisk não conseguirá efetuar chamadas por meio desse provedor, pois seu registro nele não funcionará. A maioria dos provedores possui, em seus sites, exemplos da configuração correta do arquivo `sip.conf`. Vale a pena conferir.

## Contextos de entrada e saída

É importante, neste ponto, incorporar a linha externa no plano de discagem. É preciso distinguir as diferenças entre dois contextos diferentes: o `[meus-telefones]` interno e o `[do-provedor-sip]`, que somente recebe ligações. Se as chamadas vindas do provedor SIP precisarem cair no telefone `2000`, digite no `extensions.conf` as linhas da **Listagem 7**.

Ao reiniciar o Asterisk com o comando `restart now`, veja como o Asterisk se registrou como usuário SIP no provedor externo. O comando `sip show registry` informa os detalhes disso, e `sip show users` exibe uma lista de todos os usuários SIP.

Analizar o plano de discagem não é mais tão complicado. A extensão `_X.` coincide com qualquer número que tenha ao menos dois caracteres. Se você possuir múltiplos números em um único provedor, é possível fornecer uma extensão para cada um. Se o telefone `1111-1111` precisar ser enviado ao telefone `2000` e o `2222-2222` for para o `2001`, defina essa parte do plano de discagem da seguinte forma:

```
...
[do-provedor-sip]
exten => 11111111,1,Dial(SIP/2000)
exten => 22222222,1,Dial(SIP/2001)
```

## Listagem 7: 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})
09
10 [do-provedor-sip]
11 exten => _X.,1,Dial(SIP/2000)
```

## Listagem 8: 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/${EXTEN})
09 exten => _0X.,1,Dial(SIP/${EXTEN}:1)@axxes0_saida)
10
11 [do-provedor-sip]
12 exten => 11111111,1,Dial(SIP/2000)
13 exten => 22222222,1,Dial(SIP/2001)
```

Quem aceita chamadas pelo provedor SIP também pode fazer chamadas por ele. Porém, não há semelhanças entre as chamadas recebidas e originadas por meio do provedor externo. A **Listagem 8** ilustra o plano de discagem adequado. Quando você

discar `0`, o Asterisk o desconsiderará e conectará o aparelho ao número desejado por meio do provedor SIP.

Na próxima edição da **Linux Magazine**, vamos falar sobre secretária eletrônica e demais configurações nos planos de discagem. Até lá! ■

## Mais informações

[1] Axxeso: <http://www.axxes0.de/>

## 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](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lnm.com.br/article/4455>



Segurança

# Criptografia de arquivos e diretórios

O eCryptfs criptografa seus dados com transparência, oferecendo uma proteção extra contra invasões e roubos de informações.

por Juliet Kemp

**O**eCryptfs [1] oferece criptografia PGP (Pretty Good Privacy ou Privacidade Muito Boa, em tradução livre) em nível de arquivo para Linux (**figura 1**). Toda vez que for preciso gravar um arquivo em um diretório criptografado pelo eCryptfs no disco rígido, o aplicativo irá criptografá-lo silenciosamente; cada vez que um arquivo do diretório for lido, o eCryptfs irá descriptografá-lo da mesma maneira. Esse processo acontece nos bastidores, e a configuração padrão usa a sessão de login do usuário para armazenar a chave de criptografia, tornando todo o processo contínuo e automático no login. Uma das vantagens de criptografia em nível de arquivo, ao contrário da criptografia no nível de bloco (todo o sistema) fornecida por outras ferramentas de criptografia é que é possível ter várias chaves no mesmo sistema. Isto significa que os usuários podem criptografar seus dados separadamente, ou um único usuário pode criptografar diretórios específicos ou até mesmo arquivos separadamente. Diferentes usuários podem ainda utilizar o mesmo diretório com chaves diferentes, e cada um pode descriptografar apenas seus próprios arquivos.

Caso o Ubuntu seja instalado a partir do zero, há a opção de criptografar sua pasta pessoal como parte do processo de instalação.

Além disso, é possível criar facilmente um novo usuário com um diretório `home` criptografado (certifique-se de ter instalado o pacote `cryptfs-utils`) com o seguinte comando: `sudo adduser --encrypt-home newusername`.

Infelizmente, esse comando só funciona no Ubuntu, e embora o Debian suporte o eCryptfs, ele não suporta (no momento) a opção `--encrypt-home` para `adduser`, nem suporta a criação de diretórios `home` criptografados na instalação. Felizmente, caso esteja usando o Debian, ou se já tiver um sistema operacional Ubuntu e não quiser criar um novo usuário apenas para criptografia, é possível instalar e configurar o eCryptfs, desta forma:

```
sudo apt-get install ecryptfs-
-utils
ecryptfs-setup-private
```

Esse comando cria um diretório `~/Private` e o criptografa. Ao se desconectar, o diretório será armazenado como `~/.Private`; e quando voltar a se conectar, ele será automaticamente montado como `~/Private/`. Sua senha

de login é usada para armazenar sua senha de criptografia.

Sua melhor aposta é permitir que o eCryptfs gere uma senha aleatória (uma senha aleatória será provavelmente muito mais difícil de quebrar do que qualquer coisa que você criar). É uma boa ideia armazenar a senha em algum lugar separado. Em caso de desastre (ou se esquecer sua senha de login!), use o seguinte comando para exibir a saída:

```
ecryptfs-unwrap-passphrase
.ecryptfs/wrapped-passphrase
```

Agora é possível escolher quais diretórios serão criptografados: mova-os para `~/Private`, e crie um link simbólico a partir da sua localização anterior. Por exemplo, para mover o diretório `.ssh`, use os seguintes comandos:

```
cd
mv .ssh Private/
ln -s Private/.ssh .ssh
```

Quando se desconectar (ou desmontar o diretório `Private`), o conteúdo do diretório e os nomes dos arquivos serão criptografados, para que nenhum outro usuário na máqui-



**Figura 1** Criptografia silenciosa com eCryptfs.

na seja capaz de identificar o que há nesse diretório. Mover um diretório comum para o diretório criptografado, criptografa-o automaticamente.

Se não quiser que *Private* seja automaticamente montado no login, exclua o arquivo `~/ecryptfs/auto-mount` (e `~/.ecryptfs/autounmount`). Ambos são arquivos vazios, bastando um `touch` para recriá-los e configurar o *auto-mount* novamente. Lembre-se sempre de que, se diretórios ou arquivos importantes forem movidos para *Private*, poderá haver erros no início da sessão, especialmente se todos os arquivos relacionados ao desktop foram movidos.

## Criptografar um diretório manualmente

Se não quiser que seu diretório criptografado fique em `~/Private`, ou se quiser um segundo diretório criptografado (talvez com uma chave separada), é possível configurar manualmente a criptografia em um diretório diferente, desse modo:

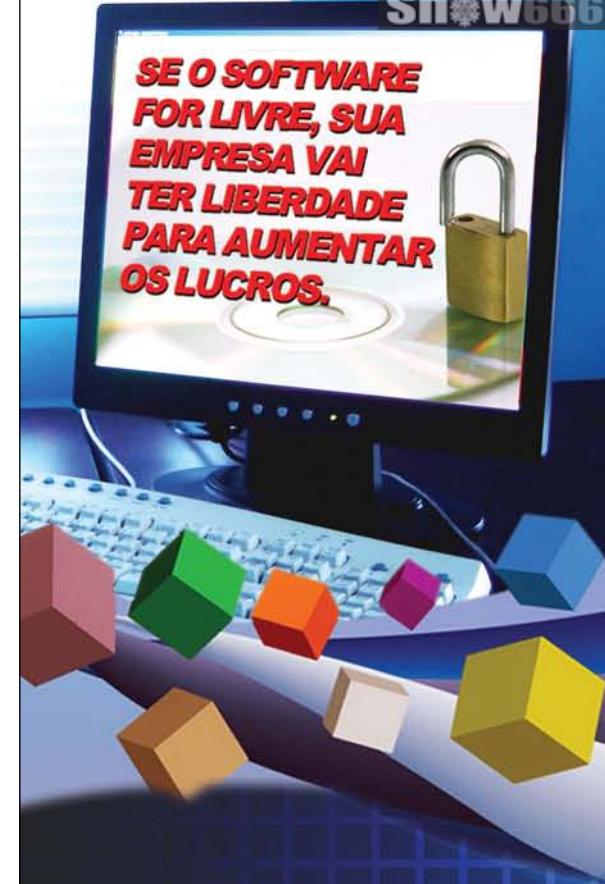
```
mkdir ~/secret
chmod 700 ~/secret
sudo mount -t ecryptfs secret ↵
secret
```

Será solicitada uma cifra e o comprimento da chave (basta usar as opções padrão se não estiver familiarizado com as opções mais complexas).

Além disso, será preciso informar se deseja permitir a passagem de texto puro. Esse recurso permite que os arquivos que não sejam de posse do eCryptfs sejam lidos e escritos dentro de uma montagem eCryptfs.

Embora isso possa ser útil em algumas situações, também tem a grande desvantagem de que não é possível ter certeza de que todos os arquivos nesse diretório estão protegidos. A configuração padrão é para desativá-lo, o que geralmente é a melhor escolha. A criptografia de nomes de arquivos faz o esperado: ela criptografa os nomes de arquivos, bem como seu conteúdo. Assim, apenas você pode ver os nomes dentro do seu diretório criptografado, e somente quando ele é montado com o eCryptfs. É melhor habilitar esse recurso, como padrão, pois ele vem desabilitado.

Uma senha será solicitada. Como essa será a primeira vez que essa montagem será utilizada, espere até ser avisado de que essa frase-senha não foi usada antes. Além disso, será



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](http://www.f13.com.br)**

**F13**  
T E C N O L O G I A

preciso informar se é preciso armazená-la no *keyring root* para evitar esse aviso no futuro.

Nos argumentos do comando `mount`, o primeiro caminho é o diretório que estiver sendo montando através do eCryptfs, e o segundo caminho é o ponto de montagem do eCryptfs. Essas configurações podem ser diferentes, mas montar dois diretórios distintos no mesmo ponto significa que os arquivos na pasta criptografada devem sempre ser acessados via eCryptfs. Isso também faz a coisa toda funcionar de forma transparente.

Depois que terminar de usar esse diretório, já é possível desmontá-lo. Agora, se tentar olhar para um arquivo no diretório, verá uma sequência de criptografia no lugar do nome do arquivo (supondo que a criptografia de nome de arquivos esteja habilitada). Se examinar os conteúdos de cada arquivo, eles serão exibidos como se estivessem em modo binário. As desvantagens com relação à criptografia manual de diretórios são duas: um problema, é que é preciso fornecer as opções de criptografia cada vez que voltar a montar o diretório. É possível passar essas opções na linha de comando da seguinte forma:

```
sudo mount -t ecryptfs secret/ ↪
secret/ -o ecryptfs_cipher=aes, ↪
ecryptfs_key_bytes=16, ↪
ecryptfs_passthrough=n
```

Infelizmente, a criptografia do nome do arquivo não tem nenhuma opção de linha de comando. Observe que é possível montar o mesmo diretório com e sem criptografia de

nome de arquivo em diversas ocasiões sem problemas.

A outra desvantagem é que é preciso autenticar-se como *root* para montar esse diretório. Para corrigir isso, monte o diretório como *root*, então verifique o arquivo `/etc/mtab` para obter as opções, e adicione o usuário *user* a elas. Em seguida, adicione a linha resultante, que deve ser algo parecido com a **Listagem 1**, no arquivo `/etc/fstab`, então desmonte o diretório com `sudo umount /secret`.

Em seguida, será preciso adicionar a chave manualmente no mollo de chaves (*keyring*) da sessão de usuário com o `ecryptfs-manager`. Escolha a opção **1** (*add passphrase key to keyring*) e digite sua senha; em seguida, escolha a opção **4** para sair. Agora, quando digitar `mount -i newsecret` (a opção **-i** evita chamar o auxiliar de montagem), será possível usar seu diretório criptografado. Para limpar o *keyring* de sessão, desmonte-o e use `keyctl clear@u`.

Mais duas etapas permitirão fazer tudo isso automaticamente no login. Para começar, adicione a linha `mount -i secret` ao seu `~/.bashrc`. Em seguida, adicione no arquivo `/etc/pam.d/login` a seguinte linha: `auth required pam_ecryptfs.so`.

Agora, quando sair e entrar novamente, verá que `secret/` foi montado automaticamente. Depois, será possível (se quiser) fazer a coisa toda de novo com outra frase-senha para outro diretório.

Se quiser, é possível criptografar o seu diretório `home` inteiro em vez de apenas criar um novo usuário, mas este é um processo bastante complicado. Para obter instruções sobre

como fazer isso, veja o post no blog de Dustin Kirkland's [\[2\]](#).

## Aumentar a segurança

Sua frase-senha do eCryptfs está armazenada no arquivo `~/ecryptfs/wrapped-passphrase` e é simetricamente criptografada com sua senha de logon do computador. Por padrão, sua frase-senha de `mount` é uma chave de 128 bits gerada aleatoriamente e que é difícil de lembrar, mas também difícil de adivinhar. Quando montar seu diretório eCryptfs, a frase-senha de montagem é carregada no *keyring* do kernel.

Se também estiver criptografando nomes de arquivo, uma segunda chave é usada, e essa também fica no *keyring* do kernel. Essas chaves são utilizadas cada vez que for necessário acessar um arquivo do seu diretório criptografado.

Este processo é conhecido como criptografia de dois fatores: é preciso usar o arquivo `wrapped-passphrase` e sua senha de login para acessar os dados criptografados. Como alternativa, é possível ligá-los à sua mídia removível e depois removê-la quando estiver longe da máquina.

Se quiser aumentar sua segurança, é possível armazenar esse arquivo em uma mídia removível (como um *pendrive* USB) ao invés de em seu disco rígido, o que significa que quem roubar seu laptop também terá que roubar a chave de segurança. Em seguida, crie um link de `~/ecryptfs/wrapped-passphrase` para o arquivo na sua mídia removível. (Para uma segurança extra, use um nome pouco óbvio). Observe que é preciso se certificar de ter adicionado uma linha em `/etc/fstab` para que sua mídia removível seja sempre montada no mesmo diretório: `/dev/sdb1 /media/usbkey ext3 defaults 0 0`. É ainda mais importante neste momento fazer um backup de sua senha em outro lugar – *pendrives* USB são úteis, mas são muito fáceis de perder!

### Listagem 1: Montagem de diretórios

```
/home/juliet/secret /home/juliet/secret ecryptfs user,rw, ↪
ecryptfs_sig=9ffcd5087c0c049,ecryptfs_fnek_sig=9ffcd5087c0c049, ↪
ecryptfs_unlink_sigs,ecryptfs_cipher=aes,ecryptfs_key_bytes=16 0 0
```

Além disso, é possível tentar a opção `-w` com o `cryptfs-setup-private`, que usa uma frase-senha separada (não a sua frase-senha de logon). Esta opção potencialmente oferece mais segurança (o invasor teria que adivinhar duas senhas), mas significa que o diretório não pode ser montado automaticamente no login.

## Backup de dados

Para fazer backup de seu diretório criptografado, demonte-o e use qualquer utilitário de backup. Os arquivos serão copiados de forma criptografada, e será possível acessá-los com a chave correta, exatamente como faria em relação ao original. Da mesma forma, não será possível acessá-los sem criptografia.

Embora não seja preciso tomar quaisquer medidas adicionais para proteger seus dados, lembre-se que, se perder seu arquivo de chave pública (ou esquecer sua senha), não será possível acessar seus dados. Mais uma vez, faça uma cópia de backup do arquivo de chave e mantenha-o em algum lugar seguro.

## eCryptfs e diretórios de sistema

Também tenha em mente que os dados sensíveis, por vezes, podem ser gravados em locais diferentes do seu diretório `home` – como por exemplo, no diretório `/tmp`.

Portanto, considere configurar sua máquina para usar eCryptfs para outras pastas, dependendo da criticidade dos seus dados.

É possível fazer isso da mesma maneira com que foi criado um diretório manualmente criptografado. Apenas certifique-se de adicionar a linha relevante em `/etc/fstab` para que os usuários que não tenham privilégios de `root` possam montar o diretório em questão.

Se já há dados no diretório, o processo é um pouco mais complicado

do que criar um diretório a partir do zero. Para começar, faça backup de seu velho diretório e, em seguida, siga os seguintes passos:

- 1 Crie o novo diretório. Ele deve ter um nome temporário diferente do diretório antigo. Configure-o como já descrito.
- 2 Monte-o e copie todos os arquivos do diretório antigo.
- 3 Renomeie o diretório antigo (`/mydir_bk`, por exemplo) e desmonte o diretório criptografado.
- 4 Mude o nome do novo diretório, edite o arquivo `/etc/fstab` de forma adequada, e depois remonte-o.

Os dados agora devem estar criptografados. O passo seguinte é salvar o diretório antigo como um backup até ter certeza de que tudo foi movido com êxito. No caso do diretório `/tmp`, faria mais sentido apenas apagar todos os antigos dados temporários, excluir o diretório, e recriá-lo como um diretório criptografado.

Além disso, é possível configurar o espaço de `swap` para ser criptografado. Criptografar o espaço de `swap` vai fazer os recursos de hibernação e de `sleep` pararem de funcionar (a equipe do Ubuntu está atualmente trabalhando nesse problema), mas vai garantir que cópias de arquivo descriptografadas não permaneçam no seu espaço de `swap`.

Para criptografar sua partição `swap`, instale `cryptsetup`, em seguida, execute `sudo cryptsetup-luks`, o que irá desmontar sua partição `swap`, criptografá-la e remontá-la novamente.

Infelizmente, apesar de uma nova entrada ser adicionada a `/etc/fstab` automaticamente, a entrada antiga não é removida. Será preciso editar o arquivo `/etc/fstab` (como `root`), e remover a entrada antiga do `swap`. A nova entrada do `swap` será identificada com `/dev/mapper/cryptswap` – essa é a linha de `swap` que precisa ser mantida.

Para informações atualizadas sobre o eCryptfs e muitos tutoriais, visite o blog de Dustin Kirkland [3]. ■

## Mais informações

- [1] eCryptfs: <https://launchpad.net/ecryptfs/>
- [2] Migrar para um diretório home criptografado: <http://blog.dustinkirkland.com/2009/06/migrating-to-encryptedhome-directory.html>
- [3] Blog de Dustin Kirkland: <http://blog.dustinkirkland.com/>

## Sobre a autora

**Juliet Kemp** se diverte com Linux desde que descobriu que ele é mais interessante do que revisão final, e é administradora de sistemas há cinco anos. Ela acredita que quanto mais automatizados forem os sistemas, mais tempo livre teremos para quando algo der realmente errado. Ou para navegar na Internet.

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lnm.com.br/article/4456>



# O observador

*Os desenvolvedores do Icinga se cansaram de esperar por atualizações da popular ferramenta de monitoramento de redes Nagios, e começaram o seu próprio e promissor projeto.*

**por Falko Benthin**

Um servidor pode sofrer por muitas razões: recursos do sistema como CPU, memória RAM, disco rígido sobrecarregado, ou serviços de rede podem cair. Dependendo das aplicações sendo executadas em um servidor, as consequências podem ser terríveis – desde usuários irritados até perdas de dados que geram grandes implicações financeiras.

Portanto, em um mundo altamente conectado a redes, é mais importante do que nunca ser capaz de monitorar o estado de seu servidor e agir imediatamente.

Logicamente, é possível verificar cada servidor e serviço individualmente, mas é muito mais conveniente usar uma ferramenta de monitoramento inteligente como o Icinga.

## Era uma vez, o Nagios

Projeto relativamente jovem, o Icinga [1] é proveniente do poderoso e popular Nagios [2], que foi descontinuado por causa de divergências sobre o ritmo e a direção do desenvolvimento da ferramenta.

O Icinga oferece melhores conectores a banco de dados (para MySQL, Oracle e PostgreSQL), uma interface

web mais amigável, e uma API que permite que os administradores integrem inúmeras extensões sem uma alteração complicada do núcleo do Icinga. Os desenvolvedores do Icinga também procuram refletir e implementar sugestões enviadas através da análise das necessidades da comunidade, além de preocuparem-se em aplicar patches de segurança ou correções de vulnerabilidades mais rapidamente. A primeira versão estável, a 1.0, foi lançada em dezembro de 2009, e o número da versão vem aumentando a cada dois meses em média, desde então.

O aplicativo contém três componentes: o núcleo, a API e a interface web, que é opcional. O núcleo reúne as informações sobre a saúde do sistema geradas por plugins e as passa através da interface IDOMOD ao *Icinga Data Out Database* (IDODB) ou ao *daemon* de serviço IDO2DB. A API baseada em PHP aceita informações do IDODB e as exibe em uma interface web. Além disso, a API facilita o desenvolvimento de complementos e plugins. O Icinga Web é projetado para ser uma interface web avançada, que pode ser facilmente personalizada para que os administradores monitorem com facilidade os sistemas que gerenciam. Até o momento da publicação desta edição da Linux Magazine, o Icinga Web estava na

**Tabela 1: Opções do Icinga**

Opção Servidor	
Servidor	Status
o	OK
d	Inoperante
u	Fora de alcance
r	Recuperado
Serviços	
o	OK
w	Cuidado
c	Crítico
r	Recuperado
u	Desconhecido

versão *beta*, e tinha alguns erros que tornam difícil recomendar seu uso em produção. Se você só precisa controlar um único servidor, o Icinga é instalado facilmente. Algumas distribuições oferecem binários em seus repositórios, mas se não, ou se preferir usar a versão mais recente, a documentação é fácil de entender e inclui um guia de iniciação rápida (para o banco de dados via `lib-dbi` com `IDOUtils`), que pode ajudar a configurar o monitor de rede em pouco tempo e que estará disponível no endereço [http://meu\\_servidor/\\_icinga](http://meu_servidor/_icinga), assim que o software estiver instalado. Os desafios surgem quando é preciso monitorar um número maior de computadores.

O Icinga pode monitorar os recursos privados em um computador, incluindo CPU, memória RAM e uso do disco, bem como serviços externos como a web, SSH, e-mail, e assim por diante. O ambiente de rede do laboratório é composto por três computadores, um dos quais atua como o servidor Icinga; os outros dois são um servidor web e um servidor de arquivos, que enviam informações para o servidor de monitoramento. Como nenhum método nativo permite solicitar informações sobre a carga da CPU, memória RAM, ou o uso de espaço em disco, será preciso instalar em cada máquina, uma ex-

## Listagem 1: my\_hosts.cfg

```

01 # Servidor web
02 define host{
03   host_namewebserver
04   aliaslanguagecenter
05   display_nameServer at ↵
      language center
06   address141.20.108.124
07   active_checks_enabled1
08   passive_checks_enabled0
09   max_check_attempts3
10   check_commandcheck-host-alive
11   check_interval5
12   retry_interval1
13   contactsspz_admin
14   notification_period24x7
15   notification_interval160
16   notification_optionsd
17 }
18
19 #Fileserver
20 define host {
21   host_namefileserver
22   aliasFileserver
23   display_nameFileserver
24   address192.168.10.127
25   active_checks_enabled1
26   passive_checks_enabled0
27   max_check_attempts3
28   check_commandcheck-host-alive
29   check_interval5
30   retry_interval1
31   contactsadmin
32   notification_period24x7
33   notification_interval160
34   notification_optionsd,u,r
35 }
```

## Listagem 2: Trecho de my\_services.cfg

```

01 # Definições de serviços
02 define service{
03   host_namewebserver
04   service_descriptionHTTP
05   active_checks_enabled1
06   passive_check_enabled0
07   check_commandcheck_http
08   max_check_attempts3 ;how ↵
      often to perform the check ↵
      before Icinga notifies
09   check_interval5
10  retry_interval1
11  check_period24x7
12  contactsspz_admin
13  notifications_enabled1
14  notification_periodweekdays
15  notification_interval160
16  notification_optionsw,c,u,r
17 }
18 define service{
19   host_namefileserver, ↵
      webserver
20   service_descriptionSSH
21   active_checks_enabled1
22   passive_checks_enabled0
23   check_commandcheck_ssh
24   max_check_attempts3
25   check_interval15
26   retry_interval1
27   check_period24x7
28   contactsadmin
29   notifications_enabled0
30 }
```

tensão como o NRPE [3], que coleta essas informações. O servidor remoto Icinga vai fazê-lo executar os plugins na máquina local e transmitir as in-

formações necessárias. O Icinga envia ao administrador do sistema todas as informações necessárias e alerta o administrador em caso de emergên-

## Listagem 3: Trecho de commands.cfg

```

01 # 'notify-service-by-email' command definition
02 define command{
03   command_namenotify-service-by-email
04   command_line /usr/bin/printf "%b" "* Icinga *\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService: ↵
      $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/ ↵
      Time:$LONGDATETIME$\n\nAdditional Info:$\n$SERVICEOUTPUT$" | /usr/bin/mail -s \"***$NOTIFICATIONTYPE$ ↵
      Service Alert: $HOSTALIAS$/SERVICEDESC$ is $SERVICESTA
05 TE$ ***" $CONTACTEMAIL$
06}
07
08 # 'check-host-alive' command definition
09 define command{
10   command_namecheck-host-alive
11   command_line$USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100% -p
12   5
13 }
```

## Listagem 4: Trecho de timeperiods.cfg

```

01 define timeperiod{
02 timeperiod_name 24x7
03 alias24 Hours A Day, 7 →
Days A Week
04 sunday00:00-24:00
05 monday00:00-24:00
06 tuesday00:00-24:00
07 wednesday00:00-24:00
08 thursday00:00-24:00
09 friday00:00-24:00
10 saturday00:00-24:00
11 }
12
13 define timeperiod{
14 timeperiod_name wochentags
15 aliasRobot Robot
16 monday07:00-17:00
17 tuesday07:00-17:00
18 wednesday07:00-17:00
19 thursday07:00-17:00
20 friday07:00-17:00
21 }

```

cia. Os recursos avançados – que são uma verdadeira ajuda no trabalho di-

ário –, incluem grupos, ambientes de monitoramento redundantes, escala de notificação e horários de verificação. O Icinga diferencia as verificações ativa e passiva. Verificações ativas são iniciadas pelo serviço Icinga e executados em horários especificados pelo administrador. Em uma verificação passiva, um aplicativo externo faz o trabalho e encaminha os resultados para o servidor Icinga, que é útil caso não seja possível verificar ativamente o computador (por exemplo, ele fica atrás de um firewall). Um grande número de plugins [4] já existe para várias finalidades no Nagios e no Icinga. Mas antes da primeira verificação, o administrador precisa configurar os computadores e os serviços que serão monitorados pelo Icinga.

Os elementos individuais envolvidos em uma verificação são chamados de objetos por ele. Os objetos incluem hosts, serviços, contatos, comandos

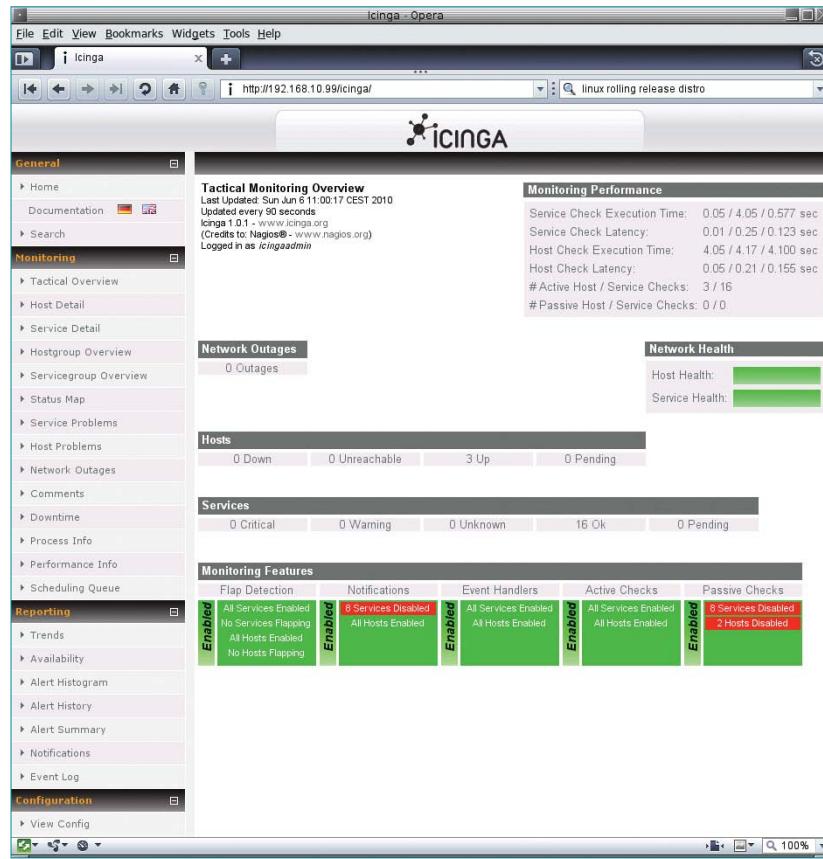
e período de tempo. Para facilitar o trabalho diário, é possível agrupar os hosts, serviços e contatos. Os objetos individuais são definidos nos arquivos CFG, que residem no diretório `etc/objects` do Icinga. O monitor de rede inclui uma série de exemplos de definições de vários objetos que os administradores precisam customizar. É possível definir vários objetos em um arquivo CFG, mas também dá para criar arquivos separados para cada objeto em um diretório abaixo de `/path-to-Icinga/etc/objects`. As linhas que começam com uma hash dentro de uma definição de objeto são consideradas comentários, assim como tudo dentro de uma linha à direita de um ponto e vírgula.

## Definição de hosts e serviços

A **Listagem 1** contém um exemplo de definição de host. Para informar o administrador (`contacts`), quando o servidor cair (`notification_options`), vamos fazer com que o Icinga dê um ping (`check_command`) no servidor a cada 5 minutos (`check_interval`). Se o servidor ainda estiver inoperante por 60 minutos (`notification_interval`), após notificação ao administrador, uma nova mensagem será enviada.

O Icinga é capaz de decidir se um determinado host está offline ou inacessível (**tabela 1**). No entanto, para determinar se um host está inacessível, é preciso definir os nós que foram informados ao host como `parents` – e isso só vai funcionar se as rotas para os pacotes de saída forem conhecidas. A definição do servidor de arquivos é semelhante.

Uma vez que os servidores estão definidos, o administrador configura os respectivos serviços que o Icinga irá acompanhar (**Listagem 2**), junto com os comandos correspondentes (**Listagem 3**), os intervalos (**Listagem 4**) e os administradores *stakeholding* (**Listagem 5**). Os arquivos de con-



**Figura 1** Hosts e serviços em funcionamento.

figuração individuais têm uma estrutura similar. Para cada serviço, é preciso considerar o intervalo entre as verificações. Um recurso útil é a capacidade de definir intervalos de tempo, dentro do qual o Icinga vai realizar verificações e, se necessário, notificar o administrador. Limitações de tempo podem ser definidas nessa fase.

A configuração de contato pode incluir endereços de email ou números de telefone celular, mas para integrar cada contato com, por exemplo, um gateway *Email2SMS* ou um sistema *Text2Speech*, é preciso um comando correspondente.

O Icinga pode usar macros, que simplificam e aceleram consideravelmente muitas tarefas, pois um comando único pode ser usado para vários hosts e serviços. As **listagens 2** e **3** dão exemplos de macros.

Todos os serviços definidos para o monitoramento do servidor de arquivos incluem uma instrução `check_nrpe` seguida de um ponto de exclamação. Cada ponto de exclamação pode ser seguido por um argumento, que por sua vez é avaliado pelas macros em outras definições. Macros são informadas através de caracteres \$.

Depois de criar os arquivos de configuração e armazená-los no diretório `etc/objects`, ainda é preciso informar ao Icinga onde estes estão, adicionando um novo `cfg_file=/usr/local/icinga/etc/objects/object.cfg` ao arquivo de configuração principal, `/etc/icinga.cfg`. Após fazer isso, verifique a configuração, `/caminho-para-Icinga/bin/icinga -v /caminho-para-Icinga/etc/icinga.cfg`; supondo que não haja erros, reinicie o Icinga com o comando `/etc/icinga/init.d restart`.

## Interface gráfica e mensagens

O Icinga funciona sem uma interface gráfica, mas é muito melhor ter uma. A interface padrão não pode

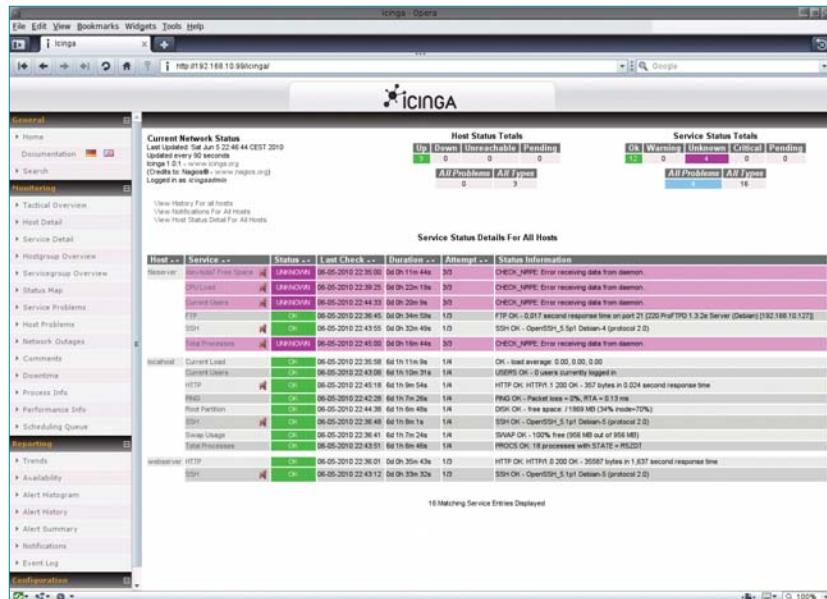
### Listagem 5: Trecho de contacts.cfg

```
01 define contact{
02   contact_nameicingaadmin
03   aliasFalko Benthin
04   host_notifications_enabled    1
05   service_notifications_enabled1
06   host_notification_period     24x7
07   service_notification_period   24x7
08   host_notification_options    d,u,r
09   service_notification_options  w,u,c,r
10  host_notification_commandsnotify-host-by-email
11  service_notification_commandsnotify-service-by-email
12  emailroot@localhost
13 }
```

negar sua ancestralidade ao Nagios, mas é clara e intuitiva.

Se tudo estiver funcionando, haverá muitos sinais verdes na interface do usuário (**figura 1**), mas se algo der errado em algum lugar,

a cor irá mudar, ficando cada vez mais próxima do vermelho, para refletir o estado dos *hosts* ou serviços (**figuras 2** e **3**). As mensagens de status são geralmente links, de modo que clicar em uma men-



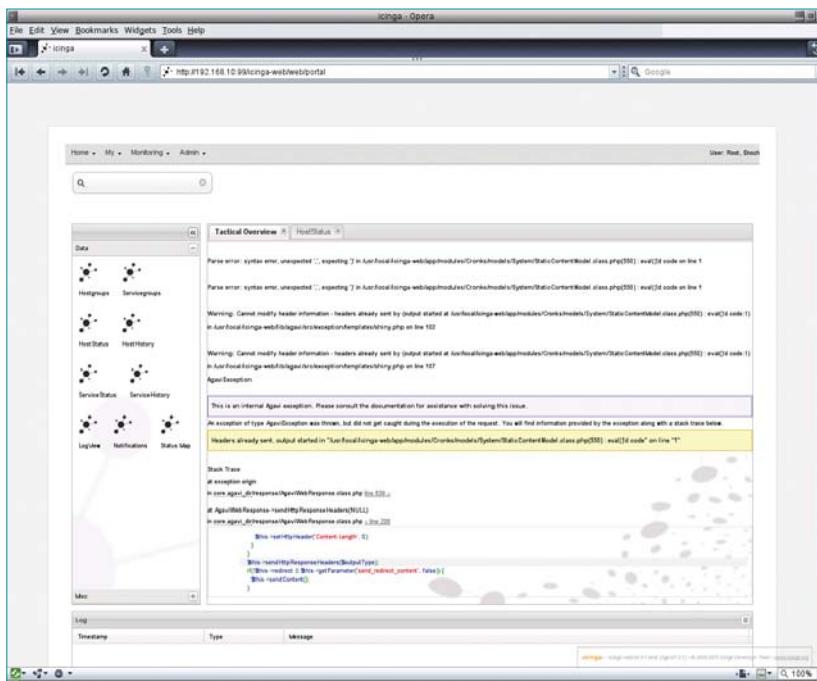
**Figura 2** Tudo está funcionando, mas o plugin NRPE está causando problemas.



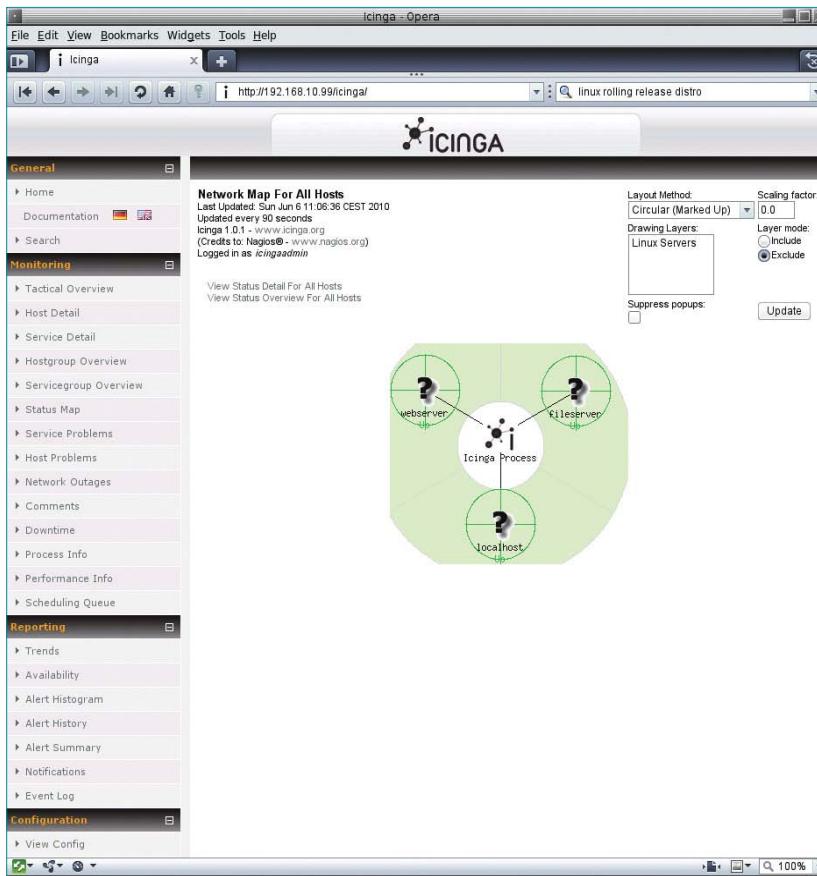
**Figura 3** Uma verificação manual dos comandos revela o culpado pelo problema.



**Figura 4** As mensagens de email enviadas pelo Icinga são curtas e diretas



**Figura 5** O Icinga Web versão beta não é muito convincente. A versão 1.0.3 já saiu.



**Figura 6** Visão geral da rede. Se for preciso monitorar muitas máquinas e ter "parents" definidos, também é possível visualizar os nós intermediários.

sagem exibirá informações mais detalhadas.

Se algo estiver drasticamente errado e uma mensagem é necessária, o Icinga irá verificar o seu conjunto complexo de regras para ver se deve enviar uma mensagem e, em caso afirmativo, para quem (**figura 4**). Os filtros através dos quais a mensagem passa verificam o seguinte: se as notificações são necessárias, se o problema ocorreu em um momento em que o *host* e o serviço deveriam estar sendo executados, se as mensagens devem ser enviadas para este serviço no horário atual e se os contatos relacionados ao serviço realmente a desejam. Cada contato pode definir suas próprias regras para estipular quando quer receber mensagens e para qual status. Se existem vários administradores que pertencem a um único grupo, o Icinga irá notificar todos eles. Novamente, é possível definir períodos de notificação individual para que cada administrador seja responsável por um período de tempo.

## Recursos interessantes

O Icinga contém várias características interessantes que permitem que os administradores personalizem o monitor de rede para refletir suas necessidades e o ambiente do sistema. Por exemplo, é possível definir ambientes distribuídos de monitoramento. Se for preciso monitorar centenas ou milhares de *hosts*, o servidor Icinga poderia eventualmente ficar sobre-carregado porque cada verificação ativa exige recursos de sistema. Para eliminar um pouco da carga do servidor principal, o Icinga pode delegar tarefas individuais para servidores auxiliares que, por sua vez, enviam os resultados para um servidor central. O agendamento das verificações também pode ajudar a reduzir essa carga. Em vez de executar todas as verificações em paralelo, é possível deixar o Icinga organizá-las.

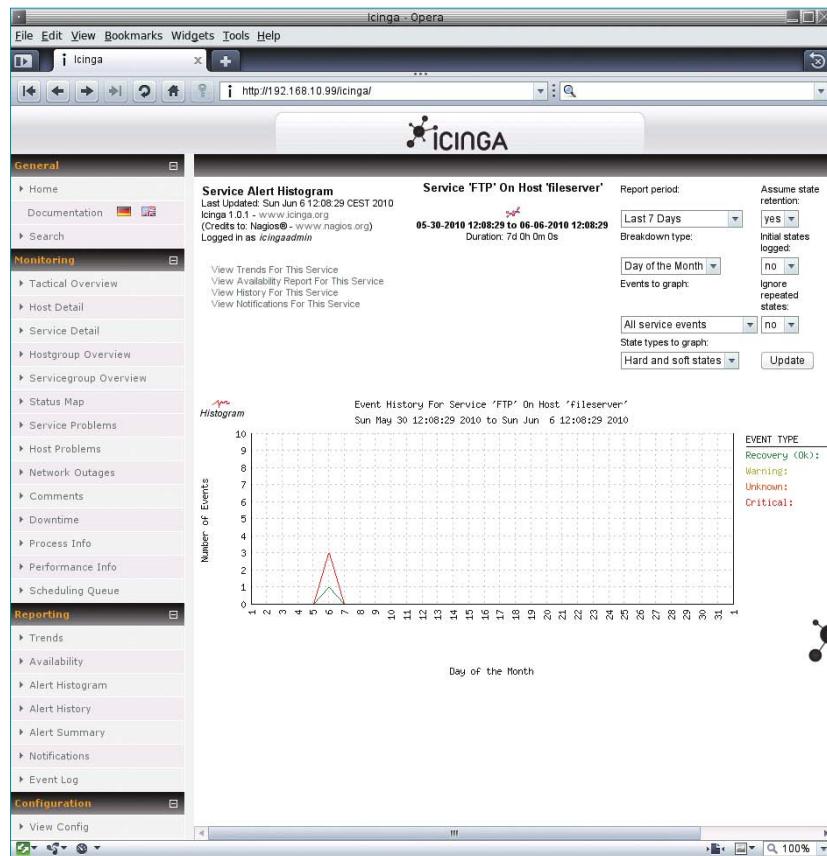
Outra característica interessante é a capacidade de escalar as notificações. Nem todo administrador pode estar disponível e pronto para a ação o tempo todo. Se o contato notificado pelo Icinga não responder dentro de um período definido, o Icinga pode tentar estabelecer contato por outro canal (por exemplo, um telefone celular em vez de um email). Se essa notificação também falhar, o caso pode ser passado para alguém mais acima na cadeia de responsabilidade – o líder da equipe, por exemplo.

## Conclusão

O Icinga é uma ferramenta complexa que fornece serviços de valor sempre que um administrador precisar monitorar computadores em uma rede. Mas não espere configurar o monitor de rede em poucos minutos; se tudo correr bem, a instalação e configuração vão demorar pelo menos algumas horas. Depois de ter lutado com a configuração completa, haverá a recompensa de um horário de almoço prolongado: se acontecer alguma coisa que necessite de sua atenção, o Icinga irá informá-lo.

A interface web tradicional é clara e repleta de informações, mas até o momento, no entanto, a nova interface não está totalmente convincente ([figura 5](#)). A instalação foi complicada, a documentação, algumas vezes, exigiu certa imaginação e o resultado final foi decepcionante. A interface estava com alguns *bugs* e muito lenta em nosso servidor de teste do Icinga, que na verdade não é muito poderoso (Via C3, 800 MHz, 256 MB de RAM). Como padrão, um novo nome de usuário e senha são necessários para o Icinga Web. Dito isso, porém, a situação atual revela algum potencial, mas é interessante verificar de tempos em tempos como a nova interface se desenvolve.

O Icinga está bem documentado, é abrangente e não deixa perguntas



**Figura 7** O histograma de alerta, outro recurso útil oferecido pelo Icinga, mostra momentos de pico de problemas.

sem respostas. O Icinga também oferece uma infinidade de dispositivos úteis, tais como o mapa de status ([figura 6](#)) ou o histograma de alerta ([figura 7](#)), tornando menos cansativo o trabalho de monitorar hosts – pelo menos inicialmente. A

profundidade das informações que o Icinga fornece é impressionante e promete soluções para evitar problemas com os usuários. Em suma, o Icinga é uma ferramenta que torna a vida do administrador mais agradável. ■

## Mais informações

- [1] Icinga: <http://www.icinga.org/>
- [2] Nagios: <http://www.nagios.org/>
- [3] NRPE: <https://git.icinga.org/>
- [4] Plugins do Nagios: <http://sourceforge.net/projects/nagiosplug/>

## Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em [cartas@linuxmagazine.com.br](mailto:cartas@linuxmagazine.com.br)

Este artigo no nosso site:  
<http://lnm.com.br/article/4461>



# 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](mailto: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
<b>Bahia</b>										
IMTECH	Salvador	Av. Antonio Carlos Magalhaes, 846 – Edifício MaxCenter – Sala 337 – CEP 41825-000	71 4062-8688	<a href="http://www.imtech.com.br">www.imtech.com.br</a>	✓	✓	✓	✓	✓	✓
Magiclink Soluções	Salvador	Rua Dr. José Peroba, 275. Ed. Metrópolis Empresarial 1005, STIEP	71 2101-0200	<a href="http://www.magiclink.com.br">www.magiclink.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Ceará</b>										
F13 Tecnologia	Fortaleza	Rua Padre Valdevino, 526 – Centro	85 3252-3836	<a href="http://www.f13.com.br">www.f13.com.br</a>	✓	✓	✓	✓	✓	✓
Nettton Tecnologia e Segurança da Informação	Fortaleza	Av. Oliveira Paiva, 941, Cidade dos Funcionários – CEP 60822-130	85 3878-1900	<a href="http://www.nettton.com.br">www.nettton.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Espírito Santo</b>										
Linux Shopp	Vila Velha	Rua São Simão (Correspondência), 18 – CEP: 29113-120	27 3082-0932	<a href="http://www.linuxshopp.com.br">www.linuxshopp.com.br</a>	✓	✓	✓	✓	✓	✓
Megawork Consultoria e Sistemas	Vitória	Rua Chapot Presvot, 389 – sl 201, 202 – Praia do Canto CEP: 29055-410	27 3315-2370	<a href="http://www.megawork.com.br">www.megawork.com.br</a>	✓	✓	✓	✓	✓	✓
Spirit Linux	Vitória	Rua Marins Alvarino, 150 – CEP: 29047-660	27 3227-5543	<a href="http://www.spiritlex.com.br">www.spiritlex.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Goiás</b>										
3WAY Networks	Goiânia	Av. Quarta Radial, 1952. Setor Pedro Ludovico – CEP: 74830-130	62 3232-9333	<a href="http://www.3way.com.br">www.3way.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Minas Gerais</b>										
Instituto Online	Belo Horizonte	Av. Bias Fortes, 932, Sala 204 – CEP: 30170-011	31 3224-7920	<a href="http://www.institutoonline.com.br">www.institutoonline.com.br</a>	✓	✓	✓	✓	✓	✓
Linux Place	Belo Horizonte	Rua do Ouro, 136, Sala 301 – Serra – CEP: 30220-000	31 3284-0575	<a href="http://corporate.linuxplace.com.br">corporate.linuxplace.com.br</a>	✓	✓	✓	✓	✓	✓
Microhard	Belo Horizonte	Rua República da Argentina, 520 – Sion – CEP: 30315-490	31 3281-5522	<a href="http://www.microhard.com.br">www.microhard.com.br</a>	✓	✓	✓	✓	✓	✓
TurboSite	Belo Horizonte	Rua Paraíba, 966, Sala 303 – Savassi – CEP: 30130-141	0800 702-9004	<a href="http://www.turbosite.com.br">www.turbosite.com.br</a>	✓	✓	✓	✓	✓	✓
Zarafa Brasil	Belo Horizonte	Rua dos Goitacazes, 103 – Sala 2001 – CEP: 30190-910	31 2626-6926	<a href="http://www.zarafabrasil.com.br">www.zarafabrasil.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Paraná</b>										
iSolve	Curitiba	Av. Cândido de Abreu, 526, Cj. 1206B – CEP: 80530-000	41 252-2977	<a href="http://www.isolve.com.br">www.isolve.com.br</a>	✓	✓	✓	✓	✓	✓
Mandriva Conectiva	Curitiba	Rua Tocantins, 89 – Cristo Rei – CEP: 80050-430	41 3360-2600	<a href="http://www.mandriva.com.br">www.mandriva.com.br</a>	✓	✓	✓	✓	✓	✓
Telway Tecnologia	Curitiba	Rua Francisco Rocha 1830/71	41 3203-0375	<a href="http://www.telway.com.br">www.telway.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Pernambuco</b>										
Fuctura Tecnologia	Recife	Rua Nicarágua, 159 – Espinheiro – CEP: 52020-190	81 3223-8348	<a href="http://www.fuctura.com.br">www.fuctura.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Rio de Janeiro</b>										
Clavis Segurança da Informação	Rio de Janeiro	Av. Rio Branco 156, 1303 – Centro – CEP: 20040-901	21 2561-0867	<a href="http://www.clavis.com.br">www.clavis.com.br</a>	✓	✓	✓	✓	✓	✓
Linux Solutions Informática	Rio de Janeiro	Av. Presidente Vargas 962 – sala 1001	21 2526-7262	<a href="http://www.linuxsolutions.com.br">www.linuxsolutions.com.br</a>	✓	✓	✓	✓	✓	✓
Múltipla Tecnologia da Informação	Rio de Janeiro	Av. Rio Branco, 37, 14º andar – CEP: 20090-003	21 2203-2622	<a href="http://www.multipla-ti.com.br">www.multipla-ti.com.br</a>	✓	✓	✓	✓	✓	✓
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4º andar Centro – CEP: 20030-012	21 2220-7055	<a href="http://www.nsi.com.br">www.nsi.com.br</a>	✓	✓	✓	✓	✓	✓
Open IT	Rio de Janeiro	Rua do Mercado, 34, Sl. 402 – Centro – CEP: 20010-120	21 2508-9103	<a href="http://www.openit.com.br">www.openit.com.br</a>	✓	✓	✓	✓	✓	✓
Unipi Tecnologias	Campos dos Goytacazes	Av. Alberto Torres, 303, 1ºandar – Centro – CEP: 28035-581	22 2725-1041	<a href="http://www.unipi.com.br">www.unipi.com.br</a>	✓	✓	✓	✓	✓	✓
<b>Rio Grande do Sul</b>										
4up Soluções Corporativas	Novo Hamburgo	Pso. Calçadão Osvaldo Cruz, 54 sl. 301 CEP: 93510-015	51 3581-4383	<a href="http://www.4up.com.br">www.4up.com.br</a>	✓	✓	✓	✓	✓	✓
Definitiva Informática	Novo Hamburgo	Rua General Osório, 402 - Hamburgo Velho	51 3594-3140	<a href="http://www.definitiva.com.br">www.definitiva.com.br</a>	✓	✓	✓	✓	✓	✓
RedeHost Internet	Gravataí	Rua Dr. Luiz Bastos do Prado, 1505 – Conj. 301 CEP: 94010-021	51 4062 0909	<a href="http://www.redehost.com.br">www.redehost.com.br</a>	✓	✓	✓	✓	✓	✓
Solis	Lajeado	Av. 7 de Setembro, 184, sala 401 – Bairro Moinhos CEP: 95900-000	51 3714-6653	<a href="http://www.solis.coop.br">www.solis.coop.br</a>	✓	✓	✓	✓	✓	✓
DualCon	Novo Hamburgo	Rua Joaquim Pedro Soares, 1099, Sl. 305 – Centro	51 3593-5437	<a href="http://www.dualcon.com.br">www.dualcon.com.br</a>	✓	✓	✓	✓	✓	✓
Datarecover	Porto Alegre	Av. Carlos Gomes, 403, Sala 908, Centro Comercial Atrium Center – Bela Vista – CEP: 90480-003	51 3018-1200	<a href="http://www.datarecover.com.br">www.datarecover.com.br</a>	✓	✓	✓	✓	✓	✓
LM2 Consulting	Porto Alegre	Rua Germano Petersen Junior, 101-Sl 202 – Higienópolis – CEP: 90540-140	51 3018-1007	<a href="http://www.lm2.com.br">www.lm2.com.br</a>	✓	✓	✓	✓	✓	✓
Lnx-IT Informação e Tecnologia	Porto Alegre	Av. Venâncio Aires, 1137 – Rio Branco – CEP: 90.040.193	51 3331-1446	<a href="http://www.lnx-it.inf.br">www.lnx-it.inf.br</a>	✓	✓	✓	✓	✓	✓
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3301-1408	<a href="http://www.tehospedo.com.br">www.tehospedo.com.br</a>	✓	✓	✓	✓	✓	✓
Propus Informática	Porto Alegre	Rua Santa Rita, 282 – CEP: 90220-220	51 3024-3568	<a href="http://www.propus.com.br">www.propus.com.br</a>	✓	✓	✓	✓	✓	✓
<b>São Paulo</b>										
Ws Host	Arthur Nogueira	Rua Jerere, 36 – Vista Alegre – CEP: 13280-000	19 3846-1137	<a href="http://www.wshost.com.br">www.wshost.com.br</a>	✓	✓	✓	✓	✓	✓
DigiVoice	Barueri	Al. Juruá, 159, térreo - Alphaville – CEP: 06455-010	11 4195-2557	<a href="http://www.digivoice.com.br">www.digivoice.com.br</a>	✓	✓	✓	✓	✓	✓
Dextra Sistemas	Campinas	Rua Antônio Paioli, 320 – Pq. das Universidades – CEP: 13086-045	19 3256-6722	<a href="http://www.dextra.com.br">www.dextra.com.br</a>	✓	✓	✓	✓	✓	✓
Insigne Free Software do Brasil	Campinas	Av. Andrade Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	<a href="http://www.insignefreesoftware.com">www.insignefreesoftware.com</a>	✓	✓	✓	✓	✓	✓
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	<a href="http://www.microcamp.com.br">www.microcamp.com.br</a>	✓	✓	✓	✓	✓	✓
PC2 Consultoria em Software Livre	Carapicuíba	Rua Edeia, 500 - CEP: 06350-080	11 3213-6388	<a href="http://www.pc2consultoria.com">www.pc2consultoria.com</a>	✓	✓	✓	✓	✓	✓

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
Cariri Livre. Em busca do conhecimento "Software Livre"	20 de novembro a 20 de dezembro	Juazeiro do Norte/CE	<a href="http://www.caririlivre.blogspot.com/">www.caririlivre.blogspot.com/</a>
5th WiMax Brazil Conference & Expo	01 de dezembro	São Paulo, SP	<a href="http://www.networkeventos.com.br/">www.networkeventos.com.br/</a>
Oracle OpenWorld América Latina 2010	07 a 09 de dezembro	São Paulo, SP	<a href="http://www.oracle.com/br/openworld/">www.oracle.com/br/openworld/</a>
Campus Party	17 a 23 de janeiro	São Paulo, SP	<a href="http://www.campus-party.com.br/">www.campus-party.com.br/</a>

## Índice de anunciantes

Empresa	Pág.
Caixa Econômica Federal	02
Locaweb	07
Rede Host	09
Central Server	11
UOL Host	15
WatchGuard	17
Academy	19
Unodata	23
Impacta	27
Vectory	63
Bull	83
Senac	84



## Nerdson – Os quadrinhos mensais da Linux Magazine

**Nerdson** não vai à escola

**ASPIRA LINUX**

A DISTRITO PRA QUEM NÃO É CAVEIRA

Uma iniciativa da fundação ODPC (One Distro Per Child)

VOCÊ ESQUECEU DE TROCAR A LOGO DO VÁRZEA PELA NOSSA.

CORRIGIDO.

QUE TAL USAR POR PADRÃO UM TEMA QUE TENTA COPIAR O DO WINDOWS XP? PRA FICAR MAIS FÁCIL PRO PESSOAL...

CARA, ALGUM DIA TEREMOS NOSSO PRÓPRIO REPOSITÓRIO.

É UMA BOA, MAS SERÁ QUE NÃO VAI DAR AOS USUÁRIOS AQUELA SENSAÇÃO RUIM DE TAMAGOTCHI FALSIFICADO?

AH! TAMBÉM PODEMOS ANUNCIAR QUE HÁ UMA COLEÇÃO DE FERRAMENTAS COMO EDITOR DE TEXTOS, PLANILHAS DE CÁLCULO, NAVEGADOR WEB E TOCADORES DE MÍDIAS!

BOA! A GALERA VAI CURTIR ISSO!

SINTO-ME TÃO BEM COLABORANDO COM O SOFTWARE LIVRE. SEREMOS CONVIDADOS PARA VÁRIOS EVENTOS!

Meses depois... (no DistroWatch.com)

The following distributions match your criteria: Discontinued

999. Aspira Linux

Aspira Linux is a brazilian distribution desktop features with CompizFusion

creative commons nerdson.com

# 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](mailto:anuncios@linuxmagazine.com.br)

11 3675-2600

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



# Linux Magazine #74

PREVIEW



## Integração Windows-Linux

Desktops Windows e servidores Linux: como tornar essa combinação mais eficiente? Três artigos vão fornecer os fundamentos da instalação e da configuração do Samba, do LDAP e do Gosa<sup>2</sup> – este último uma poderosa interface web de gerenciamento integrado de redes e sistemas. Um quarto artigo completa a série de matérias de capa, mostrando como integrar as tecnologias abordadas nos três primeiros artigos. ■

## VoIP com Asterisk – parte III

Confira na próxima edição, a terceira parte do super tutorial de Asterisk, abordando secretaria eletrônica e configurações adicionais no protocolo SIP. ■

# 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](http://www.bull.com)

**BULL**

Architect of an Open World™

# APRENDA A TRANSFORMAR INFORMAÇÃO EM INOVAÇÃO.

MULTIPLIQUE  
SUAS CHANCES

**FAÇA CURSOS DE TI COM FOCO  
EM REDES E INFRAESTRUTURA NO SENAC.**

CURSOS PREPARATÓRIOS PARA CERTIFICAÇÕES,  
TÉCNICOS, DE GRADUAÇÃO E PÓS-GRADUAÇÃO.

O SENAC SABE QUE A DEMANDA POR TECNOLOGIA NÃO PARA DE CRESCER.  
POR ISSO, FAZ PARCERIAS COM AS MELHORES EMPRESAS, OFERECE MODERNA  
INFRAESTRUTURA, O MELHOR PORTFÓLIO DE CURSOS E PROFESSORES CERTIFICADOS  
POR FORNECEDORES, COMO CISCO, MICROSOFT, FURUKAWA E LPI. O SENAC VALORIZA  
A TEORIA NA PRÁTICA, ESTIMULA A INOVAÇÃO E O EMPREENDEDORISMO.  
É POR ISSO QUE O MERCADO ESTÁ DE OLHO NO SENAC.

BOLSAS DE ESTUDO - CONHEÇA CRITÉRIOS ACESSANDO [WWW.SP.SENAC.BR/BOLSASDESTUDO](http://WWW.SP.SENAC.BR/BOLSASDESTUDO)

**senac**  
são paulo

0800 883 2000  
[WWW.SP.SENAC.BR](http://WWW.SP.SENAC.BR)

Parceiros Tecnológicos:



**Autodesk**  
Authorized Training Center

**COREL**  
TRAINING PARTNER 2010



**Microsoft**  
GOLD CERTIFIED  
Partner

Learning Solutions

**ORACLE**  
WORKFORCE DEVELOPMENT PROGRAM



**Project Management Institute**  
Registered Education Provider

