COLUNA

Coluna do Kurt

Como perder seu becape

Quem precisa de invasores quando você tem administradores de sistemas? Aprenda por que copiar seus dados não significa que eles estão seguros.

No momento em que eu escrevo esta coluna, não posso deixar de refletir sobre a ironia de ter acabado de perder um mês inteiro de dados. Entrando no espírito deste artigo, eu estava lidando com alguns becapes no meu servidor web quando acidentalmente apaguei boa parte do diretório `/var/` e todo o diretório `/home/`. Não teria sido tão mau se eu não tivesse feito becapes diários em `/home/becape/`. Ops.

Fazer é diferente de ter

Se os seus dados não estão disponíveis, assim como os sistemas que os processam e os disponibilizam, você tem um problema. No caso do meu servidor web, a perda do `/var/` e do `/home/` o deixou um tanto quanto inútil. Ele exibia erros 404 e nada mais. Para ter certeza de que os dados estão disponíveis, é preciso fazer becape. Parece simples? Na realidade, a maioria de nós (eu, inclusive) não entende o conceito corretamente, e embora tenhamos a intenção de fazer um becape, o que nós estamos de fato fazendo é apenas copiando os dados para algum outro lugar igualmente vulnerável a perdas.

No meu caso, cometi o clássico erro de guardar meus becapes no mesmo sistema onde estavam os dados – e, para piorar a situação, eu os mantinha num diretório frequentemente acessado. Mas isso era o de menos. O servidor tinha apenas um disco rígido. Bastaria uma falha de disco para perder meus dados completamente, não importa quantos becapes eu tivesse feito. Mesmo que eu instalasse um segundo disco rígido na máquina, ainda seria fácil um evento qualquer (erro na controladora do disco, ataques, incêndios, inundações, curto-circuitos, furtos etc.) ocasionar a perda de mais de um disco.

Becapes legítimos?

Há três elementos principais que devem ser considerados ao fazer becapes legítimos. Número um: tenha certeza de que você fez becape dos dados. Tenho visto muitos sistemas que salvam os dados em CDs, DVDs ou fitas de forma inadequada, o que resulta em dados irrecuperáveis. É preciso testar cada becape que se faz, mas se isso não for possível, faça no mínimo checagens ocasionais para ter certeza de que os dados podem ser recuperados.

Número dois: mantenha becapes externos em regime somente-leitura (ou o mais próximo possível disso). Isto não significa necessariamente que eles têm de estar em um local físico diferente (embora esta seja sempre uma boa ideia), mas eles têm de estar separados, pelo menos o suficiente para que uma simples falha ou evento, como a formatação de um disco ou a perda de um servidor, não venha a acabar tanto com os dados quanto com os becapes. Um exemplo perfeito disso (além, naturalmente, da minha recente gafe) foi o site AVSIM Online, que perdeu 13 anos de dados em decorrência de um simples ataque. De acordo com relatos, o AVSIM Online tinha dois servidores que copiavam e faziam becape de seus dados mutuamente. Como já disse antes, muitos de nós estamos apenas copiando dados quando fazemos becapes, e não fazendo becapes reais. Neste caso, um invasor acessou os dois servidores, uma vez que eram basicamente idênticos, e eliminou todos os dados e as cópias realizadas em ambos os servidores. O AVSIM Online perdeu seu site, emails, arquivos, fóruns e muito mais, e muito provavelmente nunca obterá os dados de volta. No meu caso, tive sorte. Perdi apenas um mês de arquivos de log e dados coletados, então tudo o que tive de fazer foi esperar um mês para recolher novos dados – que bom que não eram os registros financeiros de alguém.

Número três: tenha certeza de que você não vai apagar os arquivos de becape ou zerar o conteúdo do arquivo a menos que tenha 100% de certeza de que nunca precisará do arquivo novamente. Por este motivo, RAID não é uma solução de becape. Mesmo se você tiver vários discos rígidos em uma configuração RAID de modo que a perda de uma ou mesmo de várias unidades não cause

APRESENTAMOS O NOVO LIMITE DOS PLANOS DE HOSPEDAGEM UOL HOST.

MAIS DE 150.000 CLIENTES JÁ UTILIZAM!

HOSPEDAGEM ILIMITADA UOL HOST.

O UOL HOST acaba de lançar seus novos planos, sem limites de transferência de dados e sem limite de domínios, com preços a partir de R$ 7,90*. Além disso, suporte técnico, construtor de sites, e-mails e o mais moderno Painel de Controle para administração da sua hospedagem. Agora o céu é o limite para a audiência de seu site.

0800 723 6000
www.uol.com.br/host

UOL HOST
QUALIDADE EM SERVIÇOS WEB

*Nos primeiros 3 meses, depois R$14,90. Promoção válida até 30/08/2009.

a perda de dados, você ainda pode perdê-los por apagar (`rm`, `mkfs` etc.) ou alterar os arquivos (`cat foo > bar`).

As opções

Felizmente, quase todos os programas de becape maduros trabalham recebendo dados e armazenando-os em outro lugar – muitas vezes em um servidor dedicado, RAID, fita, DVD, e assim por diante. Existem algumas excelentes opções para Linux: o *Amanda*, que vem em quase todas as distribuições, bem como o *backupPC* e o *Bacula*, ambos abordados recentemente na Linux Magazine. Embora eu não cite seus detalhes aqui, basta dizer que são muito poderosos, têm várias opções de configuração e definitivamente fazem becape de seus dados se configurados corretamente. Uma opção rápida e "sujinha" é o *Rsync*.

Problemas do Rsync

O Rsync foi concebido para manter grandes quantidades de arquivos sincronizados entre diferentes sistemas ou diretórios. Por isso, ele faz um bom trabalho como ferramenta auxiliar de becape. Normalmente, eu faço becapes locais no sistema com `tar` e `mysqldump`, colocando os arquivos em um diretório com data (você verá por que mais adiante). Para usar o Rsync, basta criar o arquivo `/etc/rsyncd.conf` com o seguinte conteúdo:

```
uid = becapes
gid = becapes
use chroot = yes
[becapes]
      path = /becapes/
      read only = yes
```

Em seguida, habilite-o no *inetd* ou *xinetd*. No cliente, basta uar um comando como `rsync -a 10.1.2.3::becapes/* /meusbecapes/` para copiar o conteúdo do diretório `/becapes/` do servidor 10.1.2.3 para o seu diretório `/meusbecapes/` local. A fim de ter certeza de que nada de ruim aconteça, veja que eu não usei a opção `--delete`, que permitiria ao Rsync apagar os arquivos locais que não estão mais presentes no diretório remoto. O que poderia dar errado? Se um arquivo for removido no servidor, eu ainda terei uma cópia local, certo? Sim, mas se um arquivo for apagado por um invasor ou por um erro de script (por exemplo, `cat 0 > arquivo`), a cópia local também será apagada. Em outras palavras, diga adeus aos seus dados. Como a solução é fazer becapes incrementais, eu salvo meus becapes diários em um diretório que tem a data como nome e sincronizo somente esse diretório:

```
rsync -a 10.1.2.3::becapes/`date +%Y-%m-%d`
➥/meusbecapes/
```

Tudo que estiver entre acentos graves é executado pelo shell e o resultado é utilizado no comando. Isso significa que, na pior das hipóteses, eu posso perder o becape de hoje, mas não perderei os becapes antigos porque eles estarão em diretórios separados no meu servidor.

Onde estão seus becapes?

Então, agora você tem becapes diários, copiados do servidor para outra máquina mais segura. Ou não? Muitas vezes os programas automatizados falham, os endereços IP e os nomes das máquinas mudam, a configuração do Rsync é alterada, a partição de becapes do disco se enche, ou o que mais puder acontecer. A última peça do quebra-cabeça são as notificações automáticas para alertar sobre o sucesso ou a falha do becape. Os programas mencionados acima (Amanda, Bacula etc.) suportam o recurso de notificação, mas como implementar o recurso de notificação com o Rsync? A solução para isso é simples e elegante: basta adicionar a seguinte linha ao script de becape:

```
ls -la /meusbecapes/`date +%Y-%m-%d` | mail -s
➥ "Relatório diário de becape" seu@email.com
```

Esse comando fará uma listagem do novo diretório de becape e redirecionará a saída para o comando `mail`, enviando um email com uma listagem de todos os arquivos e seus tamanhos. Na verdade, você pode ir ainda mais longe e listar arquivos dentro de arquivos com o comando `tar -t`, se achar melhor. Na maioria dos casos, o comando `rsync` com a opção `-v` (*verbose*) gera a seguinte saída:

```
enviando lista de arquivos....OK
2009-05-27/
2009-05-27/home.tar.bz2
2009-05-27/etc.tar.bz2
```

Note que se você executar comandos pelo *crontab*, a saída será automaticamente enviada por email para o usuário.

Teste dos becapes

Alguns diriam que esse passo final é o mais importante ao fazer becapes. Primeiro, é preciso descompactar seus becapes, inserir a fita no leitor ou fazer o que for preciso para restaurar os dados; caso contrário, como você poderia ter certeza de que eles funcionarão? Depois disso, você poderá dormir tranquilamente sabendo que as catástrofes naturais (ou administradores de sistema) não estragarão seu dia. ■

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.

DigiVoice

A DigiVoice quer investir no crescimento de seu maior bem: você.

Líder Nacional no mercado de placas, a DigiVoice sabe que não basta apenas ter o melhor produto para satisfazer seus clientes.
É preciso auxiliá-los a extrair o máximo desses produtos, para que também possam atender bem as necessidades do mercado em suas aplicações.

Pensando nisso, A DigiVoice inaugurou um centro de treinamento onde são oferecidos diversos cursos que tratam desde os aspectos teóricos de telefonia e TI até as aplicações e técnicas de vendas dos seus produtos. Centenas de profissionais já participaram e aprovaram os treinamentos, confirmando o Êxito dessa iniciativa.

No mês de Agosto, a DigiVoice quer ir além e oferece dois grandes incentivos para que você possa **crescer** e se aperfeiçoar.

*Promoção válida até dia 31 de agosto de 2009.

Na compra das placas de voz DigiVoice*:

1) Ganhe desconto nos treinamentos sobre Asterisk.

Treinamento Asterisk Básico de **R$ 1500,00** por apenas **R$ 999,00**
Treinamento Asterisk Avançado de **R$ 2400,00** por apenas **R$ 1299,00**

2) Ganhe uma assinatura anual da LINUX MAGAZINE

(11) 3081-8877
www.digivoice.com.br