Brincando de Backup com rSync.

Autoria de Thiago J. Ruiz (Neo)
25/09/2006
Última Atualização 06/10/2006

A necessidade de se manter um backup de todas as informações/dados dos clientes se faz cada vez mais presente para nós administradores de redes, existem milhares de ferramentas capazes de suprir essa necessidade por exemplo o Amanda, Bacula (umas com facilidade, outras não tão fáceis), nesse artigo vou comentar o rSync que é uma ferramenta simples e segura pois envolve Criptografia quando necessário através do SSH com uma chave DSA provendo um túnel criptografado para fazer a transmissão dos arquivos pela rede por exemplo, que é o que cobrirei neste artigo.

Conteúdo:

1. Instalando rSync# cd /usr/ports/net/rsync
make config

Escolha a opção SSH, salve e saia.

make install clean

Estes passos devem ser seguidos tanto no seu servidor que fará o backup quanto no seu servidor que será "backupeado".

2. Montando estrutura de backupNeste ponto é necessário listarmos todas as pastas que temos que fazer backups e de quais servidores extrairemos esses arquivos e também para onde irão, vou usar como exemplo um servidor com o nome "ORIGEM" e de IP 192.168.1.254 de onde serão copiados os arquivos para o servidor chamado "DESTINO" com o IP 192.168.1.253 que será o nosso servidor de backup.

Então iremos salvar a pasta /home do servidor ORIGEM.
Para o servidor DESTINO na pasta /backups.
Faremos que o pedido do backup parta do DESTINO.

Então no DESTINO crie as pastas /backups e /backups/del

DESTINO# mkdir /backups
DESTINO# mkdir /backups/del

3. Criando chave de criptografia para tunelamentoNeste passo devemos escolher qual usuário fará o backup, ele deve existem em ambos os servidores e também tem de ter permissões de leitura no mínimo nas pastas que serão backupeadas, optei por utilizar o usuário backup que tem permissões totais e também existe em ambos os servidores.

Você irá me perguntar:
Mas não vai ser inseguro?
Eu vou responder:
Não com criptografia alta e com o SSH bem configurado como mostrarei no próximo passo.

Então vamos criar as chaves:

DESTINO# ssh-keygen -b 2048 -t dsa

Ele pedirá para que você insira uma frase (senha) para a chave dê enter apenas deixe-a em branco, senão não poderemos automatizar o serviço, pois toda vez que se for fazer o backup é necessário digitar esta senha (você vai acordar pra digitar a senha todo dia? creio que não)

Este comando criará dentro do home do usuário backup (/home/backup/) uma pasta oculta chamada ".ssh" entre nela:

DESTINO# cd ~/.ssh
DESTINO# ls -la

-rw-r--r-- 1 backup wheel 1128 Jul 3 12:41 id_dsa.pub
-rw-r--r-- 1 backup wheel 1128 Jul 3 12:41 id_dsa

EM HIPÓTESE ALGUMA DEIXE ALGUÉM TER ACESSO A ESSAS CHAVES.

DESTINO# cat id_dsa.pub
Este comando retornará algo parecido com isso:

ssh-dss A9AAB3NzaC1iGMqHpSCEliaouBun8FF9t8p...

Copie esta saída para o home do usuário backup no servidor ORIGEM na pasta ".ssh" para o arquivo chamado authorized_keys:

ORIGEM# vi ~/.ssh/authorized_keys

Cole, salve e saia.

Pronto geramos as chaves que farão a criptografia do túnel por onde os arquivos transitarão.

4. Configurando o SSHTanto no servidor ORIGEM quanto no servidor DESTINO é necessário agora configurar para que só ocorram logins utilizando chave de criptografia, sem elas nem aparecerá um prompt de senha, não rodaremos também um SSH aberto na porta padrão para o backup podemos fazer com que seja aberto outro daemon do SSH além do que utilizamos normalmente para manutenções nos servidores ouvindo numa rede específica e numa porta bem alta, dificultando ainda mais o acesso,

em ambos os servidores:

Primeiro editaremos o SSH de conexão normal (fazendo uma palinha na segurança)

cd /etc/ssh/
vi sshd_config

VersionAddendum RESTRICTED
Port 2211
Protocol 2
ChallengeResponseAuthentication no
PasswordAuthentication no
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
UseDNS no

:wq!

Agora editaremos a configuração do arquivo de SSH por onde transitará o backup

ORIGEM# vi /etc/ssh/sshd_backup_config

VersionAddendum RESTRICTED
Port 65222
Protocol 2
ListenAddress 192.168.1.254
PasswordAuthentication no
ChallengeResponseAuthentication no
AuthorizedKeysFile .ssh/authorized_keys
AllowTcpForwarding no
UseDNS no

PidFile /var/run/sshd_backup.pid

:wq!

Agora precisamos fazer com que o sistema inicialize os dois SSH's no boot

ORIGEM# vi /etc/rc.conf

```
sshd_enable="YES"
sshd_backup_enable="YES"
```

Se faz também necessário criar um script para que o sshd_backup "suba" segue abaixo exemplo:

```
#!/bin/sh

. /etc/rc.subr

name="sshd_backup"
rcvar=`set_rcvar`
start_cmd="sshd_backup_start"
stop_cmd="sshd_backup_stop"
pid_file="/var/run/sshd_backup.pid"

load_rc_config $name
eval "${rcvar}=\${${rcvar}:-'NO'}"
sshd_backup_args=${sshd_backup_args:-"-f /etc/ssh/sshd_backup_config"}

sshd_backup_start()
{
/usr/sbin/sshd $sshd_backup_args
}

sshd_backup_stop()
{
if [ -f $pid_file ]; then
kill `cat /var/run/sshd_backup.pid`
fi
}

run_rc_command "$1"
```

Salve-o como sshd_backup.sh na pasta /usr/local/etc/rc.d/ com permissão de execução
e "suba-o"

```
ORIGEM# chmod 755 /usr/local/etc/rc.d/sshd_backup.sh
ORIGEM# /usr/local/etc/rc.d/sshd_backup.sh start
```

Pronto, agora temos dois SSH's rodando um ouvindo nas redes externas e a outra apenas em um IP interno, porém, todos só aceitam conexão mediante apresentação da chave de criptografia.
Veja a saída do comando abaixo:

```
ORIGEM# sockstat -4l | grep sshd
root    sshd      4935  3  tcp4   192.168.1.254:65222    *:*
root    sshd      27271 4  tcp4   *:2211      *:*
```

SSH's configurados e o do backup protegido na rede interna, vamos ao próximo passo.

5. Scripts para automatização do serviço.Bom, já instalamos, dizemos quem será backupeado e onde será feito isto, e também preparamos o meio da comunicação entre essas pontas com um toque legal de segurança.
Então agora vamos preparar os scripts que farão o serviço por nós toda noite, sem complicações pois como dizem o pessoal da lista FUG-BR "as coisas tendem a dar certo quando são simples" e eu concordo plenamente com eles.

Segue abaixo o script:

```
#!/bin/sh
### Script de Backup
### Thiago J. Ruiz
### 20-09-06

# Programas
rsync="/usr/local/bin/rsync -avzH --delete-during --backup"

#  A opção "--delete-during" é para deletar no destino os arquivos que foram deletados na origem.
#  A opção "--backup" serve para fazer um backup dos arquivos deletados na origem para uma outra # pasta
# a qual deve ser especificada com a opção "--backup-dir" que você verá abaixo.
# Para mais informações execute o comando "man rsync" no prompt


ssh="/usr/bin/ssh -p 65222 -i /home/backup/.ssh/id_dsa"

#  O SSH que se conectará a origem especificando a porta e o arquivo da chave
#  Para mais informações execute o comando "man ssh" no prompt


# Origem dos Dados
origem="/home"

# IP do servidor de ORIGEM
host="192.168.1.254"

# Destinos dos Dados
destino="/backups/"

# Arquivos que foram deletados da Origem irão para esta pasta pela opção "--backup-dir"
origem_del="/backups/del/"

# Fazendo BACKUP

$rsync --backup-dir=$origem_del -e "$ssh" backup@$host:$origem $destino
```

Salve-o em uma pasta de sua preferencia, no nosso exemplo será /var/adm/backup.sh
Dê permissão de execução a ele:

```
DESTINO# chmod 755 /var/adm/backup.sh
```

O script faria a mesma coisa que digitar no prompt:

```
rsync -avHz --delete-during --backup --backup-dir=/backups/del/ -e "ssh -p 65222 -i /home/backup/.ssh/id_dsa"
backup@192.168.1.254:/home /backups
```

Que chamaria o rSync para que ele se conecta-se ao servidor ORIGEM por SSH usando a chave de criptografada com o usuário backup dizendo que irá fazer backup da pasta /home e tudo que foi deletado desde o ultimo backup também será deletado no DESTINO porém ficara uma cópia na pasta /backups/del/

6. Agendando no CronE para facilitar um pouquinho mais nossas noites de sono iremos usar o Crontab para agendar a execução do script todo dia a meia-noite:

```
DESTINO# crontab -e
```

Este comando abre o editor das tarefas que devem ser executadas
Insira a seguinte linha no arquivo:

```
00   00   * * *   /var/adm/backup.sh
```

Salve e saia.
Pronto temos um script que fará o backup para nós todo dia a meia-noite.

7. Considerações e Referências

Espero dar uma base para que alguem que busca como implementar um backup em seu sistema com este artigo, você pode adaptá-lo fácilmente ao seu ambiente, pode trocar o usuário, basta que este usuário tenha permissão sobre os arquivos que serão backupeados.

Tive como Referência:

rSync:
http://samba.anu.edu.au/rsync/documentation.html
man rsync

SSH:
man ssh
http://www.networknewz.com/networknewz-10-20030707AuthenticatingbyPublicKeyOpenSSH.html

Crontab:
http://focalinux.cipsga.org.br/guia/intermediario/ch-manut.htm#s-manut-cron-formato

Artigo retirado de:
http://thiagoruiz.blogspot.com/2006/09/brincando-de-backup-com-rsync.html

Até a próxima. []'z

Thiago J. Ruiz (Neo)

http://thiagoruiz.blogspot.com