Serveur de sauvegarde BACKUPPC de machines hétérogènes avec déduplication (serveur de saugegarde, partie2)

 On reprend par exemple serveurlvmraid, préparé volontairement avec LVM afin de faire face à un volume de sauvegardes qui grandit en permanence.

apt-get install backuppc rsync libfile-rsyncp-perl par2 rrdtool
openssh-client

- Ouvrir un navigateur à l'adresse <u>http://192.168.0.101/backuppc/</u> avec utilisateur : backuppc et le mot de passe donné pendant l'installation.
 - Pour le modifier si pas noté :

htpasswd /etc/backuppc/htpasswd backuppc

 $\circ\,$ Si ça ne marche pas :

#dpkg-reconfigure backuppc

Et choisir d'ajouter un alias backuppc à la configuration APACHE.

- Explorer l'interface web d'administration
- Ajouter la machine client (celle du cluster GFS) aux machines à sauvegarder :

nano /etc/backuppc/hosts

/etc/backuppc/hosts

... localhost 0 backuppc 192.168.0.3 0 root

• Configurer la méthode de sauvegarde :

nano /etc/backuppc/config.pl

```
$Conf{XferMethod} = 'rsync';
$Conf{RsyncClientPath} = '/usr/bin/rsync';
$Conf{RsyncClientCmd} = '$sshPath -q -x -l root $hostIP $rsyncPath $argList+';
$Conf{RsyncClientRestoreCmd} = '$sshPath -q -x -l root $hostIP $rsyncPath
$argList+';
$Conf{RsyncShareName} = '/mnt/glusterfs';
#$Conf{RsyncShareName} = ['/', '/var', '/data', '/boot'];
```

```
• On redémarre le service backuppc :
```

/etc/init.d/backuppc restart

 On installe le service rsync et le service openssh sur client :

apt-get install rsync openssh-server

• On crée une paire de clés publique/privée :

ssh-keygen -t rsa

• Idem sur serveurlvmraid :

```
# su - backuppc
# ssh-keygen -t rsa
```

• On copie la clé publique de serveurlvmraid vers client :

```
# cp ~/.ssh/id_rsa.pub ~/.ssh/BackupPC_id_rsa.pub
# scp ~/.ssh/BackupPC_id_rsa.pub
root@192.168.0.3:/root/.ssh/
```

 On autorise backuppc à s'authentifier automatiquement sur client soit avec ssh-copy-id soit avec :

```
# cat ~/.ssh/BackupPC_id_rsa.pub >> ~/.ssh/authorized_keys2
```

• Si authorize_keys2 n'existait pas :

~/.ssh/touch authorized_keys2

• On copie la clé publique de *client* vers *serveurlvmraid* :

```
# scp ~/.ssh/id_rsa.pub
root@192.168.0.101:/var/lib/backuppc/.ssh/client_id_rsa.pub
```

 On ajoute la clé publique client à backuppc (attention à toujours être en tant que backuppc) :

```
# cat ~/.ssh/client_id_rsa.pub >> ~/.ssh/known_hosts
```

```
# su
```

```
# rm -f /var/lib/backuppc/.ssh/client_id_rsa.pub
```

```
# su backuppc
# chmod -R go-rwx ~/.ssh
```

• Idem sur client :

chmod -R go-rwx ~/.ssh

• On teste l'authentification automatique en tant que backuppc

depuis serveurlvmraid :

ssh -l root 192.168.0.3 whoami

Doit retourner « root »

- Si problème avec les clé SSH : <u>http://wiki.networksecuritytoolkit.org/index.php/HowTo BackupPC SSH Key Authentication Setu</u> <u>p For rsync Transfer</u>
- Tester depuis l'interface web un backup et une restauration
- Configurer un partage sur le poste windows et créer un nouvel hôte à sauvegarder : dans le fichier /etc/backuppc/windows.pl

```
$Conf{SmbShareName} = 'nomdupartagesmb';
$Conf{SmbShareUserName} = 'utilisateur';
$Conf{SmbSharePasswd} = 'motdepasse';
$Conf{XferMethod} = 'smb';
Modifier pour votre partage
```

• Tester la sauvegarde