How do I setup SSH2

Key generation

As root on the client machine, use ssh-keygen2 to generate a public/private key pair:

```
ssh-keygen2 -t rsa
```

or, because this command is sometimes renamed to ssh-keygen:

```
ssh-keygen -t rsa
```

This will save the public key in ~/.ssh2/id_rsa_1024_a.pub and the private key in ~/.ssh2/id_rsa_1024_a. As a password, you would type nothing (just enter) if you wish BackupPC to start automatically; alternatively, you could set a password on the private key as stored in the file system, and use an agent as described below to store the private key without password only in memory.

Identification

Create the identification file ~/.ssh2/identification:

```
echo "IdKey id_rsa_1024_a" > ~/.ssh2/identification
```

BackupPC setup

Repeat the above steps for the BackupPC user (BACKUPPCUSER) on the server. Rename the key files to recognizable names, eg:

```
ssh-keygen2 -t rsa
mv ~/.ssh2/id_rsa_1024_a.pub ~/.ssh2/BackupPC_id_rsa_1024_a.pub
mv ~/.ssh2/id_rsa_1024_a     ~/.ssh2/BackupPC_id_rsa_1024_a
echo "IdKey BackupPC_id_rsa_1024_a" > ~/.ssh2/identification
```

Based on your ssh2 configuration, you might also need to turn off StrictHostKeyChecking and PasswordAuthentication:

```
touch ~/.ssh2/ssh2_config
echo "StrictHostKeyChecking ask" >> ~/.ssh2/ssh2_config
echo "PasswordAuthentication no" >> ~/.ssh2/ssh2_config
```

Key exchange

To allow BackupPC to ssh to the client as root, you need to place BackupPC's public key into root's authorized list on the client. Copy BackupPC's public key (BackupPC_id_rsa_1024_a.pub) to the ~/.ssh2 directory on the client. Add the following line to the ~/.ssh2/authorization file on the client (as root):

```
touch ~/.ssh2/authorization
echo "Key BackupPC_id_rsa_1024_a.pub" >> ~/.ssh2/authorization
```

Fix permissions

You will probably need to make sure that all the files in ~/.ssh2 have no group or other read/write permission:

```
chmod -R go-rwx ~/.ssh2
```

You should do the same thing for the BackupPC user on the server.

Testing

As the BackupPC user on the server, verify that the following command prints “root”:

```
ssh2 -l root clientHostName whoami
```

You might be prompted the first time to accept the client's host key and you might be prompted for root's password on the client. Make sure that this command runs cleanly with no prompts after the first time. You might need to check /etc/hosts.equiv on the client. Look at the man pages for more information. The -v option to ssh2 is a good way to get detailed information about what fails.