

We are going to do something similar to what was done in the slides, i.e.: take a backup of /etc and /usr/local/etc to ANOTHER machine in the class, effectively implementing a "remote backup".

- manipulating ssh
- also, understanding ssh keys (not mandatory)

- you need to have an account on the machine you will backup TO

1.

2.

```
# pw useradd backup -m -s /bin/sh
# passwd backup
```

Enter in a password that you will remember :-)

3.

You will copy your .ssh/id_rsa.pub key file to the ".ssh/authorized_keys" file of the account on the REMOTE machine, i.e.: if the machine you will be working with is "pc13", and YOUR machine is "pc116" then you will need:

- an account ("backup") on pc13
- a generated, passphrase-less key on YOUR machine (pc16) in .ssh/id_rsa.pub (remember, that file is in your HOME directory -- under .ssh/)
- a copy of this key on the account ("backup") on the REMOTE ("pc13") machine

```
$ cat ~/.ssh/*.pub | pcX.ghe0.dns.gh 'cat >> .ssh/authorized_keys'
```

4.

We do this as root.

```
# rsync -avzR /etc /usr/local/etc backup@<remotemachine>:
```

... where <remotemachine> is the name or IP address of the REMOTE machine you have created the account on.

5.

```
# ssh backup@<remotemachine>
```

...
% ls -l

6. :)

7.