Server administration

General helpbase for server administration stuff

- User commands
- SSH Configuration

User commands

Linux commands for handling users and roles:

- `adduser name` *//Adds a new user interactivly (creates a default shell and home directory)*
- `deluser name` //Removes a user
- `deluser --remove-home name` //Removes a user and also deletes their home directory
- `usermod -aG group name` *//Give a user a role, such as sudo*
- `passwd name` *//Set the password for a given user, or if no user is supplied for the current user*
- `groups` *//List out all groups on the system*
- `users` *//List out all users on the system*

SSH Configuration

The ssh configuration file is stored at: `/etc/ssh/sshd_config` also you want to create a file: `/etc/ssh/authorized_keys` to store the public keys that want to connect to the server

/etc/ssh/sshd_config

Add the following to the end of the sshd_config file to for the proper setup

```
Port [Portnumber]
PermitRootLogin no
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys /etc/ssh/authorized_keys
AllowTcpForwarding yes
AllowUsers [Names of the allowed users]
PasswordAuthentication no
LoginGraceTime 30
ClientAliveInterval 300
X11Forwarding no
```

Portnumber: Should be the portnumber you want to access your server on, it should not be 22 and should be above 1024

AllowUsers: Name of the users you want to allow login with

If you do not plan on acessing internal server ports over an ssh tunnel, such as cockpit you might want to remove the `AllowTcpForwarding` option

`sudo sshd -t` can be used to test out the configuration before reloading

`sudo systemctl reload sshd` actually reloads the service and the configuration