AWS

Connecting via ssh

On the EC2 instances page, select your instance and click the Connect button. Your ssh connection command will look similar to this, depending on where your Amazon private key file is kept.
ssh -i private_key.pem root@ec2-52-23-170-128.compute-1.amazonaws.com

Depending on your user access configuration, "centos" may be used as the username. For example, ssh centos@your.hostname.com

Sudo to root

To sudo to root, enter the following command when logged in a the "centos" user:

```
sudo su -
```

You will change to the root user and placed in the root user's home directory.

The hub configuration file

The hub configuration file is located in the hub document root. Located at "/var/www/hub"

Within that directory you will find a "configuration.php" file which contain many of the configuration options set by the CMS from the global configuration page in the administrator interface (/administrator) of the hub. You will also find the web username and password for the database there.

Connecting to the database as the web user with a database client

Connections to the database are restricted to localhost for security purposes.

In your database client you must select the SSH option and enter the appropriate credentials for the SSH tunnel and Database to connect.

The SSH credentials can be the "centos" user and the stored key on your workstation. Other Linux users with SSH access may be sued as well.

The database credentials to connect as the web user are found in the hub configuration.php file (var $password and var $db). You may also use another database account that has been previously granted database access.

Creating or granting additional permissions

New Linux users should be created at the system level.

New Database users and granting permission should be done by the root user. As root, you may enter MySQL by typing "mysql" at the command line, without a password.