

Docker Security

published by admin on Sat, 04/11/2015 - 20:32

The docker daemon always runs as root, and since docker version 0.5.2, docker binds to a Unix socket instead of a TCP port. By default that Unix socket is owned by the user *root*, and so, by default, you can access it with `sudo`.

Starting in version 0.5.3, if you (or your Docker installer) create a Unix group called *docker* and add users to it, then the docker daemon will make the ownership of the Unix socket read/writable by the *docker* group when the daemon starts. The docker daemon must always run as root, but if you run the docker client as a user in the *docker* group then you don't need to add `sudo` to all the client commands.

Example:

```
# Add the docker group if it doesn't already exist.
```

```
$ sudo groupadd docker
```

```
# Create the docker user if it doesn't already exist and add him to the docker group
```

```
$ sudo useradd -g docker docker
```

```
# Log in as the docker user $ sudo su - docker
```

```
# Restart the docker daemon. $ sudo service docker restart
```

```
# Now execute docker without being the super user $ docker images
```

*Mercilessly stolen and altered from the good people at Docker.io.

Source URL: <https://blackhillsystems.com/?q=node/48>