\* Docker and Splunk

- Entra no site do Docker Spluk (E segue os dois passos do tutorial)

\* Abrir a porta

- ufw status

-ufw enable

- ufw allow 8000/tcp

- ufw status

\* Splunk

- Setings ADD DATA

Pode ter arquivo txt ou csv

- Sourcetype Automatic

- Host = 1 (é o primeiro seguimento do path, é exatamente o nome da pasta)

- Index= Main é o diretório que estão guardados esses eventos (o sourcetype é o o tipo de dado)