Elasticsearch Docker

Heavily inspired by: https://github.com/deviantony/docker-elk/tree/x-pack

Getting Started

- You first need Docker to be able to set up your ES and Kibana instance locally
- Once you've done that you need to make sure you have elasticdump. It is a dependency of this repo so as long as you've run `npm install` you should have it
- Next you need to instantiate a local docker and kibana instance

```
# assuming you are at the root of this repository
cd /provision/docker
# spin up the docker and kibana instances
docker-compose up

# this will consume the entire terminal, run with a -d flag to run as a daemon
curl localhost:9200
# you should get back a response like this
{
  "name" : "C31lyFy",
  "cluster_name" : "seclock-dev",
  "cluster_uuid" : "4jZZf-OTT0a_AtmtdkzGRA",
  "version" : {
    "number" : "5.4.0",
    "build_hash" : "780f8c4",
    "build_date" : "2017-04-28T17:43:27.229Z",
    "build_snapshot" : false,
    "lucene_version" : "6.5.0"
  },
  "tagline" : "You Know, for Search"
}
```

- Next we need to get some data in elasticsearch
- First make sure your .env file has this specified

```
ES_HOST=localhost:9200
```

- Next create a tunnel to the staging environment

```
ssh -NfL 9201:internal-lb-es-stg-470443166.us-west-1.elb.amazonaws.com:80
dmzuser@52.8.83.132
```

- Now create an index on your local setup

```
# navigate to the root of the repo
```

```
sh bin/es.sh schema sec-1
# add this as an alias
sh bin/es.sh add sec-1

# now copy over data from staging into your local es instance
./node_modules/elasticdump/bin/elasticdump --input=http://127.0.0.1:9201/sec
--output=http://127.0.0.1:9200/sec --type=data
```

- That will consume a terminal window as well

Misc

- Docker data is persisted in the `/provision/docker/data` directory so when you spin up docker again the data will remain