RSyslog to Elasticsearch

Docker Container

I decided to use use a container from Allan Simon from the following git repo

https://github.com/allan-simon/docker-rsyslog-elasticsearch

Get the code

```
$ git clone https://github.com/allan-simon/docker-rsyslog-elasticsearch
```

Revise the base container to use ubuntu:20.04

Dockerfile

```
FROM      ubuntu:20.04
# Install rsyslog and rsyslog-elasticsearch extensions. All in one
# go to reduce amount of layers.
RUN       apt-get -y update && \
          apt-get upgrade -y --no-install-recommends && \
          apt-get install -y --no-install-recommends \
          software-properties-common && \
          apt-get -y update && \
          apt-get -q -y --no-install-recommends install \
          rsyslog rsyslog-elasticsearch cron logrotate && \
          apt-get clean && \
          rm -rf /var/lib/apt/lists/* && \
          chown syslog /var/log

COPY      entrypoint.sh                 /
COPY      rsyslog.conf                  /etc/
COPY      rsyslog_elasticsearch.conf    /etc/rsyslog.d/
COPY      rsyslog-rotate                /usr/lib/rsyslog/rsyslog-rotate

ENTRYPOINT ["/entrypoint.sh"]
CMD ["-n"]
```

Build

```
$ docker build -t jmehan/rsyslog .
```

Deploy

buildDocker.sh

```
CONTAINER=rsyslog
IMAGE=jmehan/rsyslog

DIR=`pwd -P`

docker stop $CONTAINER
docker rm $CONTAINER
DIR=`pwd -P`

docker run --name $CONTAINER \
--restart=always \
-p 514:514/udp \
-p 514:514 \
-e ESLOG_HOST=192.168.1.50 \
-e ESLOG_ES_PORT=9200 \
-e ESLOG_ES_USE_HTTPS=off \
-v /etc/timezone:/etc/timezone \
-d $IMAGE

docker logs -f $CONTAINER
```

Utilities

Send logs to RSyslog

```
$ logger -n localhost -P 514 "hellow world"
```

References

Reference	URL
Docker log driver syslog forward to Elasticsearch	https://github.com/allan-simon/docker-rsyslog-elasticsearch
omelasticsearch: Elasticsearch Output Module	https://www.rsyslog.com/doc/v8-stable/configuration/modules/omelasticsearch.html