Writeup:

|  |
| --- |
| # Dockerfile to illustrate how Filebeat can be used with nginx |
| # Build with: | # Filebeat 8.3.3 |
| # docker build -t filebeat-nginx-example . |  |
|  |  |
| # Run with: |  |
| # docker run -p 80:80 -it --link <elk-container-name>:elk \ |  |
| # --name filebeat-nginx-example filebeat-nginx-example |  |
|  |  |
| FROM nginx |  |
| MAINTAINER Sebastien Pujadas http://pujadas.net |  |
| ENV REFRESHED\_AT 2020-10-02 |  |
|  |  |
|  |  |
| ############################################################################### |  |
| # INSTALLATION |  |
| ############################################################################### |  |
|  |  |
| ### install Filebeat |  |
|  |  |
| ENV FILEBEAT\_VERSION 8.3.3 |  |
| ENV FILEBEAT\_BASE\_VERSION 8.3.3 |  |
|  |  |
|  |  |
| RUN apt-get update -qq \ |  |
| && apt-get install -qqy curl \ |  |
| && apt-get clean |  |
|  |  |
| RUN curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-${FILEBEAT\_VERSION}-amd64.deb \ |  |
| && dpkg -i filebeat-${FILEBEAT\_VERSION}-amd64.deb \ |  |
| && rm filebeat-${FILEBEAT\_VERSION}-amd64.deb |  |
|  |  |
|  |  |
| ############################################################################### |  |
| # CONFIGURATION |  |
| ############################################################################### |  |
|  |  |
| ### tweak nginx image set-up |  |
|  |  |
| # remove log symlinks |  |
| RUN rm /var/log/nginx/access.log /var/log/nginx/error.log |  |
|  |  |
|  |  |
| ### configure Filebeat |  |
|  |  |
| # config file |  |
| ADD filebeat.yml /etc/filebeat/filebeat.yml |  |
| RUN chmod 644 /etc/filebeat/filebeat.yml |  |
|  |  |
| # CA cert |  |
| RUN mkdir -p /etc/pki/tls/certs |  |
| ADD logstash-beats.crt /etc/pki/tls/certs/logstash-beats.crt |  |
|  |  |
| # create template based on filebeat version (assumption: it is the same version as elasticsearch version) |  |
| RUN filebeat export template --es.version ${FILEBEAT\_BASE\_VERSION} > /etc/filebeat/filebeat.template.json |  |
|  |  |
| ############################################################################### |  |
| # DATA |  |
| ############################################################################### |  |
|  |  |
| ### add dummy HTML file |  |
|  |  |
| COPY html /usr/share/nginx/html |  |
|  |  |
|  |  |
| ############################################################################### |  |
| # START |  |
| ############################################################################### |  |
|  |  |
| ADD ./start.sh /usr/local/bin/start.sh |  |
| RUN chmod +x /usr/local/bin/start.sh |  |
| CMD [ "/usr/local/bin/start.sh" ] |  |
|  |  |
|  |  |