Configuration of Certs

This page contains information about the default certs in Policy Agent and SDNC-A1 controller, as well as how to update/replace them using docker.

SDNC-A1 Controller

The SDNC-A1 controller uses the default keystore and truststore that are built into the container.

The paths and passwords for these stores are located in a properties file:
nonrtric/sdnc-a1-controller/oam/installation/src/main/properties/https-props.properties

The default truststore includes the a1simulator cert as a trusted cert which is located here:
https://gerrit.o-ran-sc.org/r/gitweb?p=sim/a1-interface.git;a=tree;f=near-rt-ric-simulator/certificate;h=172c1e5aacd52d760e4416288dc5648a5817ce65;hb=HEAD

The default keystore, truststore, and https-props.properties files can be overridden by mounting new files using the "volumes" field of docker-compose. Uncommment the following lines in docker-compose to do this, and provide paths to the new files:

```
#volumes:
#       - <path_to_keystore>:/etc/ssl/certs/java/keystore.jks:ro
#       - <path_to_truststore>:/etc/ssl/certs/java/truststore.jks:ro
#       - <path_to_https-props>:/opt/onap/sdnc/data/properties/https-props.properties:ro
```

The target paths in the container should not be modified.

For example, assuming that the keystore, truststore, and https-props.properties files are located in the same directory as docker-compose:

```
volumes:
      - ./new_keystore.jks:/etc/ssl/certs/java/keystore.jks:ro

      - ./new_truststore.jks:/etc/ssl/certs/java/truststore.jks:ro

      - ./new_https-props.properties:/opt/onap/sdnc/data/properties/https-props.properties:ro
```

Policy Agent

The Policy Agent uses the default keystore and truststore that are built into the container. The paths and passwords for these stores are located in a yaml file:
nonrtric/policy-agent/config/application.yaml

The default truststore includes a1simulator cert as a trusted cert which is located here:
https://gerrit.o-ran-sc.org/r/gitweb?p=sim/a1-interface.git;a=tree;f=near-rt-ric-simulator/certificate;h=172c1e5aacd52d760e4416288dc5648a5817ce65;hb=HEAD

The default truststore also includes a1controller cert as a trusted cert which is located here (keystore.jks file):
https://gerrit.o-ran-sc.org/r/gitweb?p=nonrtric.git;a=tree;f=sdnc-a1-controller/oam/installation/sdnc-a1/src/main/resources;h=17fdf6cecc7a866c5ce10a35672b742a9f0c4acf;hb=HEAD

There is also Policy Agent's own cert in the default truststore for mocking purposes and unit-testing (ApplicationTest.java).

The default keystore, truststore, and application.yaml files can be overridden by mounting new files using the "volumes" field of docker-compose or docker run command.

Assuming that the keystore, truststore, and application.yaml files are located in the same directory as docker-compose, the volumes field should have these entries:

```
volumes:
      - ./new_keystore.jks:/opt/app/policy-agent/etc/cert/keystore.jks:ro

      - ./new_truststore.jks:/opt/app/policy-agent/etc/cert/truststore.jks:ro

      - ./new_application.yaml:/opt/app/policy-agent/config/application.yaml:ro
```

The target paths in the container should not be modified.

Example docker run command for mounting new files (assuming they are located in the current directory):

```
docker run -p 8081:8081 -p 8433:8433 --name=policy-agent-container --network=nonrtric-docker-net --volume "$PWD/new_keystore.jks:/opt/app/policy-agent/etc/cert/keystore.jks" --volume "$PWD/new_truststore.jks:/opt/app/policy-agent/etc/cert/truststore.jks" --volume "$PWD/new_application.yaml:/opt/app/policy-agent/config/application.yaml" o-ran-sc/nonrtric-policy-agent:2.0.0-SNAPSHOT
```