Improving usage of containers technology

SECCOM

Intro

- ONAP is shipped as a set of Docker images deployed by OOM
- Images, as release artifacts, are cryptographically signed
- Issue: some of the images download additional files (Python libraries, npm packages, jars, etc.) from the Internet after they are deployed

The problem

- Container start and restart takes more time
- Time required to start the container depends on the Internet speed
- Start time of two instances of the same containers may differ due to downloaded files
- Some files are downloaded using insecure communication
- Set of downloaded files depends on actions executed (contextual download)
- Almost impossible to declare what is deployed as ONAP or to certify what is in the deployment
- Almost impossible to deploy ONAP behind restrictive firewall

Ongoing effort

- OOM is developing an Offline installer for ONAP
- Current State: OOM team collects online runtime dependencies and sets up local hosts that will provide required files to the pods
- Problem: list of dependencies is not constant and differs from release to release
- Current list of online dependencies can be found in offline installer repo
- Current solution is a work around

SECCOM recommendation

- Proposed addition to El Alto scope:
  - Remove runtime online dependencies from containers
- Add a non functional requirement:
  - ONAP Docker images shall be self-contained and not download additional files after deployment*
- Add integration test which checks if any file has been downloaded after ONAP is deployed

* time is counted from running *helm deploy*. Downloading RKE or any other packages required to setup the cluster is out of scope

SECCOM recommendation

- Add a non functional requirement:
  - All ONAP containers shall be read-only except for well-defined writable elements like log files
- Add a non functional requirement:
  - All ONAP applications shall run as a separate user with minimal privileges required to execute correctly.

Thank you

- That’s all