Agenda für eine Ausbildung zum Thema Docker, Docker Security

Rainer Sawitzki, 2.7.2019

Termin: 22.-24.7.2019

Ort: beim Kunden ING-DIBA Nürnberg

Zielgruppe: Entwickler, Buildmanager

Vorkenntnisse: Grundlagen der Programmierung, Buildmanagement

Methode: Vortrag (V), Präsentation (P), Diskussion, Übungen (Ü).

Ausgangssituation:

Eine Java-Anwendung wird über einen Maven-basierten Buildprozess als Artefakt in einem Nexus-Server abgelegt. Das Artefakt der Anwendung soll über eine anschließende Build-Pipeline in ein signiertes Docker-Image verpackt werden, das von einem OpenShift-System betrieben wird.

Zielsetzung:

- Vertiefte Kenntnisse in Docker, insbesondere Docker Security
- Docker-Build und CI/CD
- Deployment und Betrieb in OpenShift

Dauer:

- 12 Unterrichtseinheiten mit jeweils etwa 90 Minuten Dauer
- Netto-Seminarzeit pro Tag 6 Stunden
- Beginn am Montag, 22.7.2019 um 9:00, Seminarende am Mittwoch dann zwischen 15:00 und 16:00
- Kaffeepausen und Mittagspause werden vom Kunden organisiert, Gesamtpausenzeit pro Tag etwa 1:15

Lose Themenliste der ING-DIBA, Stand 2.7.2019

- Docker Basics
    - run/build/inspect/tag usw.
    - Layers, images
    - Fehler Analyse
    - Best Practises für DockerFiles
    - Versionierung
    - Docker Registries
- Docker Security
    - Hardening Docker Hosts:
        - Wie setzt man docker build Maschinen sicher auf und sichert sie ab?
    - Best-Practices Image Security:
        - Static Analysis, Blackbox/Whitebox-Testing, Integration in CI/CD
    - Attack-Vectors
        - Gemeinsames Verständnis über gängige und relevante Angriffsvektoren und wie man diese absichert.
- Modular Docker Build
    - Wie kann man Container-Workflows für Entwickler ohne lokalen Docker-Daemon etablieren?
    - Wie etabliere ich Best-Practices (z.B. no root, single process in container) und forciere sie im Enterprise-Umfeld?
- Docker Image Staging & Promotion:
    - Wie komme ich vom Applikations-Source Code zum produktiven Image?
    - App-Release vs. Container Release: Wie geht man mit Änderungen im Base-Image um?
    - Best Practice zum Zusammenspiel docker, docker registry (z.B. artifactory) und container orchestrator (z.B. openshift)
- Docker Image Release Prozess
    - Stage (dev, test, acc, PX usw.) + secret management in zusammehang mit Openshift (namespaces)
    - Deployment Strategien – Openshift ?
    - Deployment Templating – service, deployment, route yamls (Ist Helm die beste Lösung ? gibt es Alternativen ?)

Inhalte

Im Rahmen der Schulung wird die obige Themenliste in einem didaktischen Rahmen abgearbeitet:

1. Einführung in Docker: Architektur, Werkzeuge (V, P)
2. Erstes Arbeiten mit Docker (V, P, Ü)
3. Images und Container im Detail (V, P)
4. Fehleranalyse, Logfiles, Shell/Bash (V, P, Ü)
5. Der Docker Buildprozess und das Dockerfile (V, P, Ü)
6. Aufsetzen einer Docker-basierten Build-Umgebung mit Build-Machine und Docker Repository (V, P)
7. Best Practices und Richtlinien für Dockerfiles, z.B. Umgang mit Versionen, “no root”, single process (V, P)
8. Integration von Test, QS und Security in die CI-Pipeline (V, P, Ü)
9. Container-Orchestrierung - Eine Übersicht am Beispiel Kubernetes und OpenShift (V, P)
10. Integration der Orchestrierung in den CI/CD-Prozess (V, P)
11. Deployment, Staging und Promotion am Beispiel OpenShift (V, P)
12. Q&A