Dockercon16 Overview

Omid Nejati | DevOps Engineer

DockerCon 2016

Seattle

- 1 day workshops
- 2 days show
- 4000 attendees
  - DockerCon 2014 had 500
- 800 Sessions submitted
- 2900 contributors
- 460K Dockerized apps
  - 3000% growth in 2 years

Workshops

- Docker for beginners
- Docker for Java Developers
- Docker Orchestration
  - Slides
  - Orchestration Workshop
- Docker Security workshop
- https://github.com/riyazdf/dockercon-workshop

What is New on Docker

Docker for mac and windows (Beta Version)

- www.docker.com/getdocker

Docker 1.12 with orchestration built-in

- Swarm mode
- Cryptographic node identity
- Docker service API
- Routing mesh

What is New on Docker

Docker for AWS and Azure (Beta Version)

- www.beta.docker.com

Distributed Application Bundle (DBA)

- www.docker.com/dab

Docker Store

- The Store offers better discovery, security, trust and reputation indicators
- www.store.docker.com

Trends

- Cloud: 80% say Docker central to cloud strategy
- App Modernization: 3 out of 4 top initiatives resolve around application
- DevOps: 44% looking to adopt DevOps
- 60% of Docker users are running in production

Challenges on Docker

- **Docker Security**
- **Docker Storage**
- **Docker monitoring**

Docker Security

- **Image Security**

  - **Docker Security Scanning**

Docker Cloud and Docker Hub can scan images in private repositories to verify that they are free from known security vulnerabilities or exposures, and report the results of the scan for each image tag.

  - **Aqua Peekr**

Free SaaS Scanner for Container Images. Peekr scans public or private registry images for known vulnerabilities and malicious code.

- **Infrastructure Security**

  - The Docker Bench for Security is a script that checks for dozens of common best practices around deploying Docker containers in production.
  - https://github.com/docker/docker-bench-security

Docker Security

```
# ------------------------------------------------------------------------------
# Docker Bench for Security v1.0.0
#
# Docker, Inc. (c) 2015-
#
# Checks for dozens of common best-practices around deploying Docker containers in production.
# Inspired by the CIS Docker 1.11 Benchmark:
# https://benchmarks.cisecurity.org/downloads/show-single/index.cfm?file=docker16.110
# ------------------------------------------------------------------------------

Initializing Sat Apr 30 23:04:50 CEST 2016


[INFO] 1 - Host Configuration
[WARN] 1.1  - Create a separate partition for containers
[PASS] 1.2  - Use an updated Linux Kernel
[PASS] 1.4  - Remove all non-essential services from the host - Network
[PASS] 1.5  - Keep Docker up to date
[INFO]       * Using 1.12.0 which is current as of 2016-04-27
[INFO]       * Check with your operating system vendor for support and security maintenance for docker
[INFO] 1.6  - Only allow trusted users to control Docker daemon
[INFO]      * docker:x:999:tsj
[PASS] 1.7  - Audit docker daemon - /usr/bin/docker
[PASS] 1.8  - Audit Docker files and directories - /var/lib/docker
[PASS] 1.9  - Audit Docker files and directories - /etc/docker
[PASS] 1.10 - Audit Docker files and directories - docker.service
[PASS] 1.11 - Audit Docker files and directories - docker.socket
[PASS] 1.12 - Audit Docker files and directories - /etc/default/docker
[INFO] 1.13 - Audit Docker files and directories - /etc/docker/daemon.json
[INFO]      * File not found
[PASS] 1.14 - Audit Docker files and directories - /usr/bin/docker-containerd
[PASS] 1.15 - Audit Docker files and directories - /usr/bin/docker-runc


[INFO] 2 - Docker Daemon Configuration
[PASS] 2.1  - Restrict network traffic between containers
[PASS] 2.2  - Set the logging level
[PASS] 2.3  - Allow Docker to make changes to iptables
[PASS] 2.4  - Do not use insecure registries
[PASS] 2.5  - Do not use the aufs storage driver
[INFO] 2.6  - Configure TLS authentication for Docker daemon
[INFO]      * Docker daemon not listening on TCP
[INFO] 2.7 - Set default ulimit as appropriate
[INFO]      * Default ulimit doesn't appear to be set
[WARN] 2.8  - Enable user namespace support
[PASS] 2.9  - Confirm default cgroup usage
[PASS] 2.10 - Do not change base device size until needed
[WARN] 2.11 - Use authorization plugin
[WARN] 2.12 - Configure centralized and remote logging
[PASS] 2.13 - Disable operations on legacy registry (v1)
```

Docker Storage

- Storing data within the container

```
docker run --name my-special-container busybox
#then write to a directory you want to use inside the container
```

- Store your data outside Docker's Union Filesystem

```
docker run --name my-special-container -v /container/dir busybox
```

- Mounting a volume within the Docker host's filesystem

```
docker run --name my-special-container -v /host/dir:/container/dir busybox
```

- Storing data on a network-attached block device using the Volume plug-in for Docker via -volume-driver flag

Docker monitoring

https://prometheus.io/

http://www.sysdig.org/

http://www.zabbix.com/

Thanks