Docker Security

Baohua Yang

2016-01-04

Outline

- Performance
- Isolation
- Resource Limit
- Docker Daemon
- Docker Bench

Performance

- CPU
  - Container achieves near-native, 22% better than vm
- Memory
  - Container achieves near-native, slightly better than vm
- Disk IO
  - Container achieves near-native, ~100% better than vm
  - Volume works better than UFS
- Network IO
  - Latency increase ~100% with NAT
  - Throughput: both container and vm achieve near-native

- Container achieves near-native performance of cpu, memory, disk and network.

Isolation

- Memory, fork, CPU, disk, network
  - VM achieve 100% isolation
  - Container only be affected in network traffic
    - Context switching
    - Cache missing
    - Software bridge

- Seems only network side has not enough protection

Resource Limit

- Now has limit on
  - CPU
  - Memory
  - Disk
  - Network (extended with TC support)

Docker Daemon

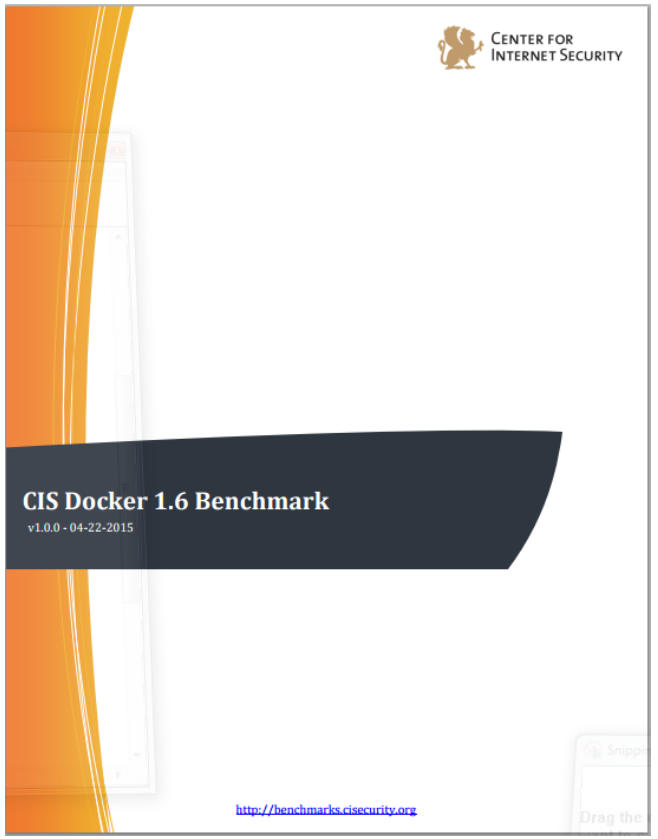
- HTTPS communication
- Container stops when daemon dies

Docker Bench

- dockerbench.com

```
➜ docker-security-benchmark git:(master) docker run -it --net host --pid host -v /var/run/docker.sock:/var/run/docker.sock \
> -v /usr/lib/systemd:/usr/lib/systemd -v /etc:/etc --label security-benchmark \
> diogomonica/docker-security-benchmark
# ------------------------------------------------------------------------
# CIS Docker 1.6 Benchmark v1.0.0 checker
#
# Docker, Inc. (c) 2015
#
# Provides automated tests for the CIS Docker 1.6 Benchmark:
# https://benchmarks.cisecurity.org/tools2/docker/CIS_Docker_1.6_Benchmark_v1.0.0.pdf
# ------------------------------------------------------------------------
Initializing Thu May 14 10:37:29 PDT 2015


[INFO] 1 - Host Configuration
[WARN] 1.1  - Create a separate partition for containers
[PASS] 1.2  - Use an updated Linux Kernel
[WARN] 1.5  - Remove all non-essential services from the host - Network
[WARN]      * Host listening on: 6 ports
[PASS] 1.6  - Keep Docker up to date
[INFO] 1.7  - Only allow trusted users to control Docker daemon
[INFO]      * docker:x:999:
```



Q&A