Analysis of Docker Securiy

Thanh Bui et al., Aalto University School of Science, 2015. 01

전상기(sanggi@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

Docker

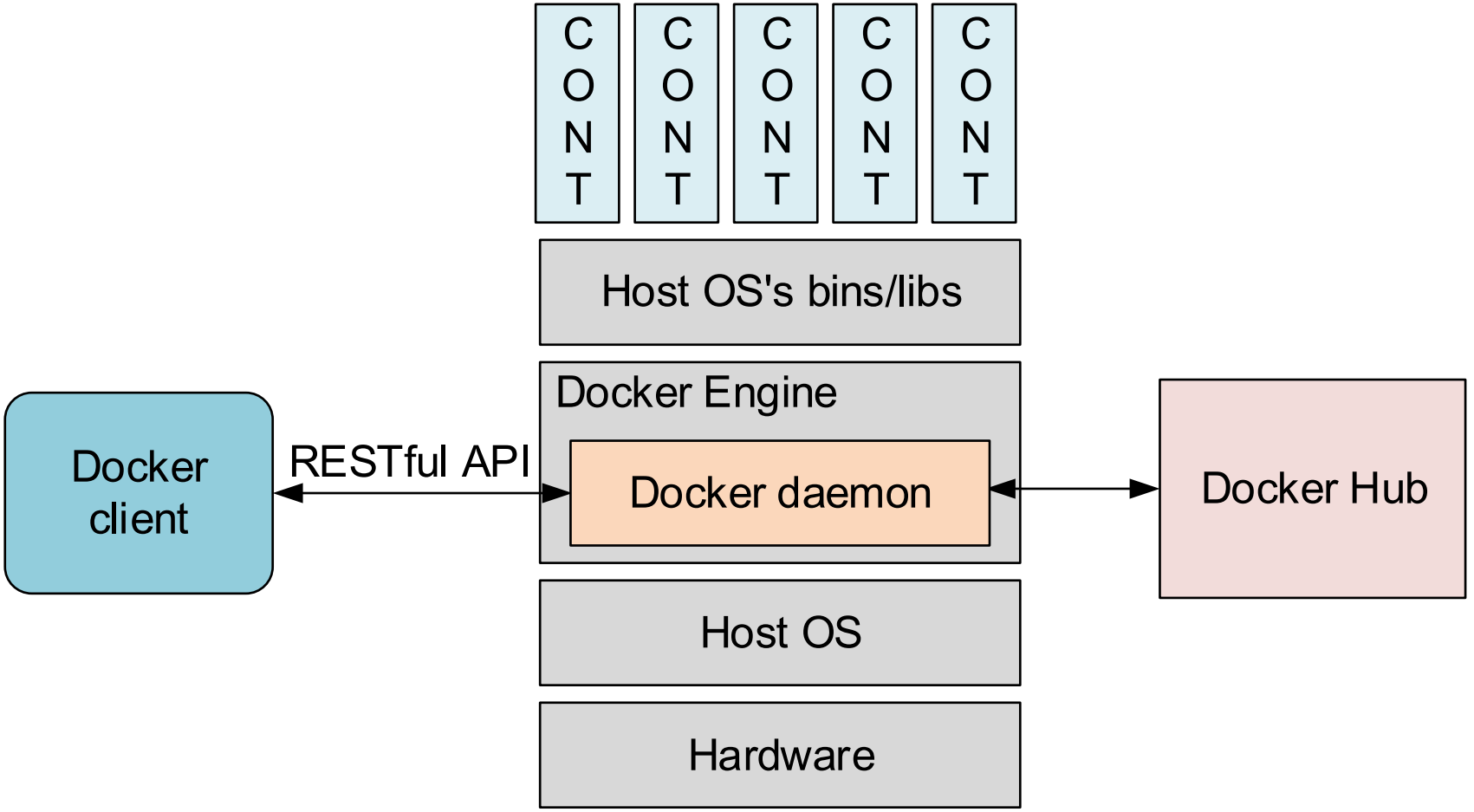
- 개요
  - Container-based virtualization
    - Container를 간단하고 안전하게 작성하고 제어하기 위한 인터페이스를 제공
    - 컨테이너 관리 및 배포 프로세스를 단순화하는 Third-party tools과 협력이 가능
    - 오픈 소스 컨테이너 기술
  - 분산 응용 프로그램을 작성, 전달 및 실행하는 기능을 함
  - 동일한 하드웨어에서 다른 기술보다 많은 가상 환경을 배포할 수 있음

Docker

- 개요
  - DevOps tool을 Docker와 통합하여 Docker container를 클라우드에 쉽게 배포 가능
    - DevOps tool은 오픈 소스 소프트웨어 구성 관리 도구임
  - Orchestration tools이 Docker container를 지원
    - Orchestration tools는 Docker에 대한 리소스 관리 및 스케줄링의 추상 계층을 제공함

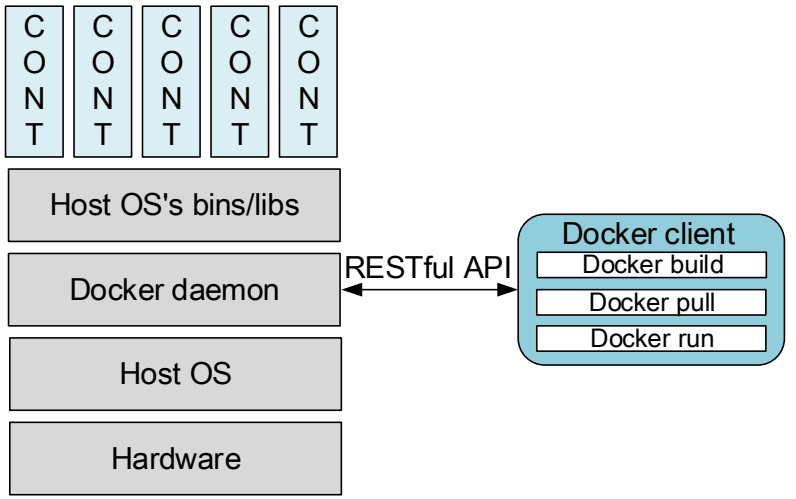
Docker

- Overview



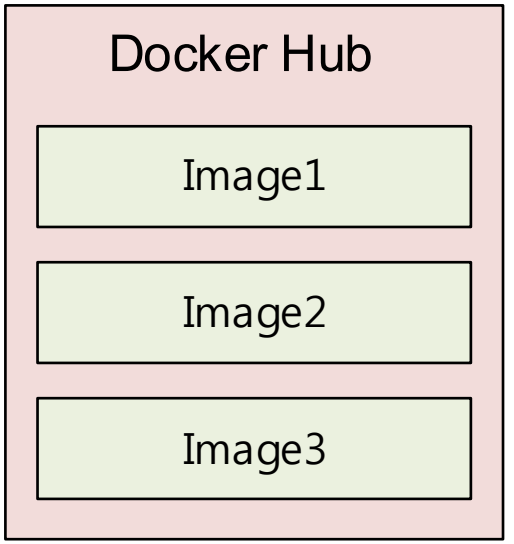
Docker

- 구성 요소
  - Docker Engine
    - Docker Engine은 경량 및 휴대용 장비 도구임
    - Container-based virtualization architecture와 유사함
  - Docker daemon
    - Docker container를 실행하고 관리함
  - Docker client
    - Docker와 사용자 간 인터페이스 제공
    - 사용자로부터 명령을 받아들인 다음 RESTful API를 통해 데몬으로 보냄



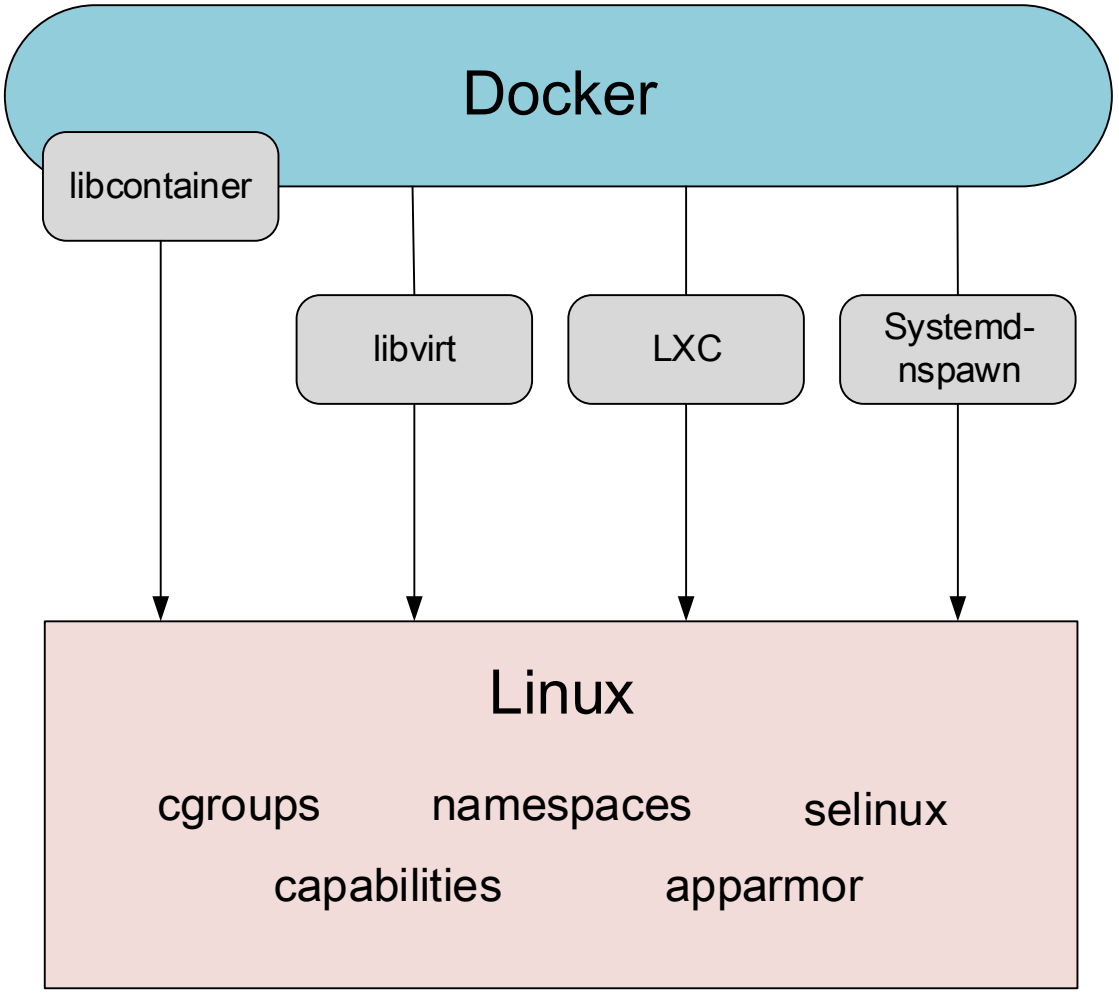
Docker

- 구성 요소
  - Docker Hub
    - 이미지를 공유 할 수 있는 중앙 저장소
      - 이미지: Container를 만들기 위한 자원
        - e.g., 실행 파일, 라이브러리, 소스코드 등이 패키지화 된 것
    - 사용자는 게시 된 이미지를 검색하여 Docker client로 다운로드 할수 있음
    - GitHub 같은 기능을 제공
    - Docker가 이미지를 서명하고 확인 후 Hub에 제출 했을 때 사용자는 이미지의 진위성과 무결성을 확인할 수 있음



Docker

- Docker system



Docker

- Docker system
  - Docker 0.9 버전 부터 LXC를 libcontainer로 대체함
    - LXC
      - Linux 커널의 cgroup과 namespaces를 이용하여 컨테이너를 관리하는 모듈
    - libcontainer
      - Docker에서 개발한 container driver
      - Docker가 LXC를 거치지 않고 커널의 container API를 직접 호출하여 효율성 향상

Docker

- Docker system
  - Docker는 Linux Capabilities, namespaces 및 cgroup을 활용
  - Cgroup
    - 계정에 대한 메커니즘을 제공
    - 각 컨테이너의 프로세스가 액세스 할 수 있는 리소스를 제한
  - Namespaces
    - 운영체제 리소스를 다른 인스턴스로 래핑함
    - 다섯가지 namespaces
      - Mount
        - Mount를 통해 filesystem을 사용자가 사용할 수 있게함
      - Hostname
      - Network

Docker

- Docker system
  - Namespaces
    - 다섯가지 namespaces
      - IPC(Inter-Process Communication)
        - 프로세스들 사이에 서로 데이터를 주고받는 방법이나 경로
      - PID(Process Identifiers)
        - 운영 체제 커널이 사용되는 번호
        - PID를 통해 프로세스를 일시적으로 식별 할 수 있음

감사합니다!