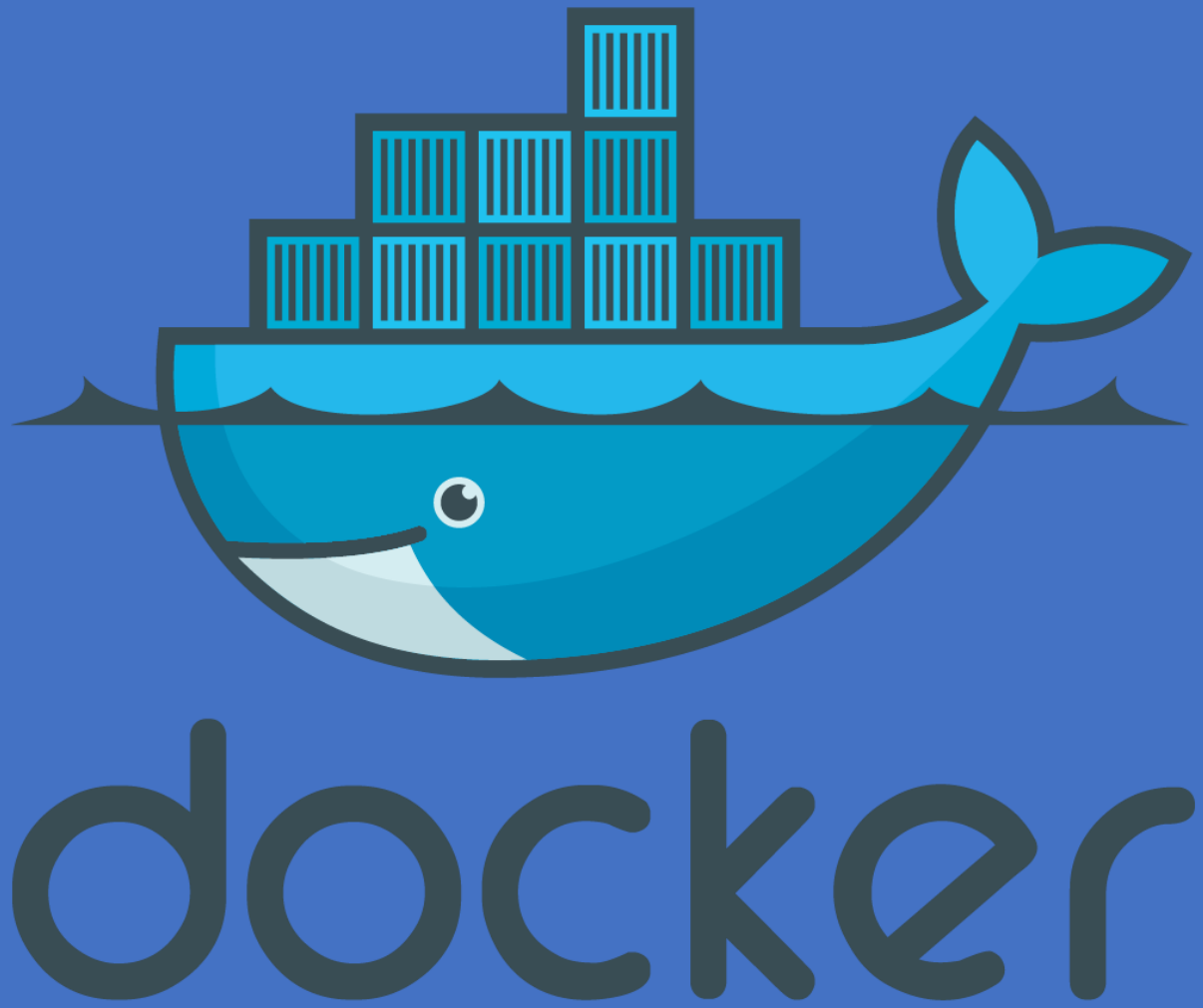
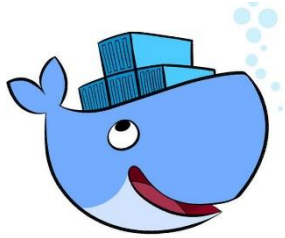


18-4Q
Crypto Lab
도커 컨테이너

1492073
임지훈



About Docker

Docker Compose

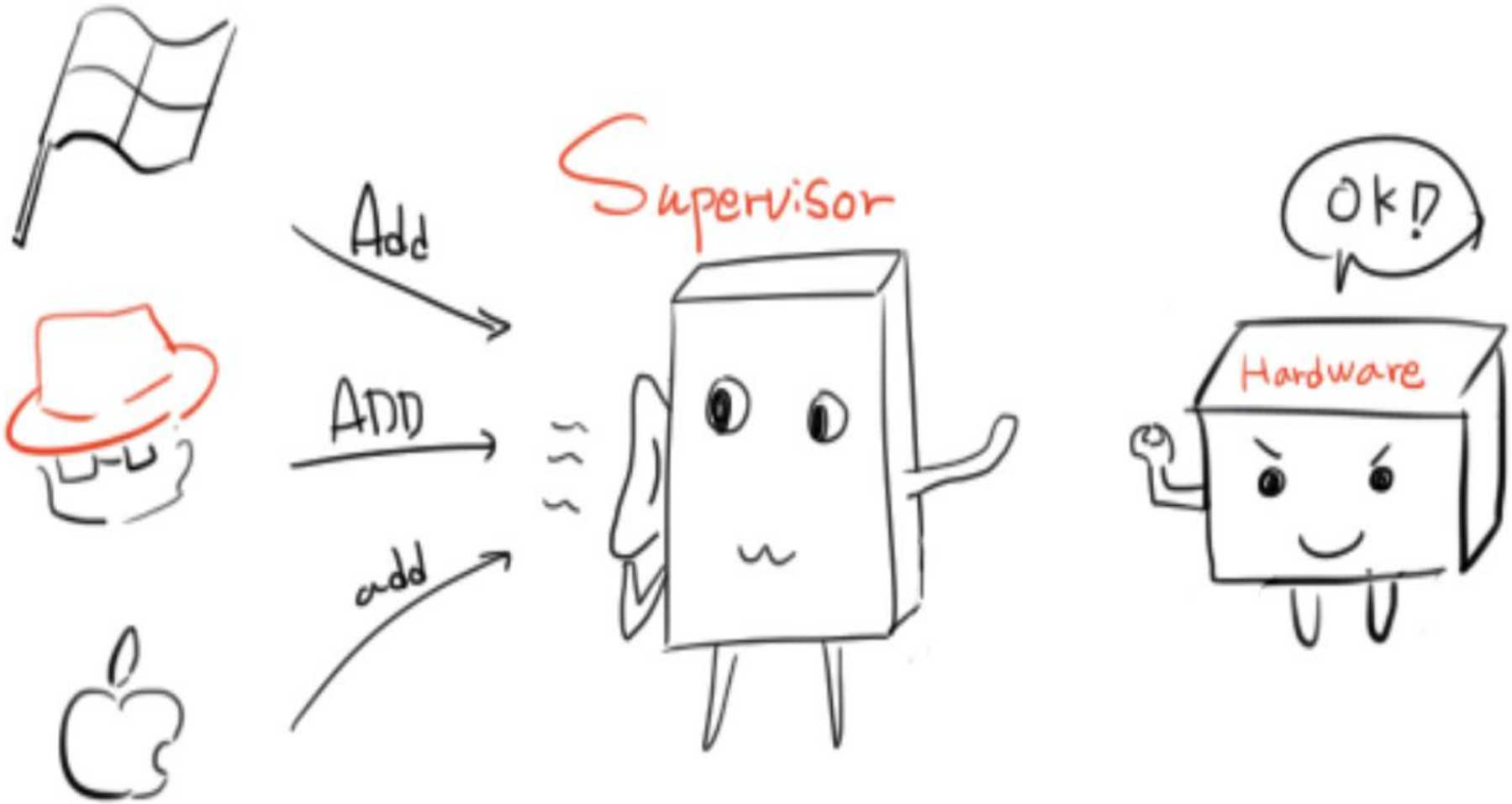
docker REGISTRY

docker MACHINE

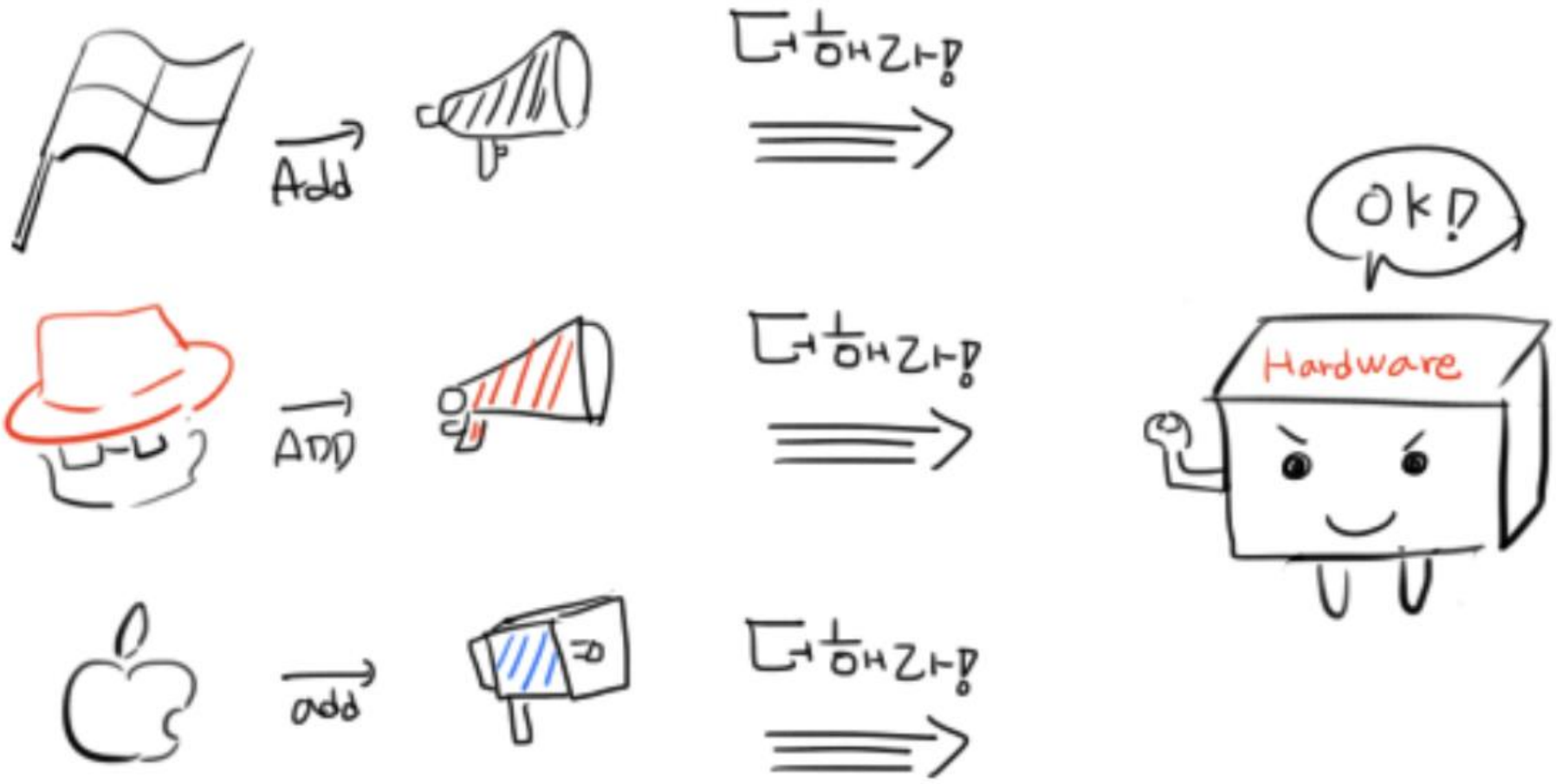
docker

Introduction

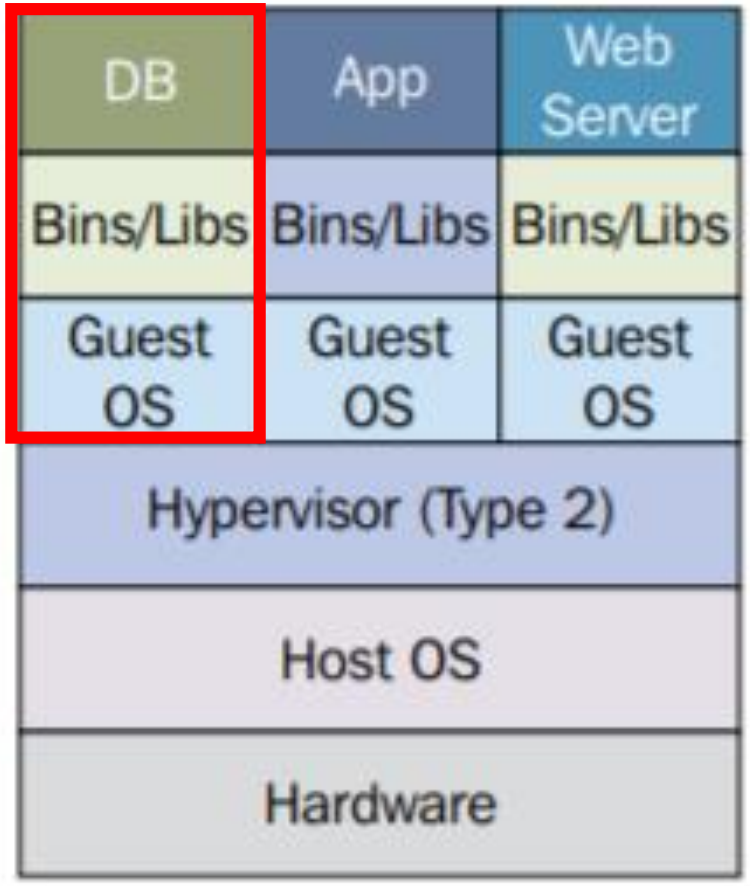
FULL VIRTUALIZATION



PARAVIRTUALIZATION



Virtual machine & Docker Container



하이퍼바이저

각종 시스템 자원을 가상화 독립된 공간을 생성

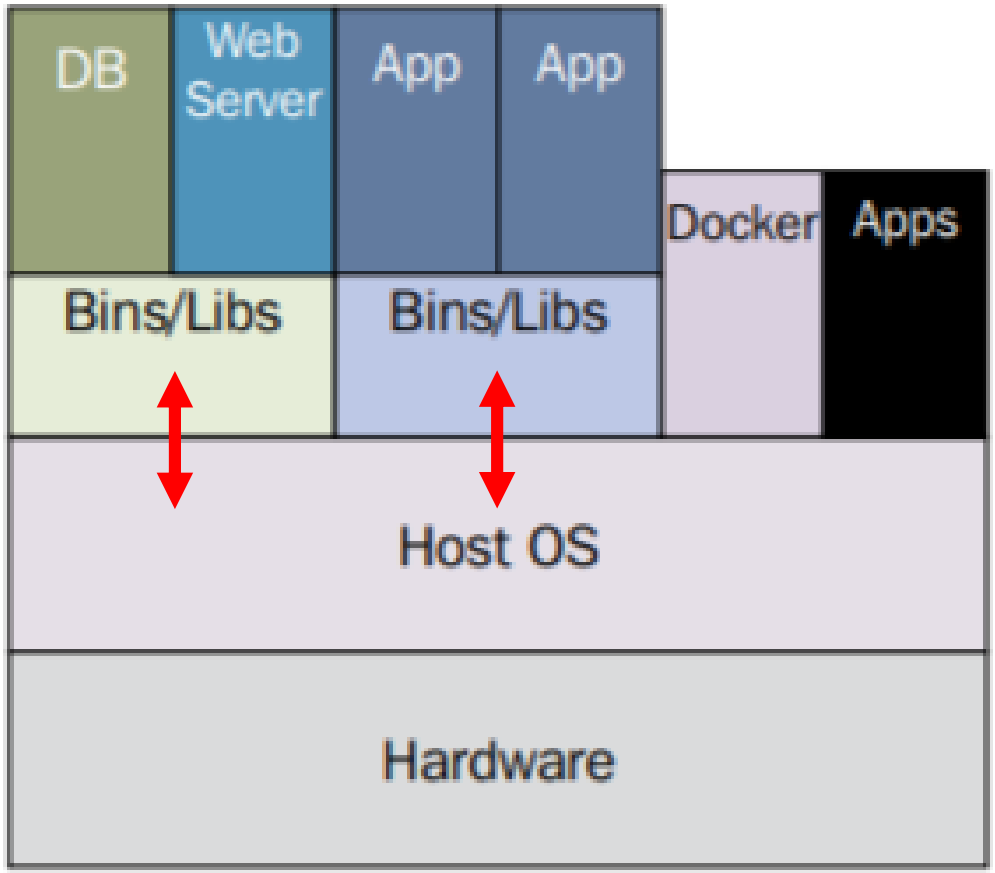
라이브러리, 커널등 을 전부 포함

장점 : 완벽한 운영체제 생성

단점 : 일반 호스트에 비해 성능의 손실 발생

배포하기 위한 이미지의 크기가 커짐

Virtual machine & Docker Container



가상화된 공간 생성 방법

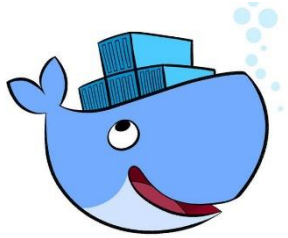
chroot, namespace, cgroup 사용

필요한 커널은 Host OS와 공유

애플리케이션을 구동하는 데 필요한 Lib 및 실행 파일만 존재

장점 : 이미지의 용량이 작음, 배포시간이 빠름

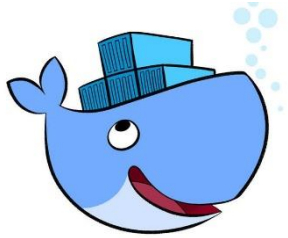
성능 손실도 거의 없음



Security

Application	Image Name	Stars
PEScanner	remnux/pescanner	******* (7)
JSDetox	renmux/jsdetox	***** (5)
YARA	blacktop/yara	***** (5)
Volatility	remnux/volatility	*** (3)
SIFT	k0st/sift	*** (3)
SpiderMonkey	nacyot/javascript-spidermonkey	** (2)
Dradis	raesene/auto_docker_dradis	** (2)
VirusTotal	malice/virustotal	* (1)
Malcom	tomchop/malcom-automatic	* (1)
ClamAV	malice/clamav	* (1)
FIR	(no public build)	

Available Container Security Features, Requirements and Defaults			
Security Feature	**LXC 2.0**	**Docker 1.11**	**CoreOS Rkt 1.3**
User Namespaces	Default	Optional	Experimental
Root Capability Dropping	Weak Defaults	Strong Defaults	Weak Defaults
Procfs and Sysfs Limits	Default	Default	Weak Defaults
Cgroup Defaults	Default	Default	Weak Defaults
Seccomp Filtering	Weak Defaults	Strong Defaults	Optional
Custom Seccomp Filters	Optional	Optional	Optional
Bridge Networking	Default	Default	Default
Hypervisor Isolation	Coming Soon	Coming Soon	Optional
MAC: AppArmor	Strong Defaults	Strong Defaults	Not Possible
MAC: SELinux	Optional	Optional	Optional
No New Privileges	Not Possible	Optional	Not Possible
Container Image Signing	Default	Strong Defaults	Default
Root Interation Optional	True	False	Mostly False



Security

Gartner analyst Joerg Fritsch

"How to Secure Docker Containers in Operation"

컨테이너에 배포된 응용프로그램은 bareOS에 배포된 것보다 안전하다.

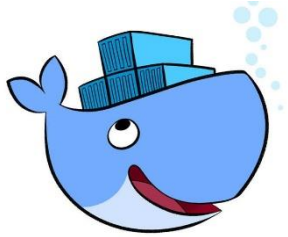
프로그램과 사용자가 컨테이너별로 분리되어 있기 때문에, 다른 컨테이너나 hostOS를 손상시킬 수 없다.

-> 또 하나의 Defense Layer를 쌓는 효과

Aaron Grattafiori, NCC Group

"Understanding and Hardening Linux Containers."

보안 측면에서, 공격 대상을 줄이고 필요한 구성 요소, 인터페이스, 라이브러리 및 네트워크 연결로만 응용프로그램을 격리하는 방법을 만듬. 요즘시기에, 리눅스 컨테이너와 같은 응용 프로그램을 사용하지 않을 이유가 거의 없다.



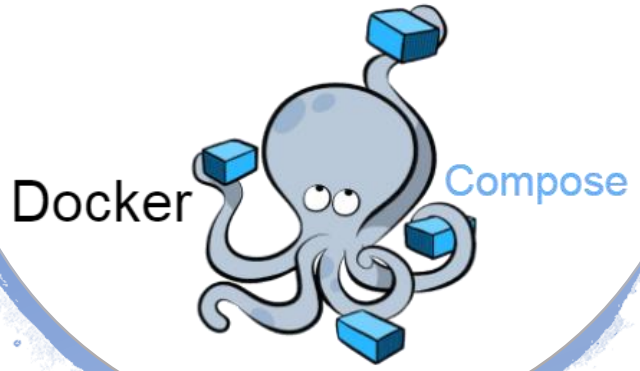
Reference

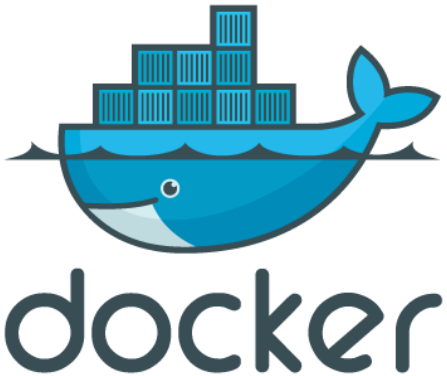
시작하세요 도커 저자 테크블로그

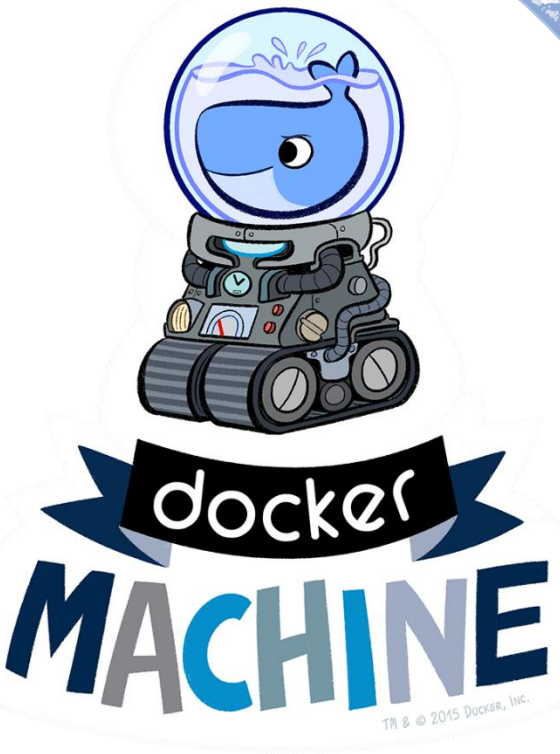
전가상화 반가상화

Incident Handling with Docker Containers

Your Software Is Safer In Docker Containers







Thank You