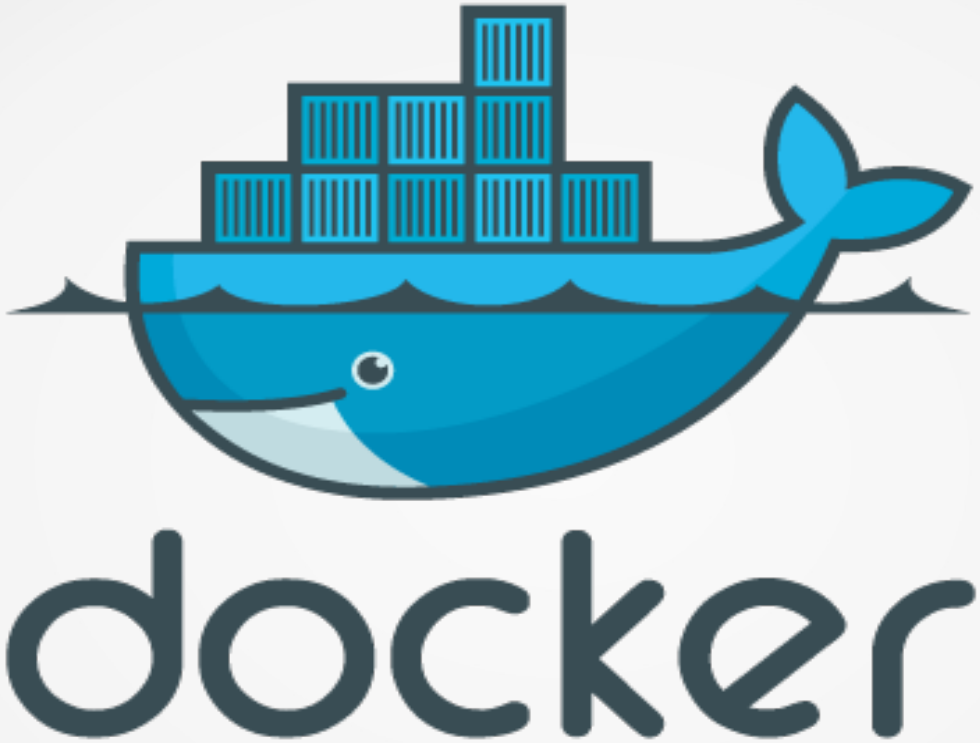
Docker and Linux Containers!



Mohamed Al-Maraghy

Red Hat Certified Architect level IV
Fedora Ambassador
m.maraghy@mazadah.com

Disclaimer

- This file is a simple introduction to the Linux docker and containers technology, it is intended to be used as a demo learning material and is not suitable for any other use.
- The information presented in this file is collected from various sources.
- The audience of this file are free to use this document as they see fit,I claim no copyrights over its content

  - Mohamed Al-Maraghy

Index

- What are containers in general?
- What are Linux Containers LXC?
- What's the fuss?
- Hypervisor vs. Linux Contaniers
- What is Docker?
- Demo!
- Is it safe to use Containers?

Containers in general!

What Are Linux Containers?

- Linux Containers (LXC) allow running multiple isolated Linux instances (containers) on the same host.

- Containers share the same kernel with anything else that is running on it, but can be constrained to only use a defined amount of resources such as CPU, memory or I/O.

- A container is a way to isolate a group of processes from the others on a running Linux system.

Cont. What Are Linux Containers?

Technically (1/2): ~ chroot on steroids

• a container is a set of processes
(running on top of common kernel)

• isolated* from the rest of the machine
(cannot see/affect/harm host or other containers)

• using namespaces to have private view of the system
(network interfaces, PID tree, mountpoints...)

• and cgroups to have metered/limited/reserved resources (to mitigate “bad neighbor” effect)

Cont. What Are Linux Containers?

From a distance (2/2): looks like a VM

- I can SSH into my container
- I can have root access in it
- I can install packages in it
- I have my own eth0 interface
- I can tweak routing table, iptables rules
- I can mount filesystems
- etc.

What's the Fuss?

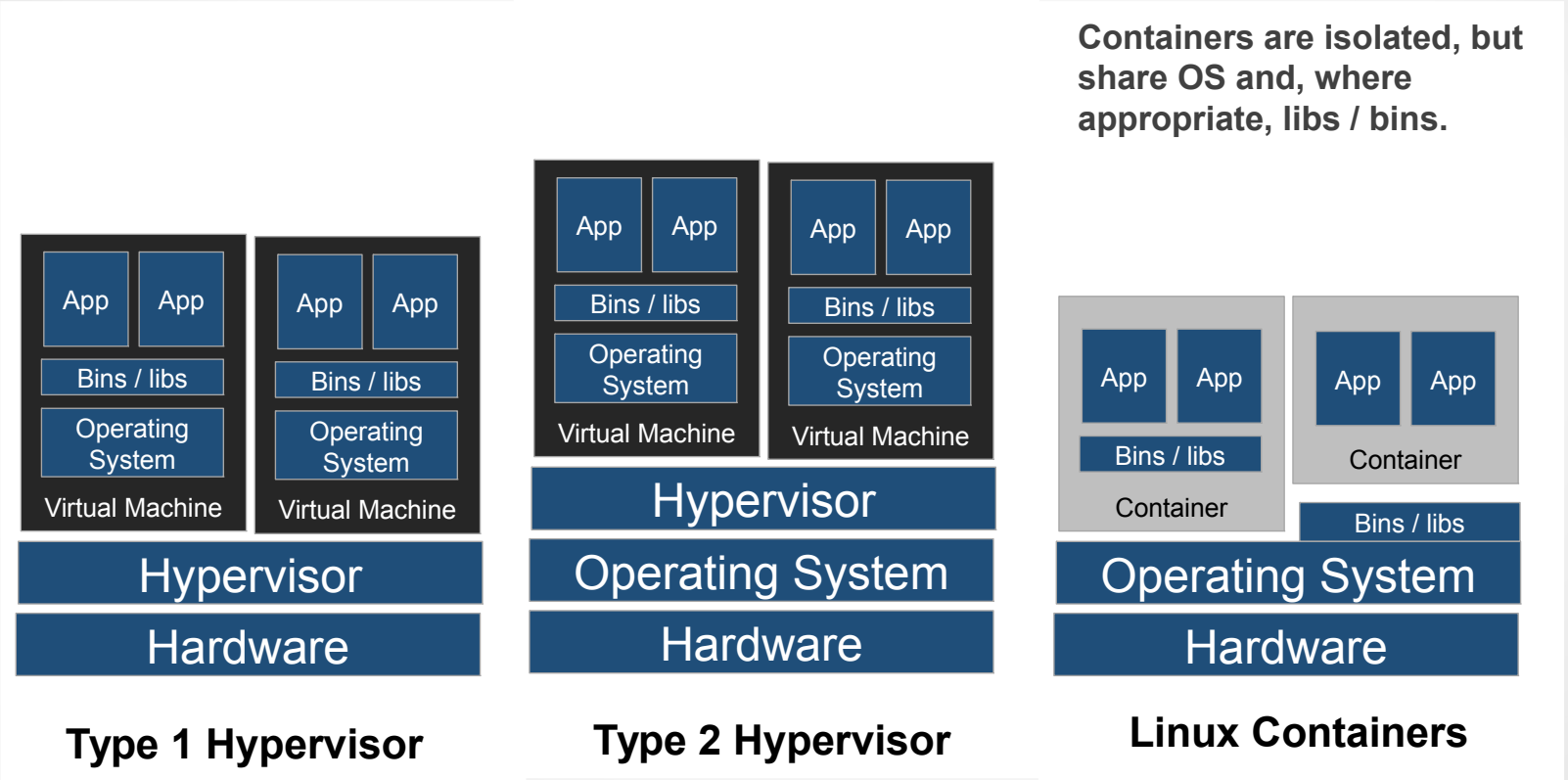
- Containers isolate and encapsulate your application workloads from the host system.
- Run multiple versions of an operating system on a single server
- Lightweight; provision and boot in milliseconds
- Near bare metal runtime performance
- Flexibility
- Containerize a “system”
- Containerize “application(s)”
- Growing in popularity

But doesn't virtualization do this?

Yes, but what about...

- Size on HDD
- Performance
- Resource Utilization

Hypervisor vs. Linux Containers

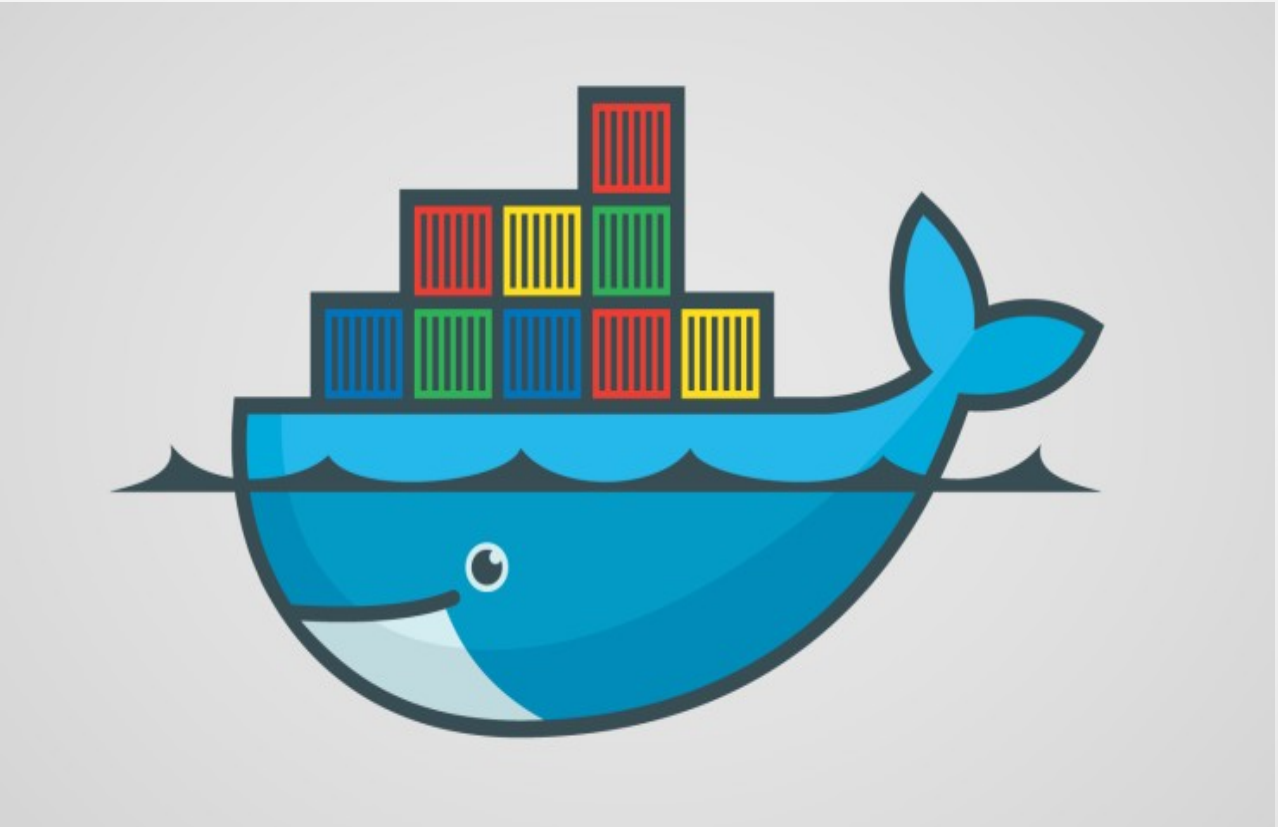


Is it game over for VMWare then?

Not so fast! Virtualization is mature with extensive tooling and ecosystems to support its deployment across various environments. And for workloads that require a non Linux OS or a specific kernel virtualization remains the only way.

What is Docker?

- Docker is a tool created by the folks at dotCloud in 2013 to make using LinuX Containers (LXC) easier to use.



Now, it is time for the Demonstration!

Is it safe to use Containers?

- “LXC is not yet secure. If I want real security,I will use KVM.”

  - Dan Berrangé (famous LXC hacker)

- “From security point of view lxc is terrible and may not be consider as security solution.”

  - Someone on Reddit

- Common opinion among security experts and paranoid people.
- To be fair, they have to play safe & can't take risks.

Fast Solutions

- don't run things as root
- drop capabilities
- enable user namespaces
- get rid of shady SUID binaries
- enable SELinux (or AppArmor)
- get a GRSEC kernel (https://grsecurity.net/)
- update kernels often
- mount everything read-only

Any Questions?

Thank You!