Primera jornada de charlas

Marzo 2017

¿ 

?

=

Tandil + **Comunidad** + InfoSec/Tecnología

- Reuniones mensuales
- Charlas
- Conferencias
- CTFs
- Talleres
- Hackathones
- ..

Introducción a contenedores en Linux

Objetivo

- Conceptos fundacionales de contenedores
- Contenedor != Docker/rkt/CoreOS/.. (+/-)
- Profundizar en cómo funciona
- DIY!

Linux y Kernel de Linux

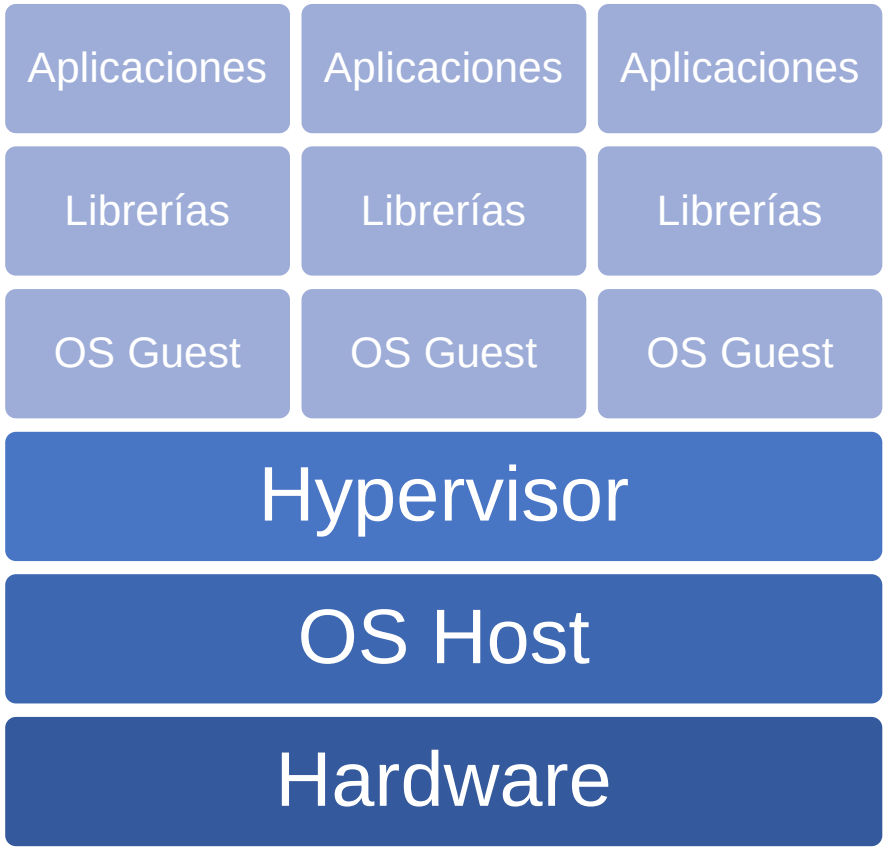
- Linux
  - Sistema operativo de código libre y abierto
- Kernel
  - Núcleo del sistema operativo
  - Arquitectura monolítica
- Conceptos
  - Procesos
  - Llamadas al sistema
  - Estructuras internas del Kernel

Virtualización

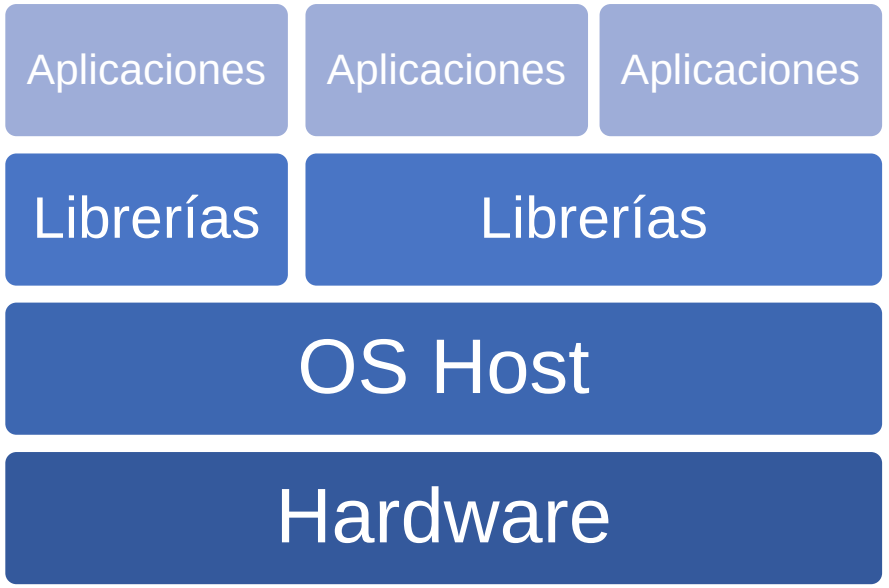
- Crear mediante software una versión virtual de recursos

- Completa
  - Xen
  - KVM
  - VirtualBox, Hyper-V, VMWare, Parallels
  - ..
- Liviana (o por sistema operativo)
  - OpenVZ
  - Jaulas (chroot, FreeBSD jail)
  - **Contenedores!**
  - ..

Máquinas Virtuales (VMs)



Contenedores



Control groups (cgroups)

- Característica del Kernel >= 2.6.24 (2008)
- Actúa sobre procesos
- Permite **limitar, priorizar, registrar y controlar** recursos
  - Memoria
  - CPU
  - Entrada/Salida
  - Red

Namespaces

- Característica del Kernel >~ 2.4.19 (2002)
- Cada proceso tiene su propia vista del sistema
- Permite **separar y agrupar** recursos
  - Sistema de archivos
  - Identificadores de procesos
  - Red
  - Comunicación interprocesos
  - Nombre de máquina/dominio
  - Usuarios

cgroups + namespaces = Contenedores!

- Granularidad / flexibilidad de acuerdo las necesidades

- Ejemplos
  - 1 – Crear un namespace de archivos
  - 2 – Unirse a un namespace existente
  - 3 – Crear un “contenedor” entero

Seguridad

- Aplicaciones
  - Isolar procesos (“sandbox”)
    - Ej. Chrome
  - Correr código no confiable
    - Ej. Servicios en el cloud

- **Kernel compartido por todos los contenedores!**
  - Contenedor-> Bug en una syscall -> Host

- Recomendaciones
  - Montar lo mínimo
  - Filtrado de syscalls (BPF)
  - **+++**

Referencias

- *The Linux Programming Interface* - http://www.man7.org/tlpi/
- https://en.wikipedia.org/wiki/Operating-system-level_virtualization
- https://en.wikipedia.org/wiki/Cgroups
- https://en.wikipedia.org/wiki/Linux_namespaces
- https://www.nccgroup.trust/us/our-research/understanding-and-hardening-linux-containers/
- https://www.nccgroup.trust/us/our-research/abusing-privileged-and-unprivileged-linux-containers/

Imagen de contenedores: https://es.wikipedia.org/wiki/Archivo:Line3174_-_Shipping_Containers_at_the_terminal_at_Port_Elizabeth,_New_Jersey_-_NOAA.jpg

Gracias!

Próximos eventos:

- Reunión mensual Abril
- FliSol Tandil (22 de Abril 2017)