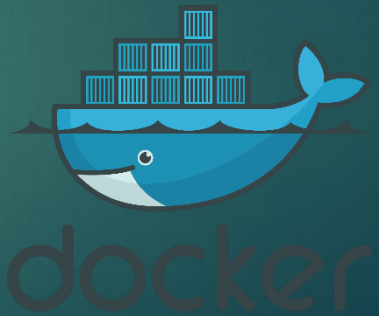
Virtualización de servidores y contenedores



MARTÍN GIL BLANCO

La virtualización: Conceptos

- Permite mejorar el aprovechamiento de recursos.
- Actualidad → perdiendo popularidad por el uso del Cloud.
- La virtualización es manejada por el proveedor de Cloud.
- Seguridad de la infraestructura.
  - Objetivo: separar y aislar al máximo cada aplicación o servicio.
  - Cuanto más aisladas estén las aplicaciones, menor es el impacto de una vulnerabilidad.
  - Se usan conceptos como “sandboxes”, jaulas o contenedores para encapsular cada servicio.
- Productos conocidos
  - VirtualBox
  - VMWare
  - Proxmox
  - Xen Hypervisor
  - Tecnoloogías de contenedores y especialmente Docker.io

La virtualización: Conceptos

- Hipervisor (o VMM, Virtual Machine Monitor): Software que controla la ejecución de las máquinas virtuales monitorizándolas y tomando el control de ellas cuando es necesario. A menudo se usan varios en la misma organización lo que hace necesario el uso de herramientas multihipervisor.
  - Sistema Anfitrión (host): Engloba al hardware real y al sistema operativo que se ejecuta sobre el hardware real.
  - Sistema Invitado (guest): Engloba al hardware virtualizado y al sistema operativo y aplicaciones que se ejecutan sobre este hardware virtual.

La virtualización: Ventajas

- Aislamiento de los servicios → importante.
- Reduce riesgos y costes al necesitar un único servidor. También se reduce en espacio, tiempo, dinero y se mejora la seguridad.
- Mejora procesos de clonación y copia de seguridad.
- Menor consumo energético.
- Más fácil la recuperación ante desastres al recuperar copias de seguridad de una forma más sencilla.
- Más fácil administrar.
- Permite añadir rápidamente recursos a los servidores balanceados o quitárselos.
- Hay menos componentes físicos lo que implica una reducción de los puntos de fallo posibles en nuestra infraestructura.

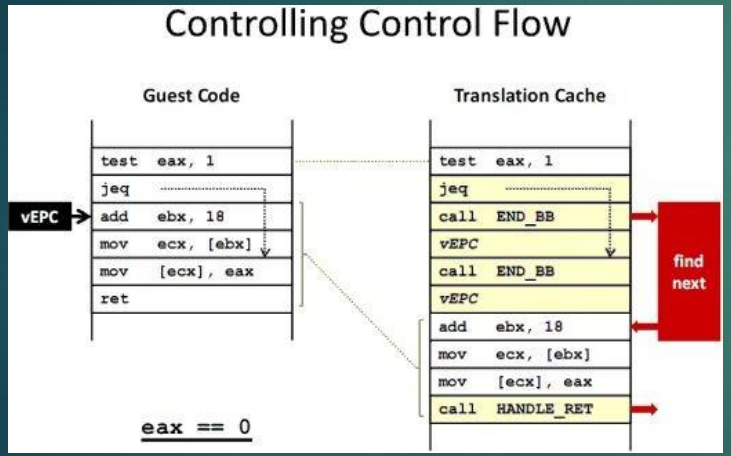
La virtualización: Desventajas

- Hay una gran inversión de software al principio, lo que puede suponer un obstáculo.
- El rendimiento de las máquinas virtuales puede ser algo más bajo.
- La máquina física o anfitrión es muy crítica.
- Algunos proveedores cobran licencias por cada guest.
- Si la planificación previa es incorrecta y no se dimensionan bien los recursos puede/n saturarse el/los servidor/es.
- Hay un conocimiento que se hace necesario para los administradores.

Conceptos relacionados

- Simulación: software que copia el comportamiento de otro intentando ser lo más parecido al que se trata de imitar. Cisco Packet Tracer.
- Emulación: ejecución de programas de ordenador en una plataforma diferente para la que fueron escritos originalmente. E.g. Emuladores de recreativas Callus, mame, No$gba (Nintendo DS). Tecnología de emulación de Apple (Roseta).
- Virtualización: El guest se ejecuta directamente sobre el hardware host anfitrión. El sistema anfitrión e invitado deben de operar en la misma arquitectura. El hipervisor sólo media en los accesos de los invitados al hardware real (e.j. disco duro → fichero imagen). Los guests tienen velocidad casi nativa.
  - *Instrucciones "peligrosas"*: acceso al hardware (e.j. dispositivo USB, o dispositivo de red), acceso a memoria, acceso a dispositivos de almacenamiento…
  - El hipervisor tiene que tomar el control al ejecutar este tipo de instrucciones.

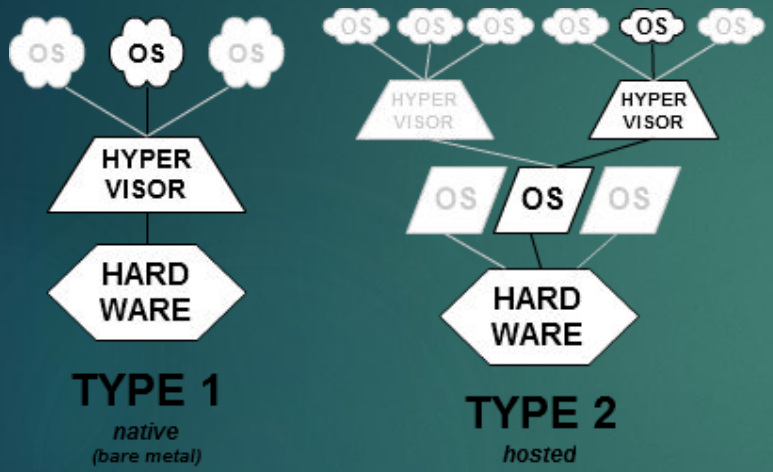
Soluciones para la virtualización: completa



Virtualización completa en host (VMWare, 1999)

- Traducción binaria: El hipervisor dispone de un hilo para cada máquina virtual que ejecuta el proceso de traducción y va almacenando instrucciones a ejecutar (ya con las operaciones peligrosas) ya en una zona de memoria.
- Las instrucciones “peligrosas” (escrituras a disco, acceso a periféricos y accesos a memoria) se traducen para evitar que se produzcan desastres. Las instrucciones no peligrosas se copian directamente.

Soluciones para la virtualización: nativa



Virtualización completa con hipervisor a nivel de kernel (nativa) (VMWare ESX, 2002, luego conocido como VMWare ESXi):

- Producto de TIPO I (también conocido como native, bare metal o hipervisor a nivel de kernel).
- El hipervisor es parte del kernel (a menudo prácticamente la totalidad -micronúcleo- así que funciona mejor).
- Pequeña mejora sobre TIPO 2.
- Mantenemos el sistema de traducción binaria visto anteriormente.

Soluciones para la virtualización: paravirtualización

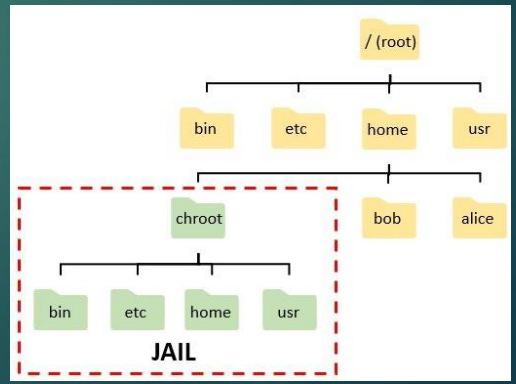
- Paravirtualización (Xen, 2003)
  - Universidad de Cambridge (investigación en el año 2002)
  - Idea: Sólo el kernel ejecuta traducciones peligrosas → ¿Sería posible traducir el kernel open source (Linux) para que las operaciones peligrosas fueran llamadas al hipervisor (hiperllamadas)?
  - Se construyeron dos versiones del kernel de Linux. Una para equipos normales y otra para el guests paravirtualizados. Se contruyó un microkernel Xen para que fuera una solución de virtualización TIPO I (native / bare metal).
  - Ventajas:
    - Es el kernel traducido el que se ocupa de llamar directamente al hipervisor.
    - Se reduce significativamente el trabajo del hipervisor: Los invitados se ejecutan directamente sobre el hardware del anfitrión sin intervención del hipervisor.
    - Fué un auténtico bombazo porque se estimaba una sobrecarga del 2% que es ridícula respecto a la de una solución de virtualización completa (traducción binaria).

Soluciones para la virtualización: asistida por hardware

- Virtualización asistida por el hardware (Intel, AMD).
  - La paravirtualización no valía para sistemas operativos propietarios (Windows, OSX, etc.)
  - El procesador detecta la ejecución de instrucciones peligrosas e invoca al hipervisor a través de la ejecución de código de ciertas zonas de memoria.
  - Inter Pentiun IV incorporó a finales de 2005 la tecnología VT-x.
  - AMD incorporó en sus procesadores en 2006 AMD-SVM (AMD-Secure Virtual Machine) que luego se llamaría AMD-V (AMD-Virtualization).
  - Via (antiguos procesadores Cyrix) desarrolló VIA VT.
  - A partir de 2006 paulatinamente desaparece la traducción binaria (en la actualidad nula).
  - VirtualBox (lanzado en 2007) no puede funcionar sin estas extensiones (por ejemplo, Intel Virtualization technology).

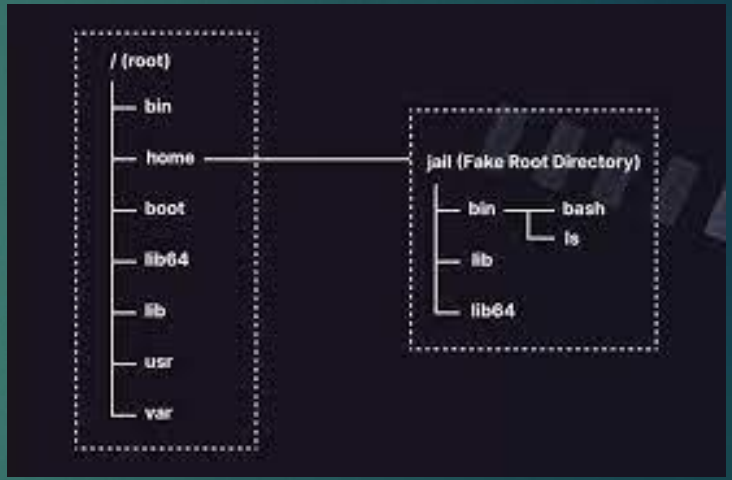
Soluciones para la virtualización: contenedores

- Virtualización a nivel del sistema operativo (virtualización basada en contenedores, contenerización con contenedorización).
  - Problema de la virtualización anterior: Cada máquina virtual tiene un kernel en memoria que ocupa espacio y consume ciclos de CPU.
  - Se pretende conseguir aislamiento (la característica más importante de la virtualización) pero con un único kernel (el que ejecuta el anfitrión).
  - Se parte de la idea de chroot (BSD Unix versión 7, año 1979). Se permite cambiar el directorio raíz (/) visible para un usuario o aplicación.



Soluciones para la virtualización: contenedores

- El problema de la virtualización hasta este punto es que requiere un sistema operativo para el invitado completo, lo que implica una gestión de recursos destacable.
- Virtualización a nivel del sistema operativo (virtualización basada en contenedores, contenerización con contenedorización).
  - En 1991 Bill Cheswick habla por primera vez del concepto Jail (jaula).
  - En el 2000 surge el comando Jail de FreeBSD.
  - En 2002 se incluye Makejail en las principales distribuciones de Linux.

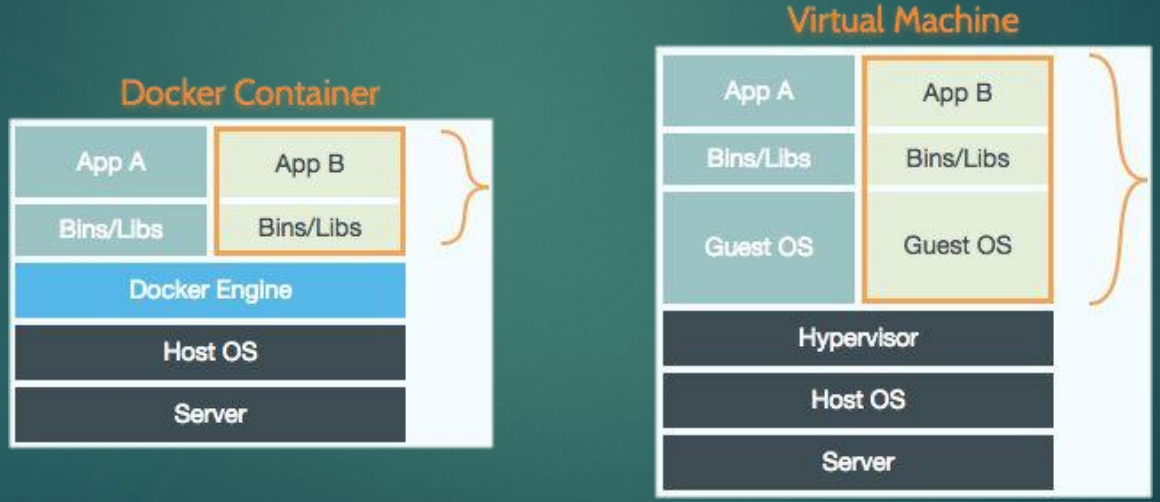


Soluciones para la virtualización: contenedores

- Virtualización a nivel del sistema operativo (virtualización basada en contenedores, contenerización con contenedorización).
  - Solaris Containers (Solaris 10, 2005). La 51 beta de Solaris 10 ya lanzada en febrero de 2004 tenía esta característica.
  - Un contenedor era un conjunto de procesos de un contenedor se ejecutaban en una "zona" separada. Los procesos ejecutados en una zona no se podían comunicar con los demás.
  - En 2005 surge OpenVZ/Virtuozzo que permitía crear contenedores (llamados SPV, Servidores Privados Virtuales). Se incorporó una modificación del kernel del linux para incorporar la noción de entorno virtual. Cada contenedor ya tenía sus propias interfaces de red separadas, su propio sistema de ficheros.
  - En el año 2008 se introduce en Linux el la funcionalidad cgroups (control de grupos) que permite aislar grupos de procesos concediéndoles unos determinados recursos (CPU, memoria, IO a disco) y aislándolos de los demás grupos. Es la base para la aparición de LinuX Containers y, más tarde, Docker IO.

Soluciones para la virtualización: contenedores

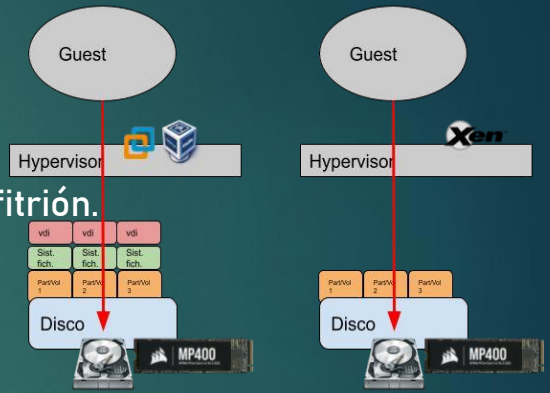
- Virtualización a nivel del sistema operativo (virtualización basada en contenedores, contenerización con contenedorización).



Soluciones para la virtualización: contenedores

- Virtualización a nivel del sistema operativo (virtualización basada en contenedores, contenerización con contenedorización).
  - Ventajas:
    - Sólo se mantiene un kernel en ejecución (lo comparten anfitrión e invitados).
    - El arranque del contenedor es inmediato.
    - El consumo de memoria y CPU se reduce al máximo.
    - Se puede particionar mucho más ya que las sobrecargas adicionales son muy pequeñas.
    - No requiere extensiones de virtualización.

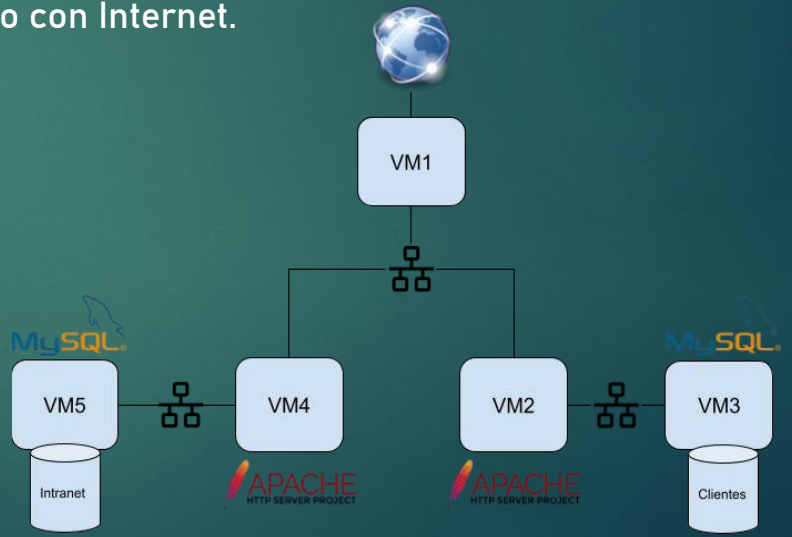
Elementos de un sistema de virtualización



- Acceso al hardware del anfitrión
  - El procesador y la RAM se comparte siempre
  - Se puede acceder a dispositivos USB conectados al anfitrión.
  - Muy limitado en contenedores
- Representación del almacenamiento
  - Imágenes de disco
  - Formato de imagen dinámico: se reserva el espacio dinámicamente)
  - Formato de imagen splitted (partido): Se representan en varios ficheros
    - Interesante según el sistema de ficheros subyacentes (XFS vs EXT4)
  - RAW vs VDI (VirtualBox, dinámico) o VMDK (VMWare, dinámico y splitted)
  - Layered-based FS en Docker
  - Estrategias de representación de las imágenes RAW en volúmenes LVM (particiones) o en LUNs.

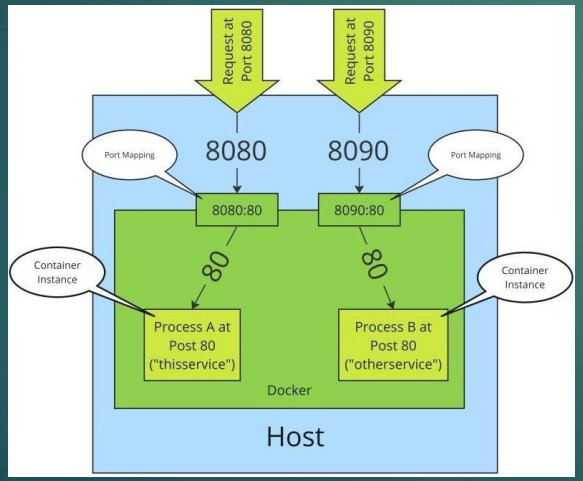
Elementos de un sistema de virtualización

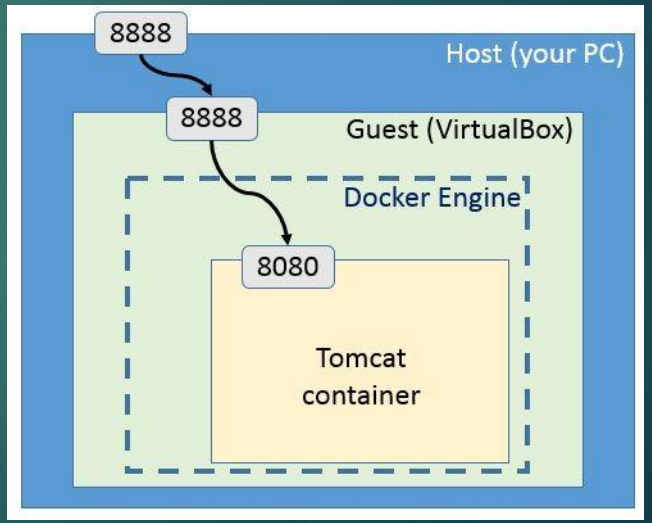
- Red
  - Distintos tipos de dispositivos con distintas características y donde se va a poder limitar que dispositivos de red virtuales se interconectan entre si y si existe o no posibilidad de conectar con el anfitrión o con Internet.
  - Muy importante → Aislamiento



Elementos de un sistema de virtualización

- Red
  - Posibilidad de reenvío de puertos (port forwarding).
    - En contenedores especialmente importante para permitir que el tráfico que llega al host lo atienda uno de los contenedores.





Elementos de un sistema de virtualización

- Red

Tipo de red	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Solo host	✔	✔	✔	-	-
Red interna	-	-	✔	-	-
Adaptador puente	✔	✔	✔	✔	✔
NAT	✔	Port forward	-	✔	Port forward
Red NAT	✔		✔	✔	

Elementos de un sistema de virtualización

- Otros
  - Carpetas compartidas
  - Portapapeles
  - Arrastrar y soltar
  - Integración del ratón
  - Aceleración 3D en el guest
  - …

Libguestfs-tools

- Posibilidad de tratar las imágenes de disco al mismo nivel de los discos
  - Obtener información de una imagen
  - Extender una imagen
  - Montar una imagen en un directorio
- Muy útil con para trabajar con virtualización