75-08 Sistemas Operativos
Lic. Ing. Osvaldo Clúa
2010

Facultad de Ingeniería
Universidad de Buenos Aires

Virtualización

Virtualización

- La abstracción de recursos de computación
  - Virtualización de Aplicaciones.
  - Virtualización de Plataforma.
  - Virtualización de Escritorio.
  - Virtualización de recursos.
    - Red, Memoria, Almacenamiento, clusters, grids.

¿Para qué se usa?

- Aumento de confiabilidad.
  - El software tiene mas fallas (bugs) que el Hardware.

- Aplicaciones antiguas ("legacy").
- Desarrollo y prueba en múltiples plataformas.
- Balanceo de cargas y escalabilidad futura.
  - Es mas fácil migrar de una VM a otra en un host demasiado cargado.

Virtualización de Aplicaciones

- Compatibilidad y portabilidad entre distintos Sistemas Operativos y distintas arquitecturas.
  - Máquinas Virtuales (JVM, .net CLR)
  - Compatibility Layers
    - Wine,WOW,WOW64,Linux on BSD.
      - En general requiere de una CPU compatible (upwards)

Virtualización de Plataforma

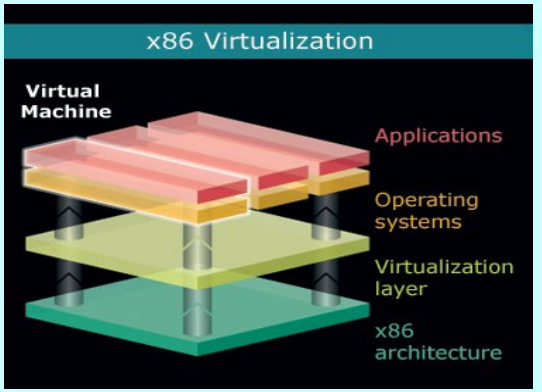
- Abstracción de todos los recursos de computación de un huésped dentro de un anfitrión (host).
  - Virtualización total.
    - Emulación de plataforma.
    - Hipervisores
  - Paravirtualización.
  - Virtualización del mismo Sistema Operativo.

¿Cuando es posible virtualizar?

- Condiciones de Popek y Goldberg.
  - Instrucciones privilegiadas
    - Las que ocasionan un software trap.
  - Instrucciones delicadas ("sensitive")
    - Las que solo pueden ejecutarse en Modo Supervisor del procesador.
- Una arquitectura es virtualizable si las instrucciones delicadas son un subconjunto de las privilegiadas
  - La arquitectura Intel IA32 no lo es.
    - Por ejemplo, POPF tiene distintos resultados según el modo del procesador ...

Virtualización de la IA32

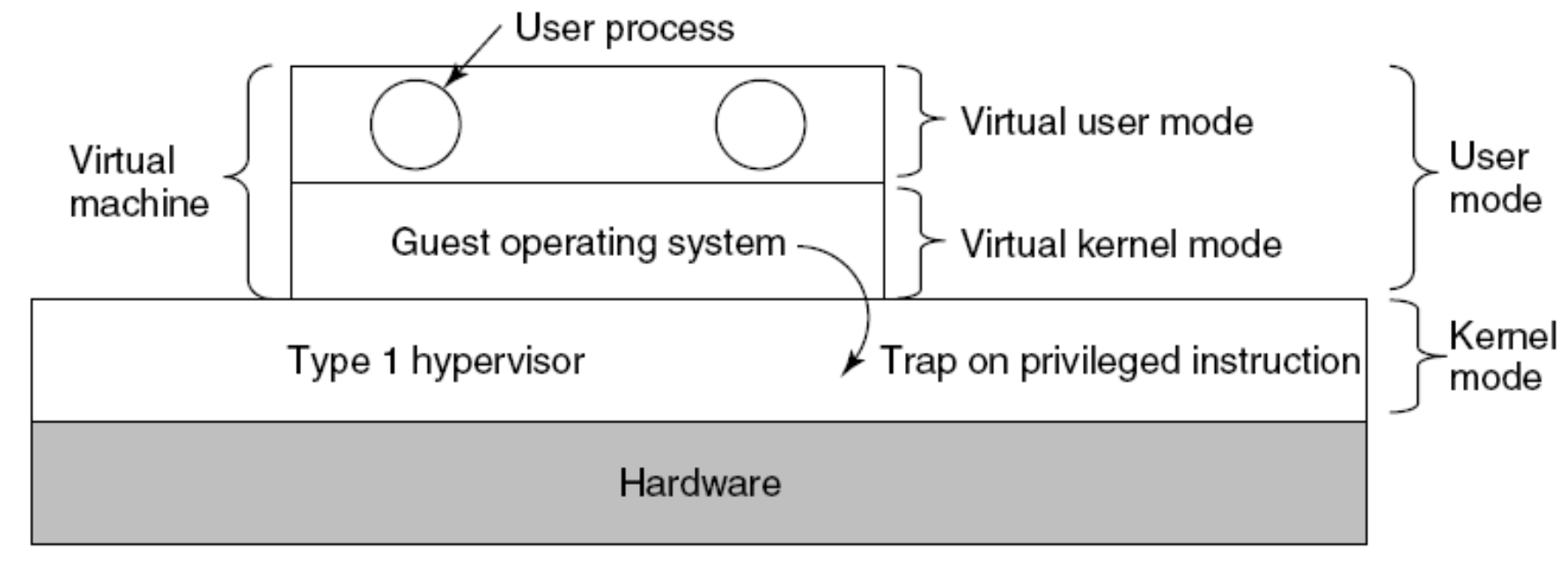
- AMD-V o Pacífica para procesadores AMD.
- Intel IVT o Vanderpool.
  - La idea es generar "containers" donde la ejecución de una instrucción delicada provoque un software trap.
    - (trap & emulate)
    - Usando IOMMU para acceder a memoria virtual



Hipervisores

- Monitor de máquinas virtuales
  - Tipo I
    - Corren directamente sobre el Hardware.
    - El huésped debe tener una arquitectura virtualizable.
  - Tipo II
    - Corre como un programa bajo un sistema operativo anfitrión (Host).
    - Pueden virtualizar cualquier ambiente.

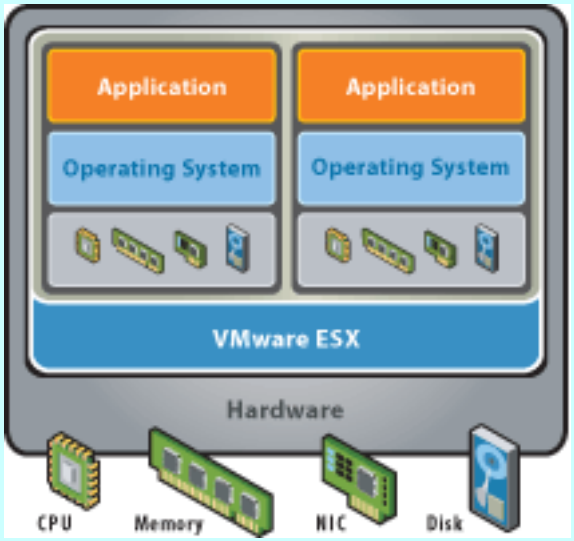
Hipervisor Tipo I



- El huésped corre en modo usuario.
  - Su Kernel cree haber pasado a modo supervisor, pero continúa en modo usuario.

Hipervisor Tipo I (2)

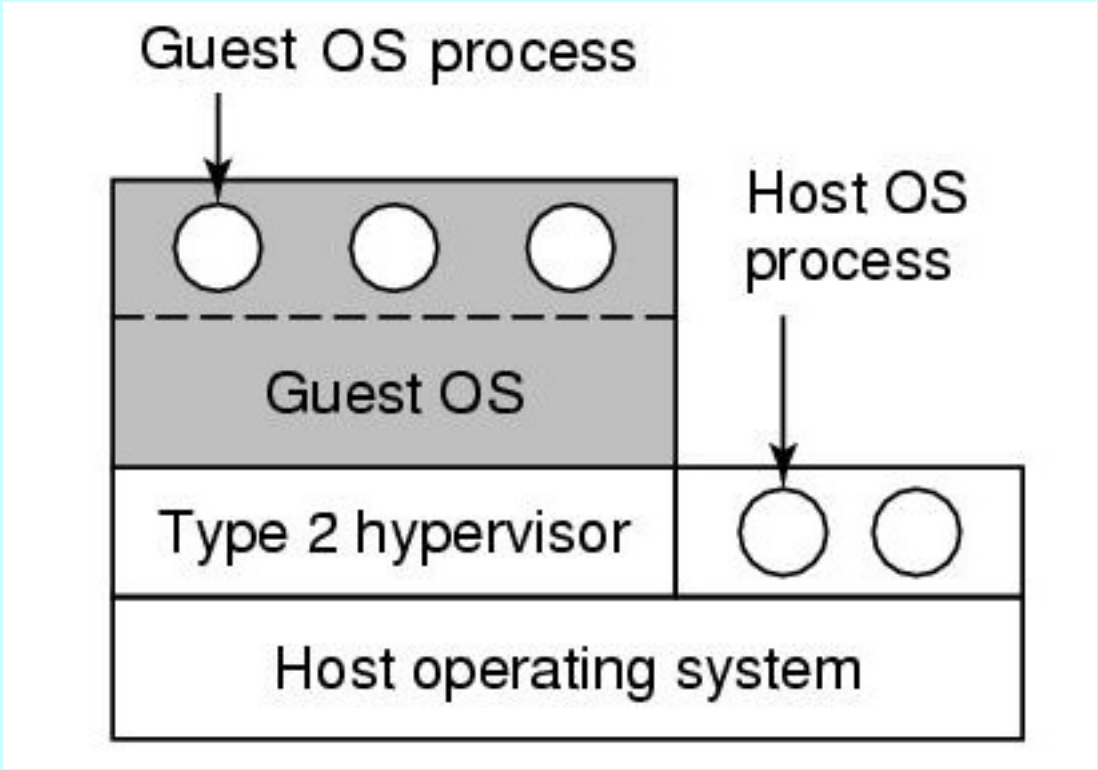
- Al ejecutar una instrucción delicada,se produce una software trap.
- El Hipervisor toma el control.



- Si la trap proviene del kernel del guest, lleva a cabo la acción correspondiente.
- Si proviene de un programa en modo usuario, responde como lo haría el Hard.

–VMware ESX, Xen, Hyper-V

Hipervisor Tipo II



- Corre bajo el control de otro sistema operativo.
- Modifica el programa que está corriendo.

Binary translation

- Basic Block
  - Código con un punto de entrada, uno de salida y sin "jumps".
- El Hipervisor examina los Basic Blocks ...
  - ... y reemplaza las instrucciones delicadas por llamadas al hipervisor
  - ... y guarda el código traducido en el cache.
    - Lo que aumenta su performance.

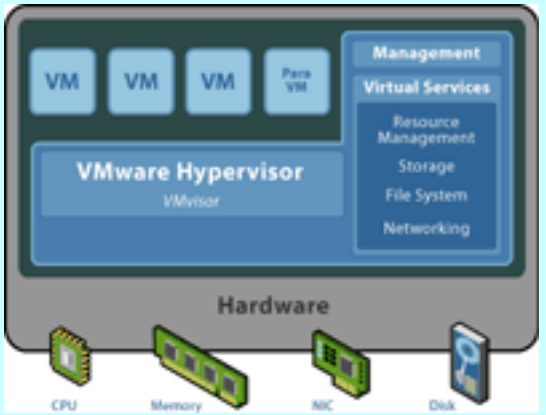
Hipervisores

- El tipo I no siempre es mas rápido que el tipo II.
  - Las traps consumen muchos recursos.
    - Y una vez en el cache, el tipo II tiene velocidad casi nativa.

- Virtual PC, VMware server, Virtual Box

Paravirtualización

- Reemplazar en el sistema operativo guest las instrucciones delicadas por llamadas al hipervisor.
  - Una API es VMI de Vmware.
  - Requiere modificaciones en el guest.
    - En Linux a partir del Kernel 2.6.21.
    - La mayor parte de los hipervisores la adoptaron como opción.



Máquinas Virtuales

- La lista de VM sigue creciendo ...
  - ... y aparece una nueva forma de distribución, los Aparatos Virtuales o Virtual Appliances.
  - ...o de distribución de aplicaciones usando streaming.
- Algunos enfoques diferentes:
  - Un traductor binario dinámico: QuickTransit.
  - Uno destinado a los empotrados: MPLAB (ICE).

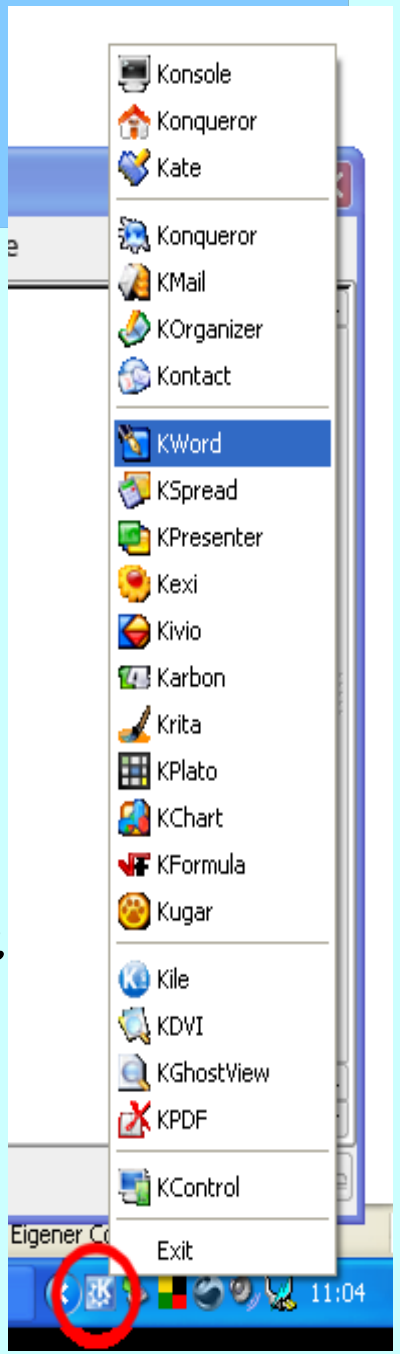
Virtualización del Escritorio

- Las aplicaciones se hospedan en un sistema central pero cada usuario tiene su escritorio local.
  - Concepto tomado de los thin client.
    - Citrix, MokaFive y varios mas.
    - Y algunos Web Desktops como Glide o eyeOs

Virtualización de recursos

- Usar los recursos del sistema operativo host para apoyar la ejecución del guest.

  - Colinux Es un kernel que corre como servico de XP...
  - ...y andlinux es una aplicación de colinux



Virtualización del Sistema Operativo

- Cuando el Kernel permite distintos ambientes de usuarios aislados entre sí.
  - Una extensión del chroot.
  - Usado por seguridad en aplicaciones como hosting virtual.
  - Linux VServer, Virtuozzo, Solaris containers o BSD Jails.

El lado (azul) oscuro ...

- En una conferencia de seguridad, Joanna Rutkowska afirma tener una píldora que despierta a Windows en la Matrix...