CC4302
Sistemas Operativos
Profesor: Luis Mateu

- Virtualización
- Virtualización del hardware
- Tipos de virtualización
- Los desafíos de la virtualización completa y su implementación
- Espacios de direcciones virtuales virtuales

Virtualización

- Es el acto de crear una versión virtual de algo **al mismo nivel** de abstracción.
- Ejemplos: virtualizar el computador, virtualizar el disco o virtualizar la red.
- Tiene que ser el mismo nivel de abstracción, es decir si se virtualiza un computador x86, el resultado es también un computador x86 pero virtual.
- Crear una versión virtual de un computador arm en un computador x86 no es virtualizar, es **emular**.
- Fuente: Wikipedia
- Pionero: El hipervisor VM/370 de los IBM 370 ofrecía una máquina virtual (VM) a cada usuario. La VM corría el sistema operativo CMS que era monoproceso, pero también podía correr VM/370.

Virtualización del hardware

- Es la virtualización de un computador, como plataforma completa, algunas de sus componentes o solo **la funcionalidad requerida para correr un sistema operativo** (invitado o guest).
- Se ocultan las características físicas de la plataforma real (anfitrión o host) presentando una plataforma abstracta.
- En el anfitrión el software que realiza la virtualización se denomina *hipervisor* y requiere privilegio de administrador para instalar módulos en el núcleo del sistema operativo anfitrión.
  Ejemplos: VirtualBox, Vmware, Hyper-V, Xen, Kvm
- Permite correr múltiples sistemas operativos en un solo computador: uno actúa como anfitrión y el resto como invitados.
- Facilita la administración de granjas de servidores.

Tipos virtualización de hardware

- Completa (full): la abstracción ofrece el mismo set de instrucciones que el del computador anfitrión, permitiendo correr el sistema operativo invitado sin ninguna modificación. Ejemplo: VM/370
- Asistido por harware: el computador anfitrión incluye hardware específicamente destinado a su virtualización para mejorar el desempeño.
- Paravirtualización: la máquina virtual no necesariamente ofrece el mismo hardware del computador anfitrión. Podría no ofrecer las instrucciones privilegiadas como inhibir las interrupciones. A cambio ofrece una biblioteca de funciones que proveen la misma funcionalidad. Se necesita modificar el sistema operativo para que llame a estas funciones en vez de usar las instrucciones privilegiadas.

Beneficios de la virtualización

- Snapshots: se graba el estado de la máquina virtual en un instante dado, para que sea restaurado más tarde de ser necesario, por ejemplo porque se descubrió un virus.
- Migración: la máquina virtual se transporta a otra máquina física, porque se requiere hacer mantención en la máquina física original.
- Failover: Cuando falla la máquina virtual, se restaura a una snapshot que se conoce en un estado consistente con el fin de mejorar la disponibilidad del sistema
- Containerization: Es una máquina virtual que ofrece un mejor aislamiento del resto de los usuarios, que lo que ofrecen los procesos y archivos.

Los desafíos de la virtualización completa

- El núcleo del sistema operativo invitado corre sin cambios.
- El núcleo del sistema operativo necesita ejecutarse en modo sistema para poder ejecutar las instrucciones privilegiadas como inhibir/habilitar interrupciones, establecer las tablas de páginas para implementar los espacios de direcciones virtuales.
- Permitir que los núcleos invitados se ejecuten en modo sistema significaría que si un núcleo invitado se cae, ¡se cae también el anfitrión!
- Se necesita correr los núcleos invitados en modo usuario, como cualquier otro proceso.
- Cuando un núcleo invitado ejecuta la instrucción que inhibe las interrupciones: ¡se gatilla una interrupción que captura el anfitrión!

Implementación

- Las interrupciones gatilladas por instrucciones privilegiadas de un núcleo invitado son capturadas por el hipervisor.
- Emula el comportamiento de esas instrucciones.
- El núcleo invitado no captura ninguna interrupción real.
- El anfitrión captura todas las interrupciones, pero redirige al hipervisor las relacionadas con un núcleo invitado.
- El hipervisor gatilla la interrupción virtual en el núcleo invitado solo cuando están habilitadas por el núcleo invitado.
- Es similar a lo que ocurre con las señales de Unix, solo que las señales están relacionadas a eventos abstractos, no a dispositivos.
- Las interrupciones en el núcleo invitado están relacionadas a dispositivos virtuales.

Espacios de direcciones virtuales virtuales

- El núcleo invitado cree tener acceso a la memoria real del computador.
- Pero lo que considera memoria real es solo su propio espacio de direcciones virtuales, provisto por el anfitrión.
- El núcleo invitado construye tablas de páginas para sus propios procesos. No sirven porque referencian las páginas virtuales del núcleo invitado.
- Durante el cambio de contexto ejecuta la instrucción que cambia la tabla de páginas, gatillando una interrupción por instrucción privilegiada.
- El hipervisor traduce la tabla de páginas virtuales a una tabla de páginas reales.