La arquitectura de les màquines virtuals

Lluís Garrido

lluis.garrido@ub.edu

Grau d'Enginyeria Informàtica

Introducció

La virtualització és una eina important avui en dia.

- S'utilitzen en disciplines que cobreixen aspectes com sistemes operatius, llenguatges de programació o arquitectures de processadors.
- Les màquines virtuals milloren la interoperatibilitat de programari, la inexpugabilitat de sistemes o la versatilitat de sistemes.
- Allibera els desenvolupadors de les restriccions d'interfície i de recursos.

En aquestes transparències cobrim els aspectes bàsics de les màquines virtuals i els descrivim de forma unificada.

Concepte: abstracció i virtualització

Al primer tema hem vist que el sistema operatiu proveeix d'abstracció del maquinari

- Les aplicacions disposen d'una interfície comuna per utilitzar el maquinari; les aplicacions poden ser escrites de forma independent del dispositiu específic.
- Aquesta abstracció facilita que el programari (aplicacions d'usuari, sistemes de fitxers, ...) i el maquinari pugui evolucionar de forma pràcticament independent.

Concepte: abstracció i virtualització

Hi ha altres tipus d'interfícies que proveeixen abstracció

- El USB (Universal Serial Bus) és un estàndard que defineix el cablejat, connector i protocol de comunicacions per comunicar i alimentar perifèrics d'ordinador.
- L'ISA (Instruction Serial Architecture) és una interfície que permet que Intel i AMD desenvolupin microprocessadors que implementin el conjunt d'instruccions Intel IA-32 (x86).

Concepte: abstracció i virtualització

Interfícies ben definides també tenen les seves limitacions

- Un aplicació compilada, binària, està restringida a executar-se a una ISA específica i depèn d'una interfície específica de sistema operatiu.
- Components dissenyades per a una interfície determinada no funcionaran amb altres interfícies.

La falta d'interoperatibilitat és restrictiva, especialment avui en dia, en un món amb ordinadors connectats en xarxa. Seria ideal poder moure programari de forma "lliure" de forma similar amb què ja ho fem amb les dades!

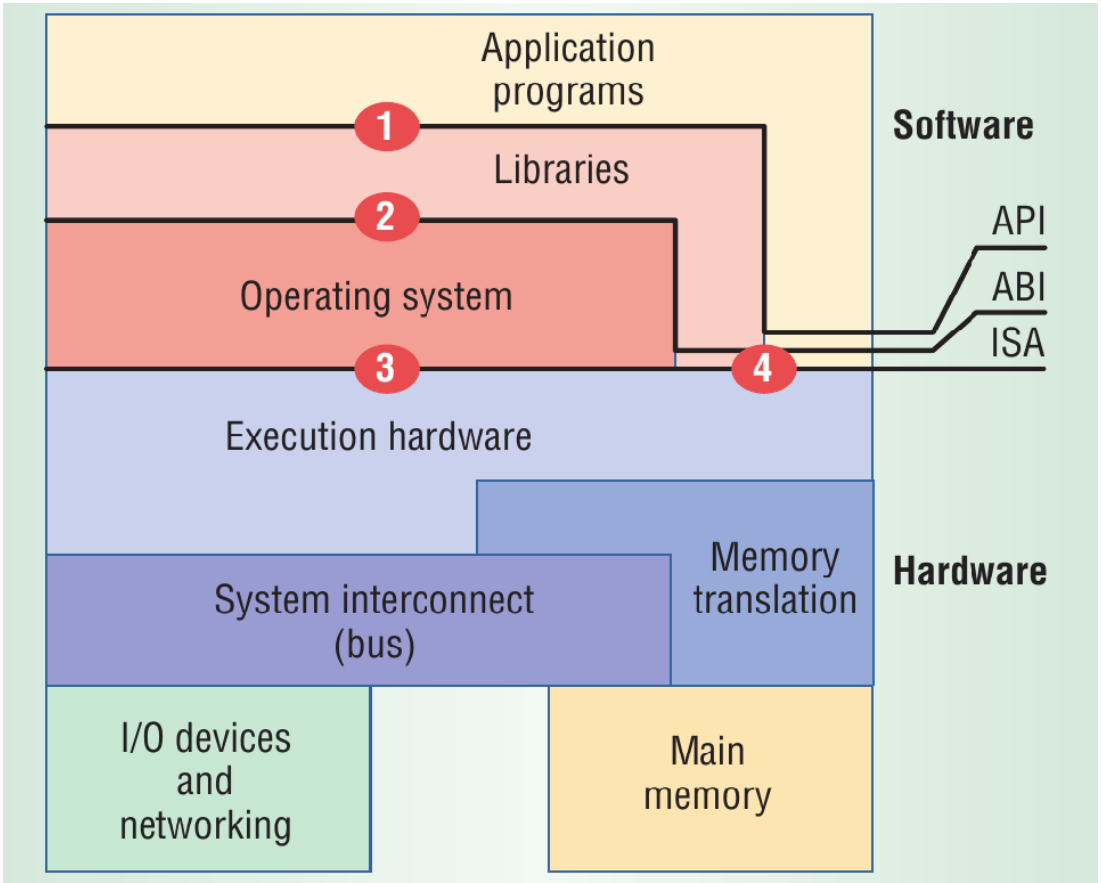
Concepte: abstracció i virtualització

La virtualització és una forma d'abordar les limitacions anteriors

- Virtualitzar un sistema o component (processador, memòria, dispositiu) implica mapar la interfície i recursos d'aquest sistema a sobre d'una interfície i recursos d'un sistema real, possiblement diferent. El sistema real apareix a les aplicacions com un sistema virtual diferent, o inclús com múltiples sistemes virtuals.
- A diferència de l'abstracció, no es tracta de simplificar els detalls, sinó d'afegir una capa de programari per suportar la arquitectura desitjada. Es "burlen" doncs les limitacions i compatibilitat de la màquina real.

Interfícies

Es mostren aquí tres interfícies (ISA, ABI i API) especialment importants per a la construcció d'una màquina virtual.



Interfícies

- ISA (Instruction Set Arquitecture): marca la divisió entre maquinari i programari; correspon a les interfícies 3 i 4. El 3 correspon al mode privilegiat d'execució i el 4 al mode usuari d'execució.
- ABI (Application Binary Interface): permet a les aplicacions accedir als recursos i serveis del maquinari mitjançant a les crides a sistema del sistema operatiu, interfície 2, o al maquinari directament, interfície 4.
- API (Application Programming Interface): permet a les aplicacions accedir als recursos i serveis del maquinari mitjançant llibreries, interfície 1 i 4. Les llibreries acostumen a permetre que una aplicació sigui fàcilment portable si es recompila l'aplicació.

Màquines virtuals: processos i sistemes

Recordem, abans de tot, uns conceptes

- Un procés és una aplicació d'usuari que executa a la màquina. El procés té assignat un espai virtual de memòria, pot utilitzar instruccions mode usuari i utilitza les crides a sistema operatiu per accedir als dispositius d'entrada-sortida.
- Un sistema és un entorn que inclou el sistema operatiu així com múltiples processos de forma simultània. Els processos comparteixen la memòria i els dispositius de la màquina. La ISA proveeix la interfície entre la màquina i el sistema.

Màquines virtuals: processos i sistemes

Definim el concepte de màquina virtual per a processos i màquines

- Una màquina virtual de procés és una plataforma virtual que executa un procés individual. La maquina virtual es crea en crear-se el procés i finalitza en finalitzar el procés. Aquesta màquina virtual es coneix amb el nom de *runtime software* o simplement *runtime*.
- Una màquina virtual de sistema és un entorn que té capacitat per suportar un sistema operatiu amb els seus múltiples processos. El programari que implementa la màquina virtual es coneix amb el nom de *virtual machine monitor*.

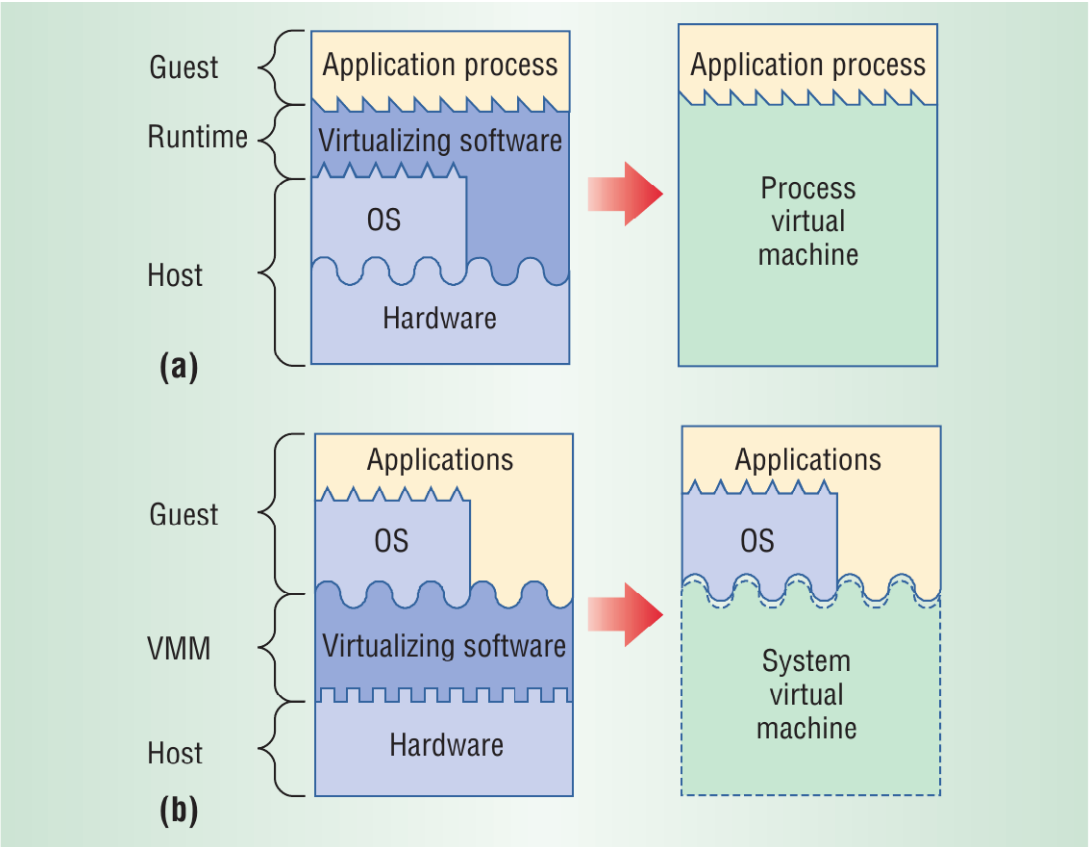
Màquines virtuals: processos i sistemes

Alguns conceptes més

- El procés o sistema que s'executa dintre d'una màquina virtual és el convidat (*guest*).
- La plataforma que permet que la màquina virtual funcioni és l'amfitrió (*host*).

Màquines virtuals: processos i sistemes

Esquema gràfic de màquines virtuals de procés, (a), i màquines virtuals de sistema (b).



Màquines virtuals de procés

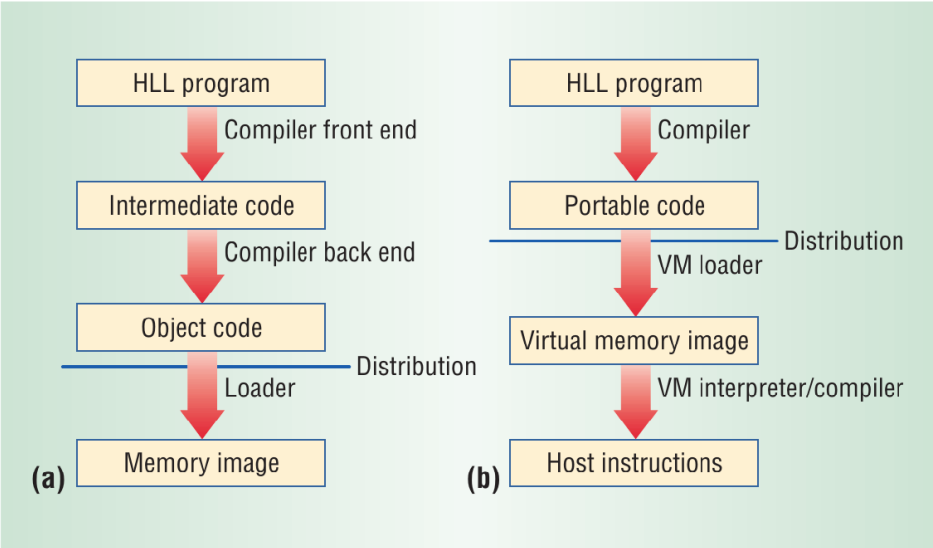
Hi ha diversos tipus de màquines virtuals de procés

- Sistemes multiprocés: a l'actualitat els sistemes operatius proveeix de la "il·lusió" que un procés cregui que té tota la màquina per ell mateix. Cada procés té el seu propi espai d'adreces, té els seus propis registres, i permet que els processos comparteixin els recursos. El sistema operatiu ofereix, en el fons, una màquina virtual a cada procés!
- Emuladors: permetre que es pugui executar codi executable compilats a amb un *set* d'instruccions diferent del que executa el *host*. Aquesta execució es pot fer mitjançant la interpretació (es tradueix mentre s'executa) de codi o la traducció binària dinàmica (es tradueix per blocs abans d'executar).

Màquines virtuals de procés

Altres tipus de màquines virtuals de procés

- Màquines virtuals de llenguatge d'alt nivell: una forma d'aconseguir compatibilitat entre diverses plataformes és dissenyar una màquina virtual amb un llenguatge d'alt nivell que no estigui associa a cap màquina real. Qualsevol procés de la màquina virtual es pot executar un cop s'implementa la màquina virtual al host. Per exemple: el llenguatge Java.



(a) Entorn en què es distribueix codi depenent de la plataforma, (b) Màquina virtual que depèn de la plataforma i que executa codi portable. Nota: HLL = High Level Language.

Màquines virtuals de sistema

Què és una maquina virtual de sistema?

- Una màquina virtual (*virtual machine*, VM) de sistema és un entorn en què un sistema operatiu executa múltiples processos.
- Un sistema amfitrió (*host*) pot executar de forma simultània múltiples sistemes operatius convidats (*guest*) que són independents entre sí.
- El Virtual Machine Monitor és qui controla l'execució del sistema operatiu convidat i té accés als recursos de la màquina.

Avantatges

- Permet aillar múltiples sistemes i usuaris entre sí. Si hi ha una fallada en un dels sistemes operatius convidats, els altres sistemes operatius així com el programari que s'hi executa no queda afectat.

Màquines virtuals de sistema

Quina és la història de les màquines virtuals?

- Els entorns van aparèixer a principis dels anys 70. Els ordinadors d'aquell moment, els *mainframes*, eren grans i cars. Eren compartits entre usuaris: cada usuari podia executar un sistema operatiu diferent.
- Amb l'aparició dels ordinadors de sobretaula l'interés en les màquines virtuals va disminuir.
- Avui en dia les màquines virtuals tornen a tenir gran popularitat: els *mainframes* han sigut substituïts per servidors o granges de servidors que utilitzen tot el món.

Màquines virtuals de sistema

A grans trets, s'aconsegueix executar un sistema operatiu convidat en mode usuari?

El sistema operatiu convidat executarà instruccions privilegiades: en fer-ho es produirà una excepció que captura el Virtual Machine Monitor. Aquest darrer executa l'operació en nom del sistema operatiu convidat.

El sistema operatiu convidat es desconeixedor de la feina que realitza el Virtual Machine Monitor "darrera de les càmeres".

Màquines virtuals de sistema

Quin tipus de màquines virtuals existeixen?

- El "tipus clàssic" és aquell en què el Virtual Machine Monitor (VMM) executa directament a sobre del maquinari i "fa" de sistema operatiu.
- Una alternativa, anomenada *hosted* VM, és aquella en què el VMM utilitza el sistema operatiu amfitrió: el VMM utilitza els drivers i serveis del sistema operatiu amfitrió per virtualitzar. L'avantatge és que es pot instal·lar com una aplicació més. Exemples: VMware.
- Una altra alternativa és aquella en què el maquinari és un gran multiprocessador de memòria compartida. L'objectiu és particionar el sistema en trossos més petits entre les diverses màquines virtuals que s'executen.

Hem acabat! Espero que us hagi agradat!