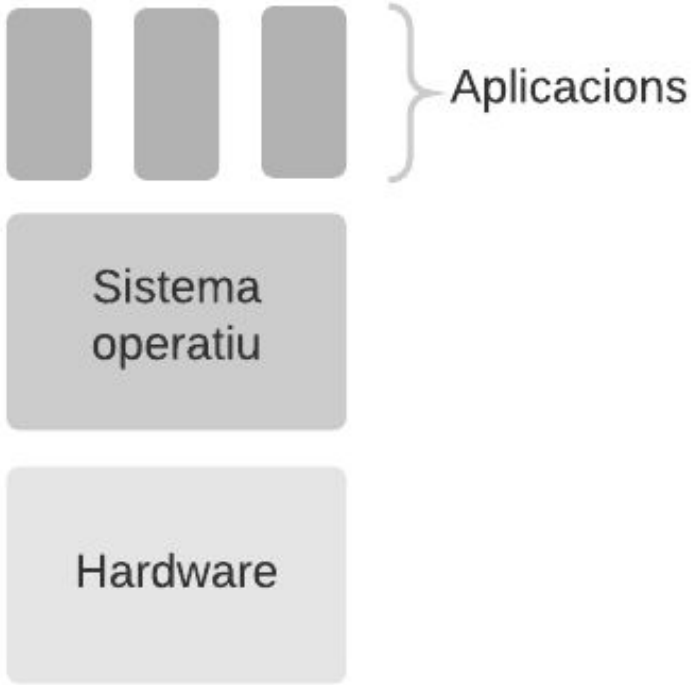
2.2. Virtualització

Yolanda Alemany Ruiz 2020-2021

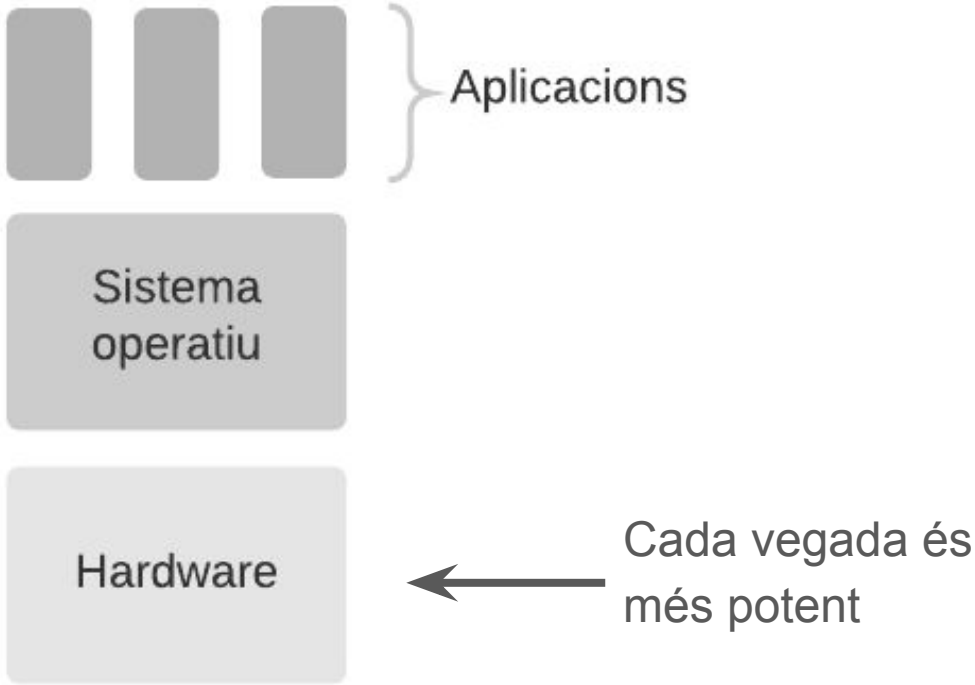
Introducció a la virtualització

Ja sabem que actualment un sistema informàtic es composa de la següent manera:



Introducció a la virtualització

Per mitjà de la virtualització, es volen aprofitar les màquines per fer la simulació de hardware i, sobretot, utilitzant diversos sistemes operatius virtuals en una mateixa màquina.



Introducció a la virtualització

- La virtualització permet aprofitar els recursos d'una màquina que no s'estan utilitzant.
- Per mitjà de la virtualització es volen aprofitar les màquines per fer la simulació de hardware i, sobretot, és possible **executar i tenir a una mateixa màquina diversos sistemes operatius** de manera virtual i simultània.

Introducció a la virtualització

Per què volem tenir a un mateixa màquina diferents sistemes operatius?

Introducció a la virtualització

Per què volem tenir a un mateixa màquina diferents sistemes operatius?

- **Educació**: volem un entorn segur en el que poguem fer proves sense por a "rompre" el sistema.
  - Si volem estudiar els virus informàtics i els executam dins una màquina virtual només afectarà en aquesta màquina.
- **Serveis**: si tens una màquina per cada servei, si es cau el servei, només afectarà en aquella màquina en concret. Seria poc eficient si tinguem màquines físiques.
- **Emulació de màquines** que poden tenir diferents arquitectures.

Introducció a la virtualització

- **Desenvolupament de software:** els desenvolupadors de software poden fer ús de la virtualització per escriure i provar programes. Pot ser complicat realitzar proves a un programa amb una fallada que faci que es penji tot el sistema, reiniciant a cada prova.

  Els desenvolupadors també poden utilitzar la virtualització per escriure programes que funcionin en un sistema operatiu diferent al que estan utilitzant.

- **Suport de sistemes antics**: un ús popular de la virtualització és l'emulació de hardware obsolet, especialment consoles antigues de videojocs.

Definició

La **virtualització** és una tecnologia que, a través de software, permet crear una versió virtual d'algun recurs tecnològic, com pot ser una plataforma de hardware, un sistema operatiu, un dispositiu d'emmagatzemament, etc.

Definició

- A partir de la virtualització **es poden utilitzar els recursos lliures d'una màquina física per executar diverses màquines virtuals.**
- Aquests recursos poden ser, per exemple, **el processador, la memòria, emmagatzemament i l'entrada/salida** que d'altra manera estarien lliures esperant feina.
- Permet utilitzar les màquines virtuals amb **independència del hardware**.
- El software encarregat de la virtualització crea una capa d'abstracció entre el hardware de la màquina física i el sistema de la màquina virtual.

Tipus de virtualització

Podem distingir 3 tipus de virtualitzacions:

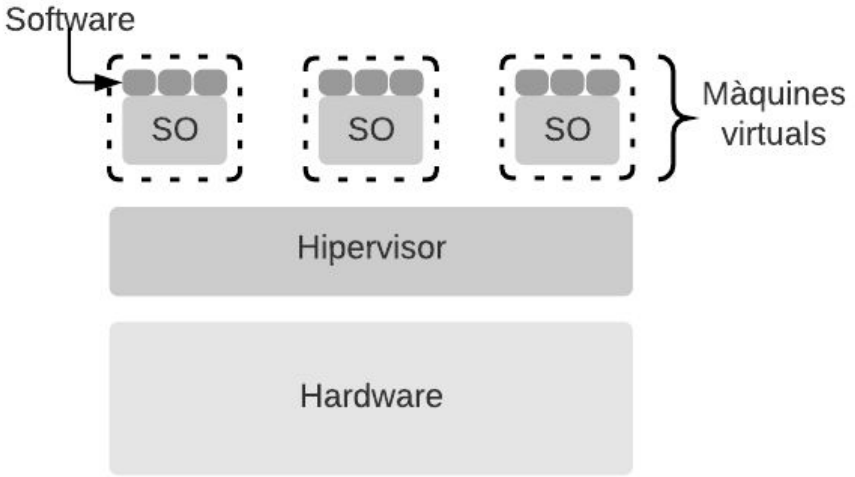
- Hipervisor
- Amfitrió/convidat (host/guest)
- Contenidors

Tipus de virtualització - Hipervisor

També anomenat **hipervisor tipus 1**.

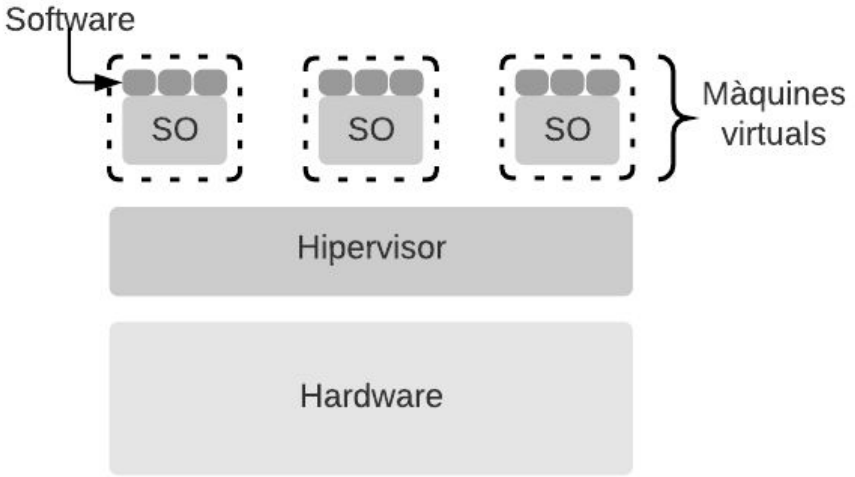
L'**hipervisor** és una capa de software que hi ha entre el hardware y els sistemes operatius huèsped, que són els que s'executen sobre l'hipervisor.

Cada sistema operatiu executa aplicacions de manera independent.



Tipus de virtualització - Hipervisor

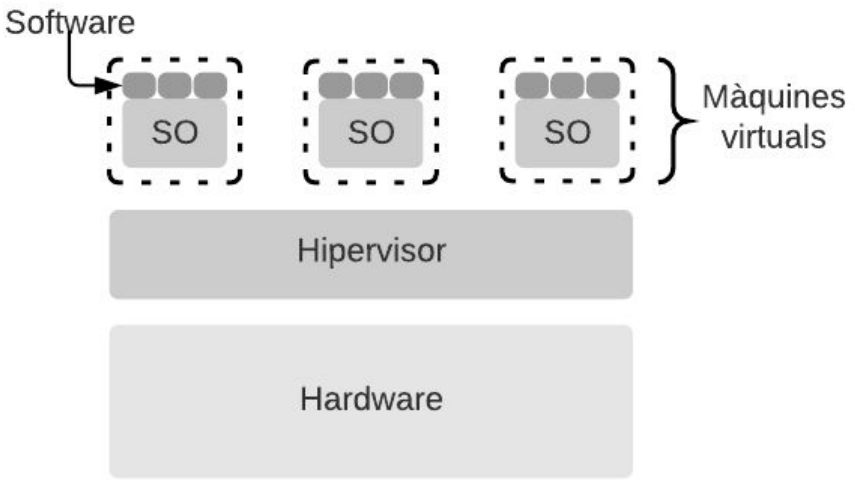
Per crear la il·lusió de què cada sistema operatiu tingui accés exclusiu al hardware, l'**hipervisor** (també anomenat **monitor de màquina virtual - VMM**) presenta al sistema operatiu huèsped una simulació creada pel software d'un ordinador idealitzat. Aquestes simulacions són anomenades **màquines virtuals**.



Tipus de virtualització - Hipervisor

En resum:

1) L'hipervisor executa múltiples màquines virtuals
2) Cada màquina virtual alberga un sistema operatiu
3) Cada sistema operatiu executa múltiples aplicacions.
4) L'hipervisor administra l'accés de les diferents màquines virtuals als recursos reals del hardware del sistema.



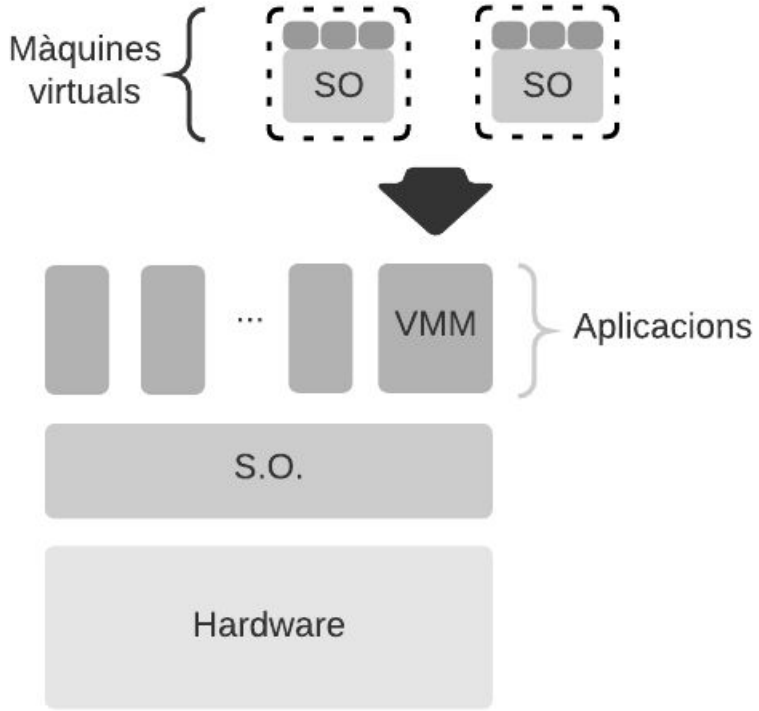
Tipus de virtualització - Amfitrió/huèsped

També anomenat **hipervisor tipus 2**.

En la virtualització amfitrió/huèsped les màquines virtuals s'executen sobre el sistema operatiu amfitrió.

Això és degut a què el VMM s'executa com una aplicació més. I aquest software alberga les màquines virtuals.

Les màquines virtuals allotgen els sistemes operatius huèsped.



Tipus de virtualització - Comparació

La virtualització d'**amfitrió/huèsped és més lent** que el d'hipervisor ja que hi ha molts de software entre el sistema operatiu huèsped i el hardware real del sistema.

La virtualització d'**amfitrió/huèsped és més còmode** degut a què aquestes virtualitzacions es poden instal·lar i executar-se com qualsevol altra aplicació, sense necessitat de reiniciar.

La virtualització d'**hipervisor és més segura**, si falla algun dels sistemes els altres poden funcionar. Mentre que en el cas de l'**amfitrió/huèsped** si falla el sistema operatiu amfitrió, conseqüentment fallen totes les màquines virtuals.

Tipus de virtualització - Exemples

Exemples d'Hipervisor tipus 1:

- Linux KVM
- Proxmox VE
- Citrix XenServer
- Oracle VM Server para x86

Exemples d'Hipervisor tipus 2:

- VirtualBox
- VMware
- Microsoft Virtual PC

VirtualBox

vmware

Termes

A continuació, es mostren els termes utilitzats a la virtualització:

- La màquina sobre la qual es virtualitza s'anomena **amfitrió**, més conegut en anglès, **host**.
- El software encarregat de la virtualització s'anomena ***software amfitrió o host software.***
- Es simula un entorn computacional anomenat **màquina virtual**.
- El software del entorn s'anomena **huèsped**, en anglès, **guest**. Sol ser un sistema operatiu i s'executa com si estigués instal·lat a una plataforma de hardware autònoma.

Tipus de virtualització segons què s'està virtualitzant

Hi ha una altra classificació de la virtualització segons les característiques de la virtualització:

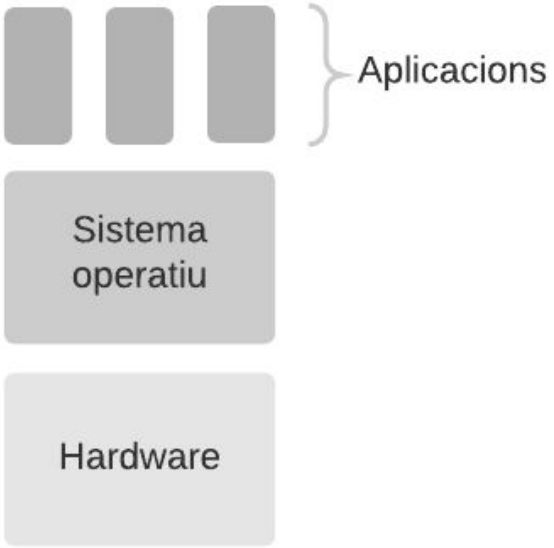
- Virtualització clàssica
- Emulació
- Paravirtualització

Anam a introduir un mecanisme dels sistemes lligat a la virtualització que necessitarem per explicar aquesta classificació.

Anells de privilegis

Per ara hem vist que es separen per nivells les tasques que han de fer els diferents components del sistema (hardware, SO i aplicacions).

Aquesta manera d'explicar les coses es bastant introductori perquè… realment no funciona exactament així. Aquesta abstracció sòl ser modificada per dues raons: velocitat i seguretat.



Anells de privilegis

Imaginau que el sistema operatiu hagués de controlar tota la seguretat del sistema, les aplicacions haurien de sol·licitar sempre les execucions al sistema operatiu i aquest d'acceptar les sol·licituds o no, fent un anàlisis del que volem realitzar. Aquest fet suposaria un alentiment del sistema.

Per evitar l'alentiment del sistema i que les aplicacions accedesquin a qualsevol part privilegiada, els processadors ofereixen un mecanisme que permet a diferents programes executar-se amb diferents *nivells de privilegi*. En aquests nivells se'ls hi anomena *anells de privilegi*.

Anells de privilegis

Els **anells de privilegi** són un mecanisme que té l'objectiu de protegir l'accés a dades, millorar la tolerància a les fallades i protegir el sistema davant comportaments maliciosos.

Els programes es classifiquen en nivells: 3, 2, 1 i 0. Generalment, la majoria de sistemes operatius utilitzen només dos nivells: 3 i 0.

Anells de privilegis

Els programes que s'executen als anells més alts tenen restriccions sobre quines parts del sistema no es poden tocar. És més difícil que els programes de baix nivell de privilegis (anell 3) puguin fer danys al sistema (per exemple, sobreescriure dades d'accés d'usuaris).

Una fallada accidental o maliciosa en un programa d'anell 0 (on normalmente el kernel del sistema operatiu té accés exclusiu) pot tenir conseqüències catastròfiques.

Anells de privilegis

Situació 1: Un programa d'anell 3 sol·licita accés que entra en els seus privilegis.

1) Sol·licitud del programa al processador
2) El sistema operatiu administra el procés i l'envia al processador.
3) El processador comprova si el programa té l'accés corresponent i respon amb la informació sol·licitada.

Anells de privilegis

Situació 2: Un programa d'anell 3 sol·licita accés que entra no en els seus privilegis. Per exemple, és de nivell 3 i sol·licita un accés corresponent al nivell 0.

1) Sol·licitud del programa al processador.
2) El sistema operatiu administra el procés i l'envia al processador.
3) El processador comprova si el programa té l'accés corresponent. Veu que no té accés i manda al sistema operatiu "matar" al programa corresponent. Aquesta acció s'anomena *fault*.
4) El sistema operatiu mata el programa.

Anells de privilegis

Què té tot això que veure amb la virtualització?

Anam a analitzar l'abstracció de virtualització d'amfitrió/huèsped (hipervisor tipus 2) tenint en compte l'aspecte dels anells de privilegis.

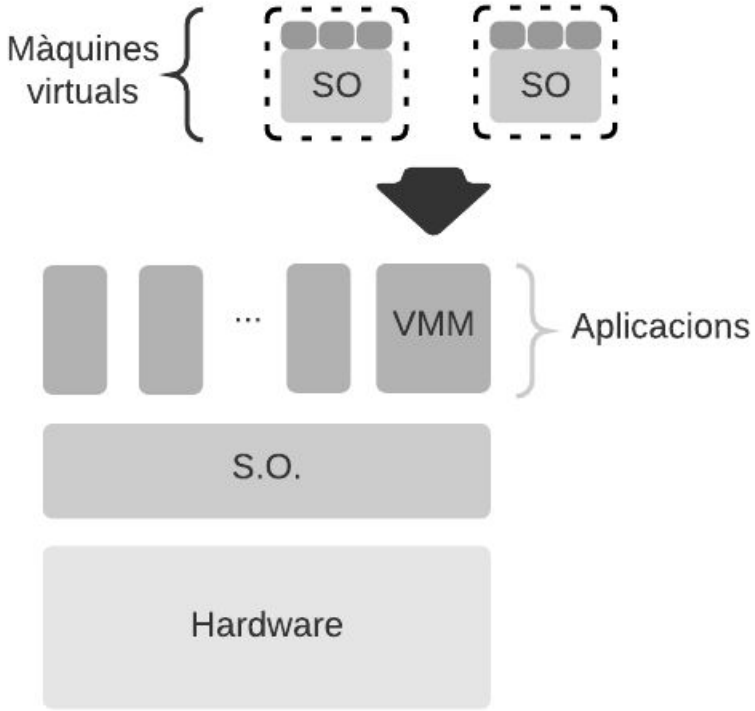
Anells de privilegis i virtualització

Un programa de la màquina virtual sol·licita accés de nivell 0, la sol·licitud arribarà a les diferents parts:

Software -> SO huèsped -> VMM -> SO -> HW

I com hem dit, el hardware comprovarà que no té accés i sol·licitarà matar el programa.

En aquest cas, es matarà el VMM!



Virtualització clàssica

La **virtualització clàssica** consisteix en que el sistema operatiu huèsped no ha de saber que és virtual i ha de seguir pensant que pot tenir privilegis de nivell 0.

Per tant, hi ha diferents maneres de sol·lucionar el problema dels privilegis degut a aquesta virtualització.

Una d'elles és la de *captura-i-emula.*

Virtualització clàssica

Captura-i-emula

En aquest cas, en lloc de matar el programa directament, es dona un avís a l'hipervisor. En aquest moment, l'hipervisor pren el control del processador per poder emular l'execució de les instruccions. Capturant les instruccions que requereixen privilegis d'anell 0 i executant-les de manera emulada.

D'aquesta manera, l'hipervisor pot evitar que el sistema operatiu huèsped detecti que s'està executant en un anell diferent al 0.

Virtualització clàssica - Instruccions de virtualització

Els sistemes operatius moderns ja no poden virtualitzar si no activam les **instruccions de virtualització**. Aquestes es poden habilitar o deshabilitar a través de la BIOS del sistema.

Aquestes instruccions s'anomenen VT-x a processadors Intel i AMD-V a processadors AMD.

Les instrucccions de virtualització permeten executar màquines virtuals en virtualització clàssica sense cap tipus de modificació.

Paravirtualització

Degut a que la virtualització clàssica requereix que el VMM capturi i emuli un gran nombre d'instruccions problemàtiques comunes, els sistemes operatius huèsped i el seu software poden executar-se més lentament del que ho farien nativament.

Una solució és la tècnica anomenada **paravirtualització**. En aquets casos, el sistema operatiu sap que és virtual i es modifica perquè no suposi cap problema posteriorment. Per tant, el VMM pot confiar en el sistema operatiu huèsped.

Paravirtualització

La distribució del sistema operatiu huèsped ha de suportar la paravirtualització.

El principal inconvenient de la paravirtualització és que el sistema operatiu huèsped ha de ser modificat per permetre l'ús de d'aquesta tècnica. Encara que les modificacions solen ser mínimes, es requereix l'**accés al codi font del sistema operatiu**. Per aquesta raó, Linnux és el sistema operatiu paravirtualitzat més popular.

Emulació

El VMM presenta a cada sistema operatiu huèsped un model software del sistema emulat complet, incloent el processador.

Totes les instruccions executades pel sistema operatiu huèsped i les seves aplicacions deuen ser passades al VMM antes de passar al processador perquè puguin ser traduïdes al joc d'instruccions natiu del processador i executades.

Incloent les parts del sistema operatiu que precissen interfície amb el hardware.

Emulació

L’emulació és el tipus de virtualització que **col·loca una major quantitat de software entre el hardware i el sistema operatiu huèsped**, i per això mateix pot ser el més lent dels tres tipus.