Redes e Segurança

Universidade de Mogi das Cruzes (UMC)

Parte 1:
Sistemas de Virtualização

Origem da **Virtualização**

- Surgimento em meados da década de 60
- Grandes computadores ficam mais velozes ao processar dados.
  - Ineficientes em aproveitar o tempo de cálculo.
  - Motivo: gerenciamento manual de processos por um operador (humano)
- Surge o conceito de tempo compartilhado (Time Sharing)

Origem da **Virtualização**

- Robert P. Goldberg (1972)
  - Dissertação na Universidade de Harvard
  - Bases teóricas da arquitetura para sistemas computacionais virtuais

Origem da **Virtualização**

- IBM
  - Lança um mainframe capaz de executar de forma simultânea diferentes SOs
    - Sob a supervisão de um controlador
    - Controlador = Hypervisor

O que é um **Mainframe**?

Um computador de alto desempenho usado para fins de computação em grande escala que exige mais disponibilidade e segurança do que uma máquina de menor escala pode oferecer.

Um mainframe possui recursos redundantes que permitem oferecer 99,99% de disponibilidade.

Motivação para a **Virtualização**

- Organizar vários servidores virtuais em um conjunto reduzido de servidores físicos.
- Consolidação de aplicações
- Ambiente de teste e homologação de sistemas
- Execução de diferentes SOs
- Provisionamento de servidores
- Recuperação de desastres
- Migração de sistemas

Motivação para a **Virtualização**

- Diminuir custos com TI
- Diminuir custos com energia
- Diminuir lixo tecnológico
- Flexibilidade e agilidade para criar ambientes
- Administrar e gerenciar melhor os ambientes de teste e produção

Benefícios da Virtualização

- **Instalações:** espaço, resfriamento, energia
- **Hardware:** servidores, switches, roteadores, armazenamento
- **Software:** suporte, licenças, manutenção
- **Administração de servidores:** servidores, sites, dados, softwares, aplicações

Princípios de **Virtualização**

- Capacidade de se executar simultaneamente mais de um sistema operacional em um único servidor físico.

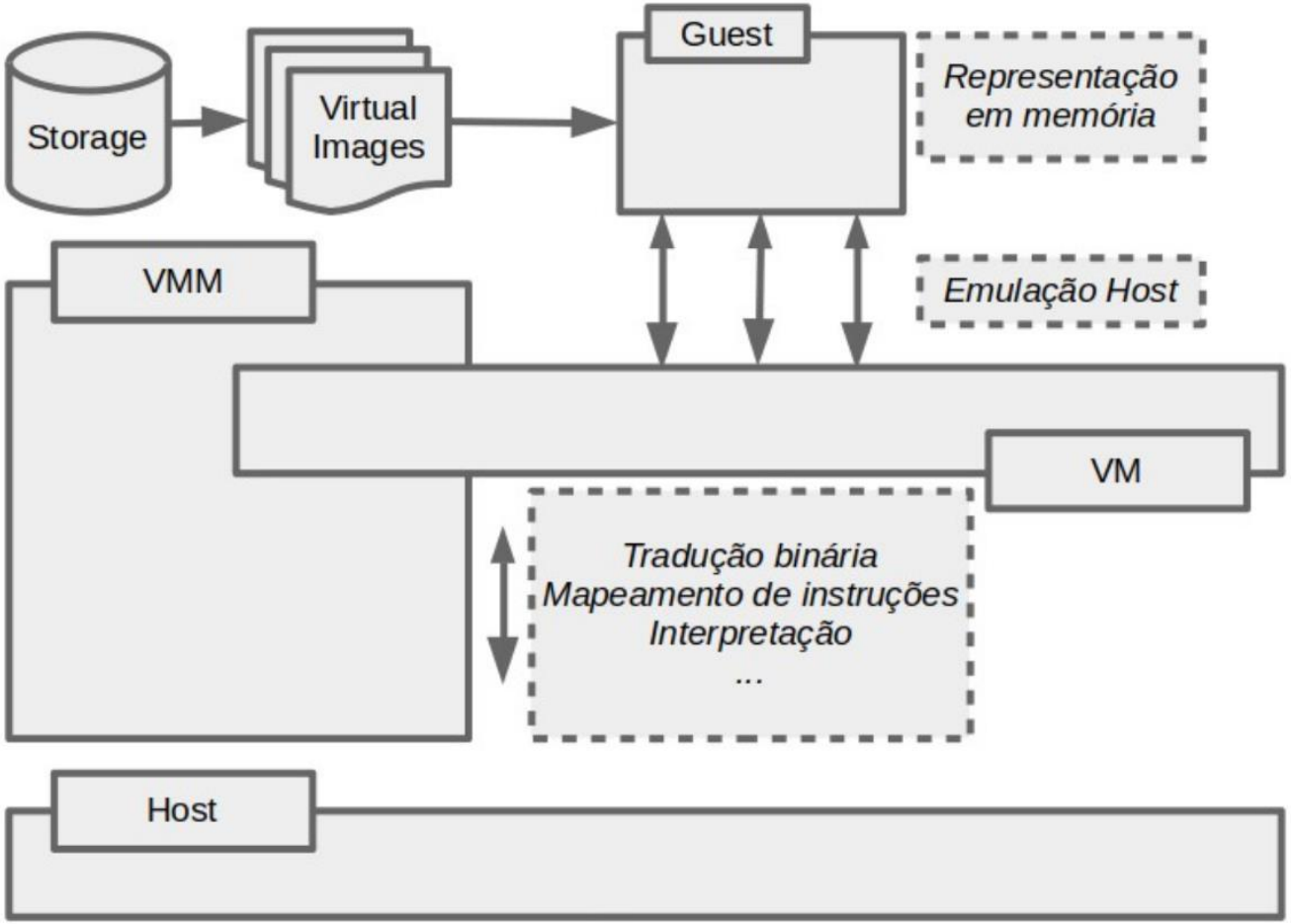
Princípios de **Virtualização**

- Pode ocorrer em diferentes níveis:
  - Nível de linguagem de programação
  - Nível de biblioteca
  - Nível de S.O
  - Nível de abstração de hardware
  - Nível de conjunto de instruções

Virtualização por **Hardware**

- Método de virtualização mais comum
- Modelo de virtualização que fornece um ambiente de execução abstrato, em termos de hardware de computador
- SO convidado (guest) pode ser executado.

VIRTUALIZAÇÃO DE HARDWARE



Nesse modelo, o convidado (guest) é representado pelo sistema operacional, o sistema operacional hospedeiro (host) pelo computador físico hardware, a máquina virtual por sua emulação (VM) e o gerenciador de máquina virtual (VMM) pelo hypervisor.

O que é um **Hypervisor**?

- O hypervisor, também chamado de monitor de máquina virtual (ou VMM, do inglês Virtual Machine Monitor), permite que várias VMs sejam executadas simultaneamente em um mesmo host.

O que é um **Hypervisor**?

- Ele oferece uma plataforma em que VMs podem ser iniciadas, gerenciadas, executadas e finalizadas isoladamente umas das outras e do host.

O que é um **Hypervisor**?

- O hypervisor geralmente é um programa, ou uma combinação de software e hardware, que permite a abstração do hardware físico subjacente, interceptando uma variedade de instruções sensíveis entre a VM e o hardware do host.

O que é um **Hypervisor**?

- Esse tipo de virtualização também é conhecida como virtualização do sistema, pois fornece a arquitetura do conjunto de instruções (ou ISA) para VMs, que define o conjunto de instruções para o processador, registros, memória e gerenciamento de interrupção.

O que é um **Hypervisor**?

- Sendo uma interface entre hardware e software, a ISA é importante para o desenvolvimento do SO (componente denominado System ISA) e de aplicativos que gerenciam diretamente o hardware subjacente (componente denominado User ISA).

O que é um **Hypervisor**?

- Sendo uma interface entre hardware e software, a ISA é importante para o desenvolvimento do SO (componente denominado System ISA) e de aplicativos que gerenciam diretamente o hardware subjacente (componente denominado User ISA).

Módulos do Hypervisor

- É composto por três módulos principais, despachante (dispatcher), alocador (allocator) e interpretador (interpreter).

Módulos do Hypervisor

- O dispatcher tem como função redirecionar as instruções emitidas pela instância de uma VM para um dos dois outros módulos.

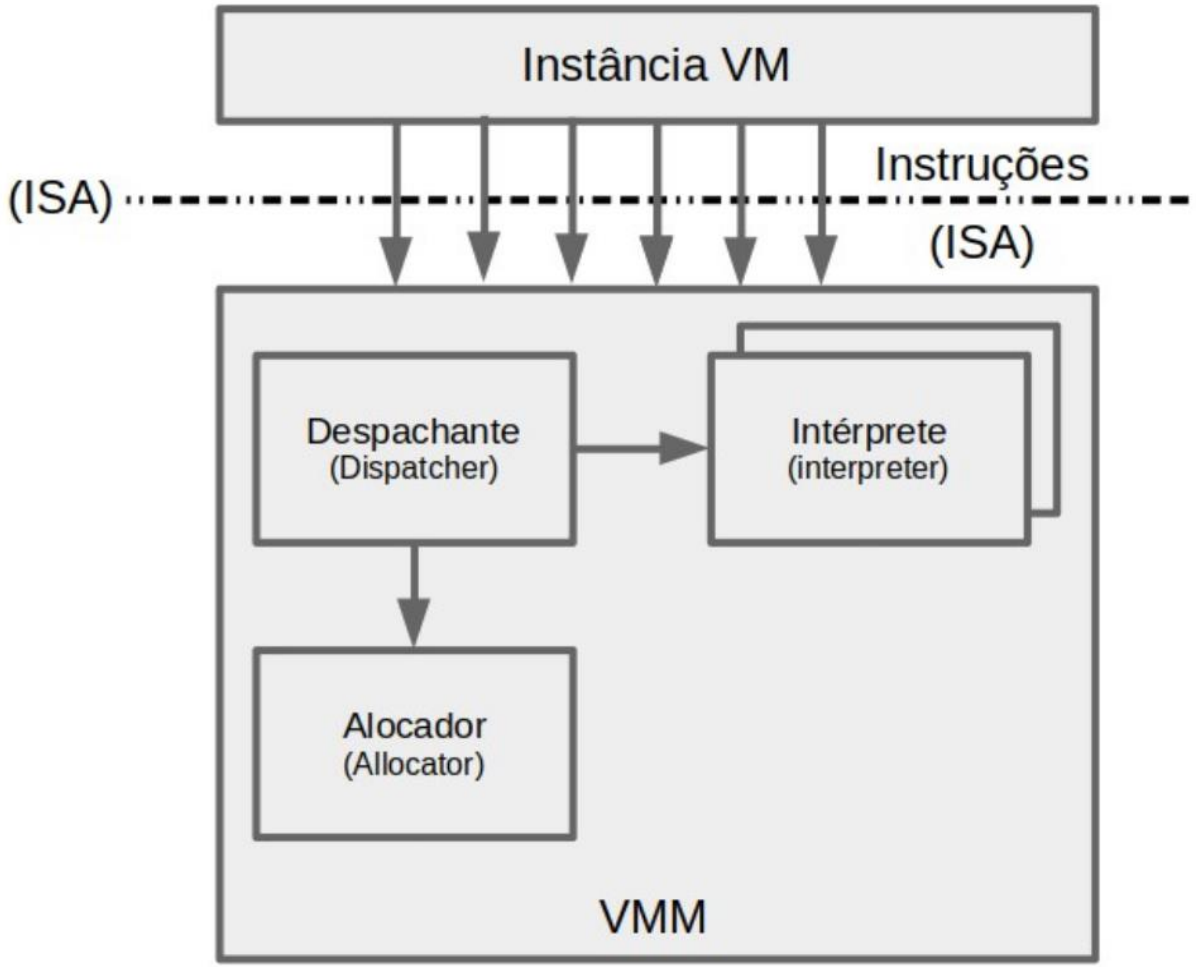
Módulos do Hypervisor

- O allocator é iniciado pelo dispatcher e executado quando uma VM tenta executar uma instrução que resulta na alteração dos recursos da máquina associados a essa VM, sendo responsável por decidir os recursos do sistema a serem fornecidos à VM.

Módulos do Hypervisor

- O interpreter é composto por rotinas de interpretação que são executadas sempre que uma VM realiza uma instrução privilegiada

ARQUITETURA HYPERVISOR



Organização interna do gerenciador de máquina virtual (VMM) apresentando seus três módulos principais: despachante (dispatcher), alocador (allocator) e intérprete (interpreter), responsáveis por coordenar suas atividades para emular o hardware subjacente.

Problemas da Virtualização por Hardware

- Necessidade de isolamento de diferentes ambientes virtuais, garantindo que o compartilhamento de recursos físicos do host não permita que dois ambientes guest virtualizados interfiram um no outro

Problemas da Virtualização por Hardware

- Definir como instruções privilegiadas serão executadas por um sistema hóspede, já que essas instruções, por questões de segurança, são restritas ao sistema hospedeiro.

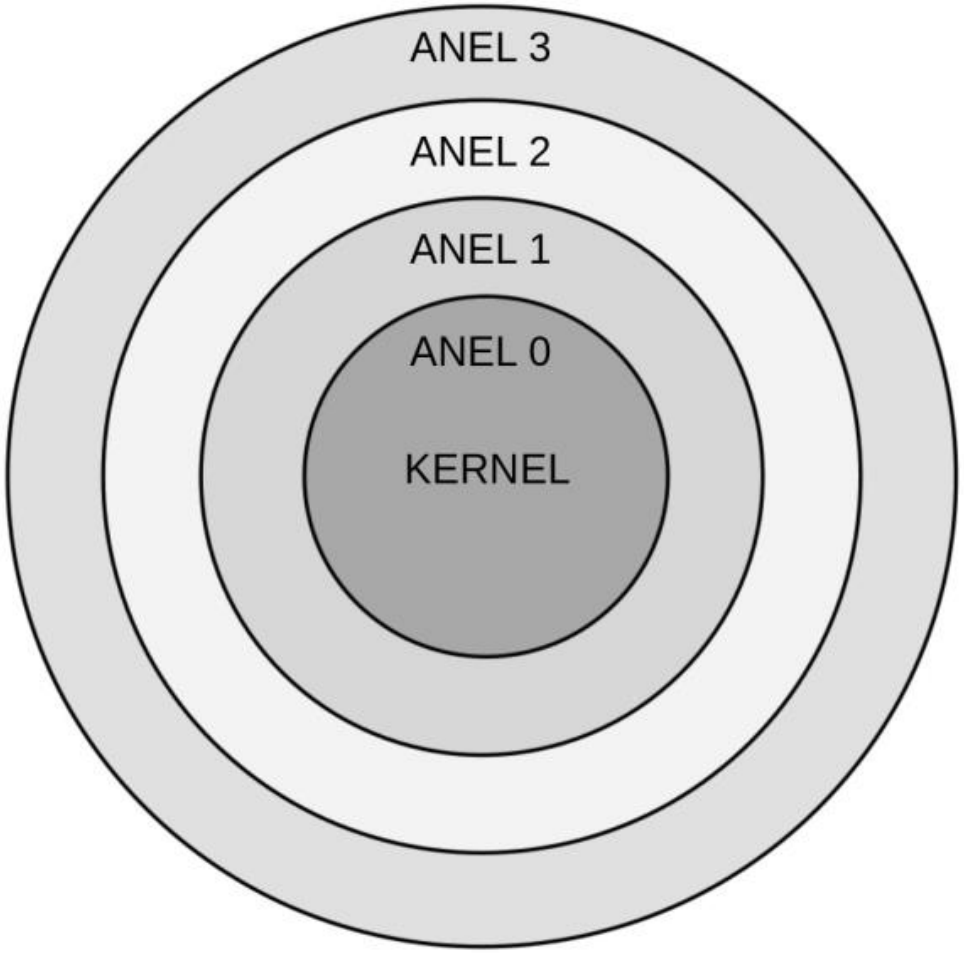
Problemas da Virtualização por Hardware

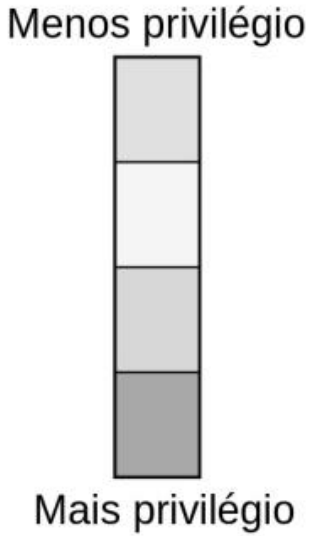
- As instruções privilegiadas são aquelas executadas sob restrições específicas e utilizadas principalmente para operações confidenciais, que expõem (sensível ao comportamento) ou modificam (sensível ao controle) o estado privilegiado.

Problemas da Virtualização por Hardware

- Diferentes implementações podem ser encontradas, sendo que um exemplo de hierarquia de privilégios de segurança baseada em Anéis.

ANÉIS DE SEGURANÇA





Hierarquia de privilégios de segurança baseada em anéis, na qual o Anel 0 corresponde o nível com maior privilégio, o Anel 3 apresenta o nível com menor privilégio e os Anéis 1 e 2 apresentam um nível de privilégios intermediários.

Problemas da Virtualização por Hardware

- Buscando tratar esse tipo de problema relacionado aos privilégios de instruções, diferentes técnicas de virtualização por hardware foram desenvolvidas ao longo do tempo.

Virtualização **Completa**

- Capacidade de executar um programa diretamente em uma VM, sem qualquer modificação, como se fosse executado em um hardware físico.

Virtualização
Completa

- VMMs fornecem uma emulação completa de todo o hardware subjacente, disponibilizando um isolamento pleno, que leva a segurança aprimorada, facilidade de emulação de diferentes arquiteturas e coexistência de diferentes sistemas na mesma plataforma

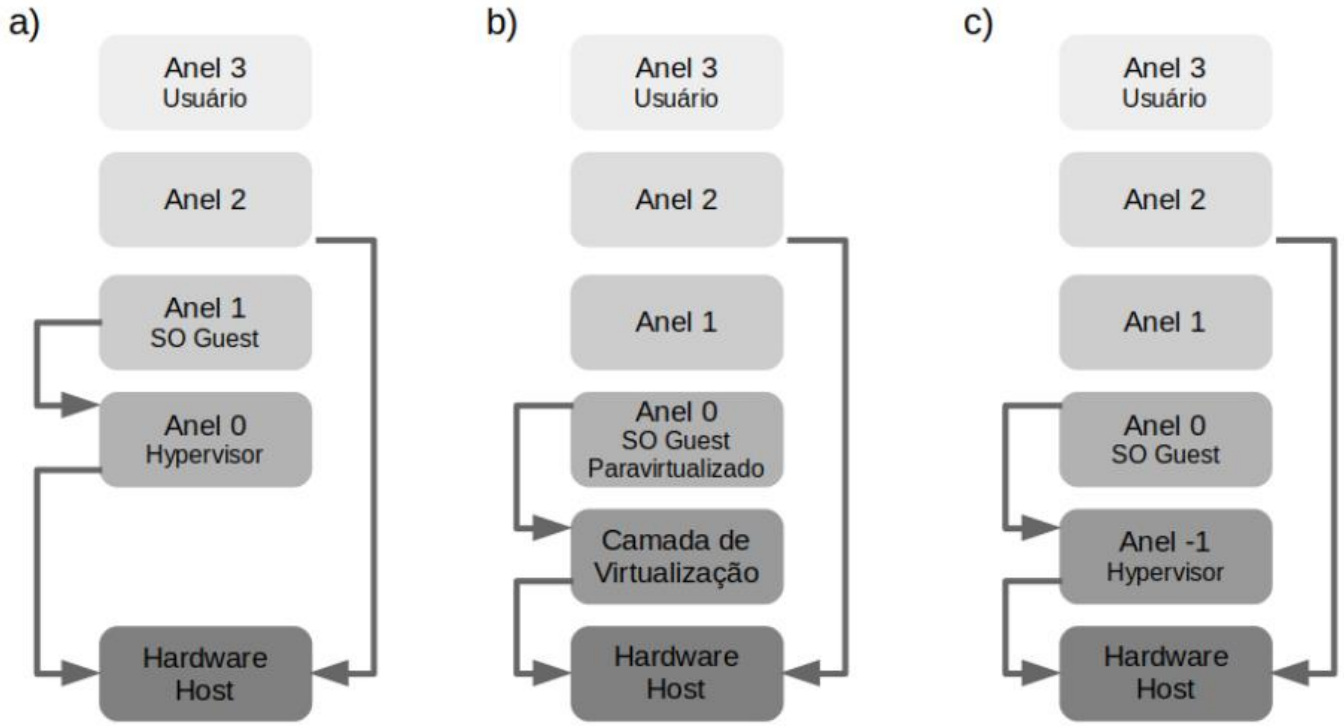
Virtualização **assistida por hardware**

- Fornece um modo de privilégio adicional abaixo do Anel 0 em que o hypervisor pode operar, deixando o Anel 0 disponível para SOs hospedeiro.

Virtualização **parcial**

- Fornece uma emulação parcial do hardware, não permitindo a execução completa do SO guest em isolamento total.

TÉCNICAS DE VIRTUALIZAÇÃO



(a) Virtualização completa;
(b) Paravirtualização;
(c) Virtualização assistida por hardware.

Tipos de virtualização baseadas em hypervisor

- Fornece uma emulação parcial do hardware, não permitindo a execução completa do SO guest em isolamento total.
- Baseados na localização onde o VMM está sendo executado

Hypervisor
Tipo 1

- Pequeno conjunto de softwares necessários para a virtualização responsável pelo gerenciamento de recursos e acesso aos dispositivos de I/O entre máquinas virtuais e o hardware.

Hypervisor
Tipo 1

- Esse tipo de hypervisor toma o lugar do SO e interage diretamente com a interface ISA exposta pelo hardware subjacente, que emula a interface para permitir o gerenciamento de SOs.

Hypervisor
Tipo 1

- Ele também é chamado de máquina virtual nativa, já que é executado nativamente pelo hardware.
- O hypervisor tipo 1 fornece melhor desempenho, segurança e disponibilidade do que o hypervisor tipo 2.

Hypervisor
Tipo 1

- Exemplos de hypervisores de tipo 1 são Xen, KVM, VMWare ESX, Microsoft Hyper-V, Citrix Xen Server, Proxmox e oVirt.

Hypervisor
Tipo 2

- Utiliza o SO host subjacente para suas funções.
- Isso significa que es- ses hypervisores são programas gerenciados pelo SO, que interagem com ele e emulam o ISA do hardware virtual para SOs guest.

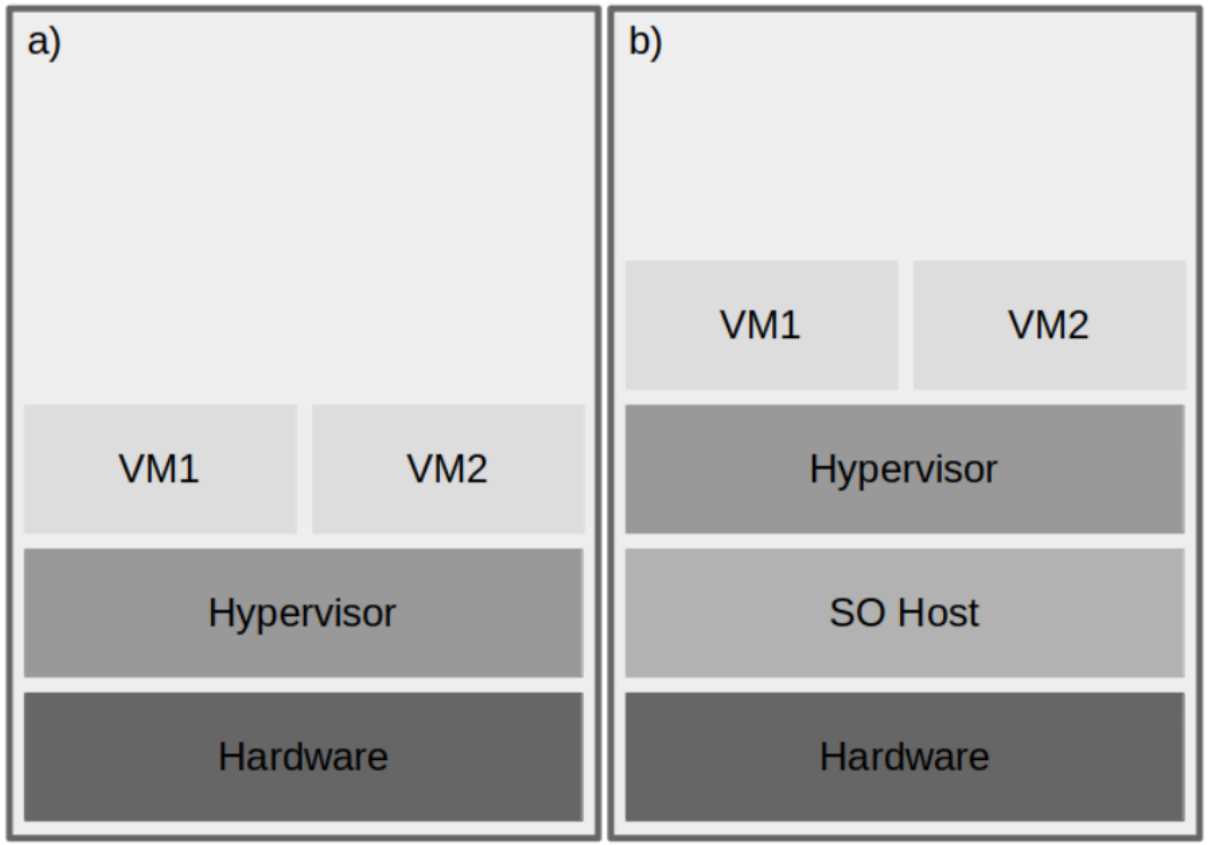
Hypervisor
Tipo 2

- É frequentemente usado em sistemas que requerem suporte para diversos dispositivos de I/O.
- Esse tipo de hypervisor também é chamado de máquina virtual hospedada, pois é hospedado em um SO.

Hypervisor
Tipo 2

- Exemplos de hypervisores do tipo 2 são o QEMU, VMWare Workstation, Microsoft Virtual PC, VMWare Player e o Oracle VM Virtualbox.

TIPOS DE VIRTUALIZAÇÃO HYPERVISOR



Representação dos dois tipos de virtualizações baseadas em hypervisor, sendo (a) hypervisor nativo (tipo 1) executado diretamente sobre o hardware e (b) hypervisor hospedado (tipo 2) executado no sistema operacional do host.

VIRTUALBOX

VirtualBox

- Site: www.virtualbox.org
- Multiplataforma (Windows, MacOS e Linux)
- Mantido pela Oracle
- Fácil de utilizar e instalar
- Gratuito

VirtualBox

- Hypervisor tipo II
- Código aberto (open-source)
- Suporta a criação e gerenciamento de VMs host (Windows, Linux, BSD, MacOS)
- Fornece um pacote de device drivers denominado "Guest Additions" para melhorar o desempenho.

VirtualBox

- Hypervisor tipo II
- Código aberto (open-source)
- Suporta a criacao e gerenciamento de VMs hospedes (Windows, Linux, BSD, MacOS)
- Fornece um pacote de device drivers denominado "Guest Additions" para melhorar o desempenho.

Fim do Módulo