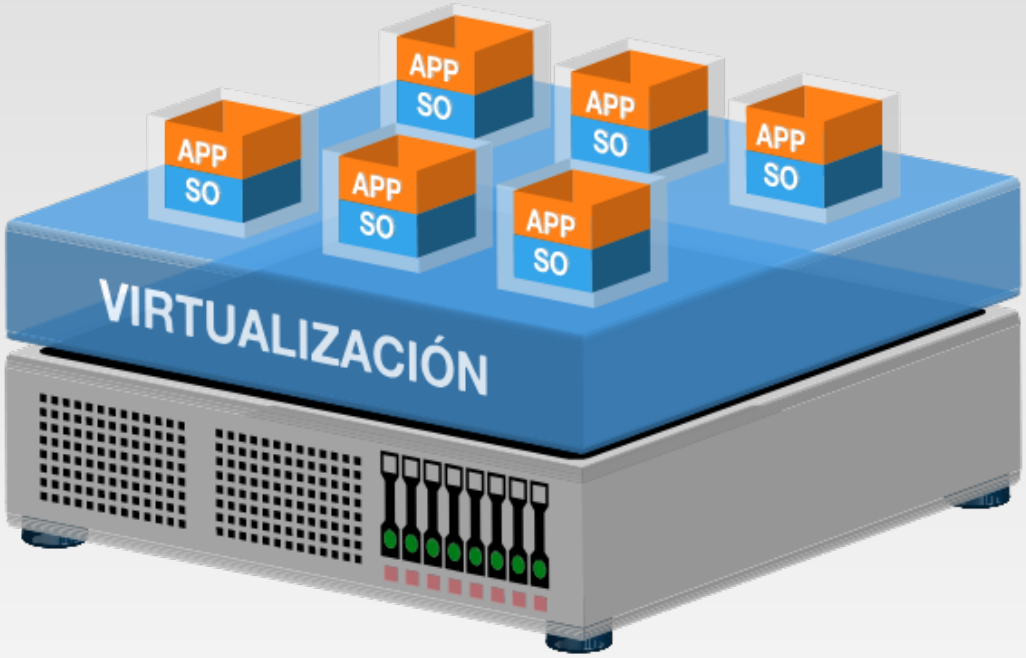
**Pontificia Universidad Católica de Chile**
**Escuela de Ingeniería**
**Departamento de Ciencia de la Computación**

Virtualización

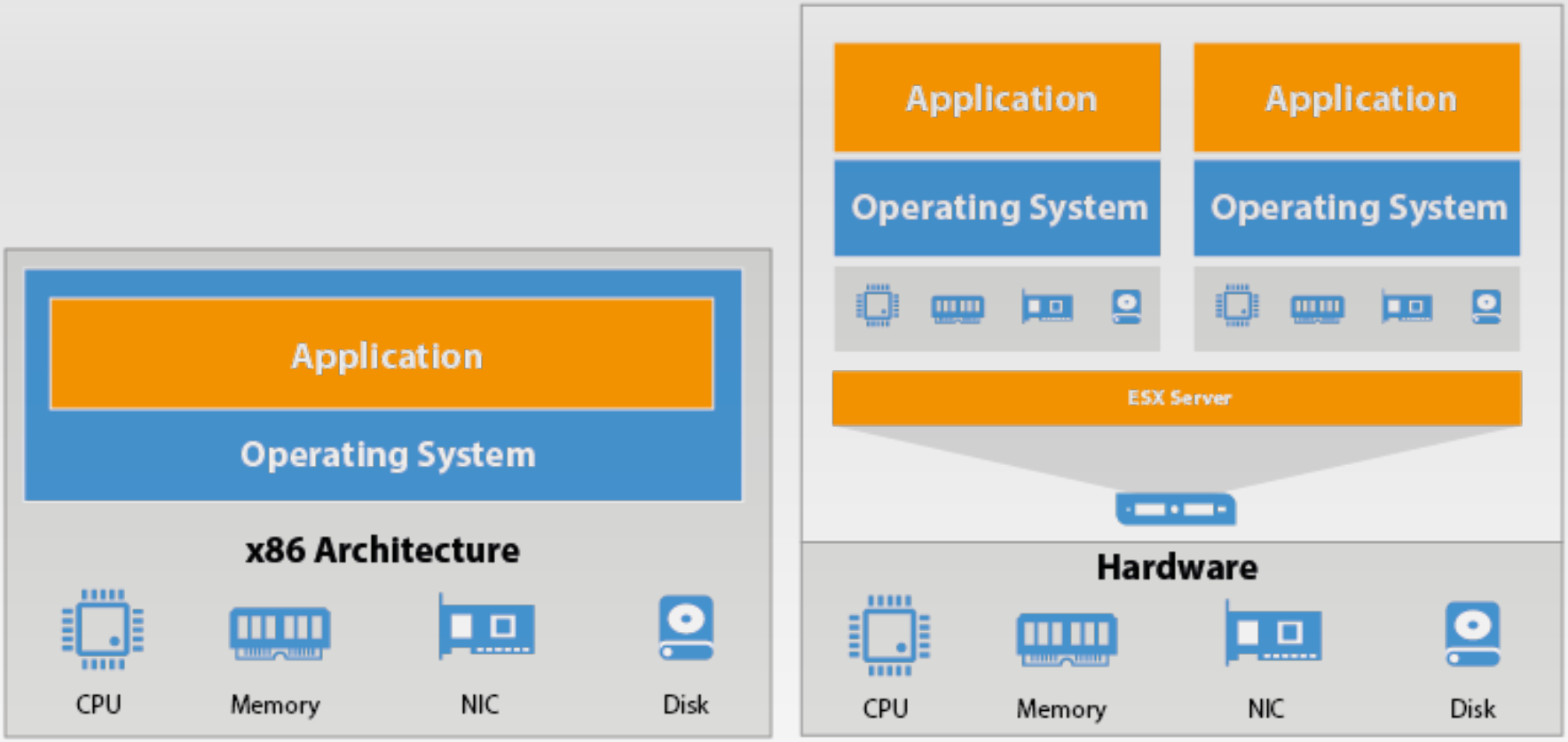
# Sistemas distribuidos

Gabriel Vidal Salazar

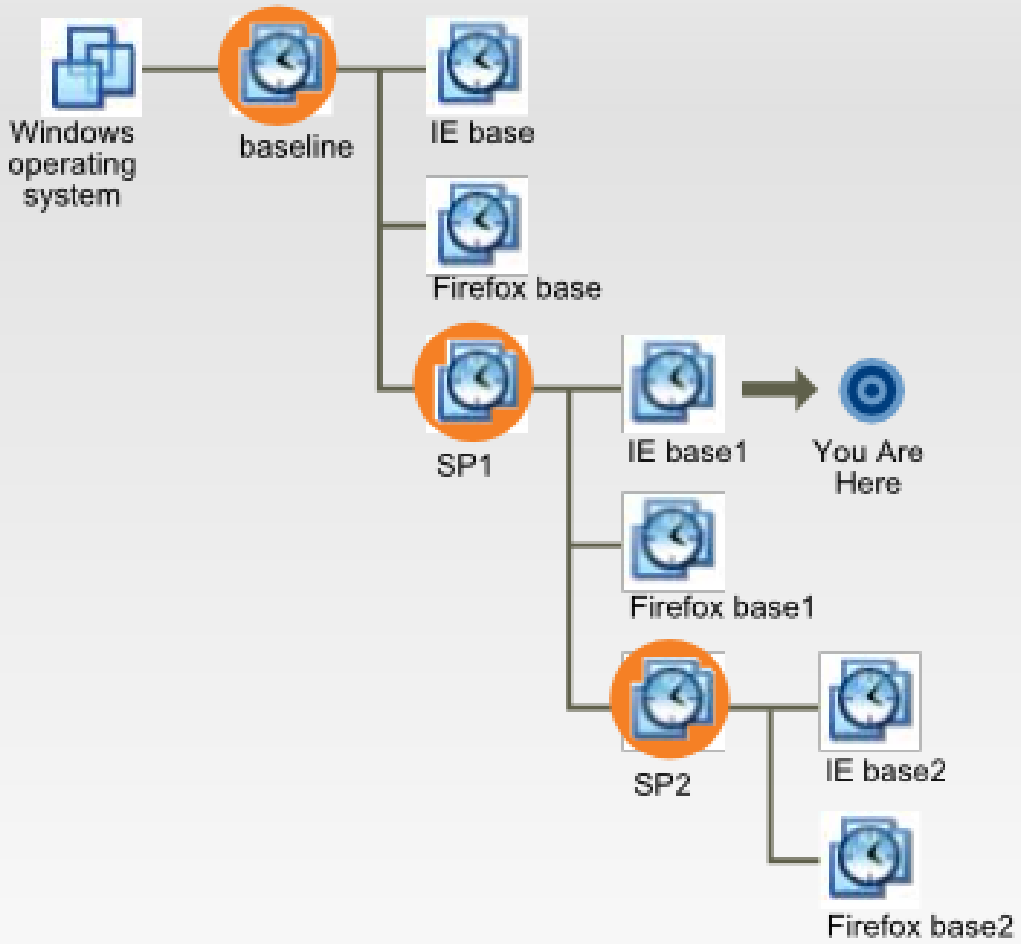
# ¿Qué conocen de virtualización?



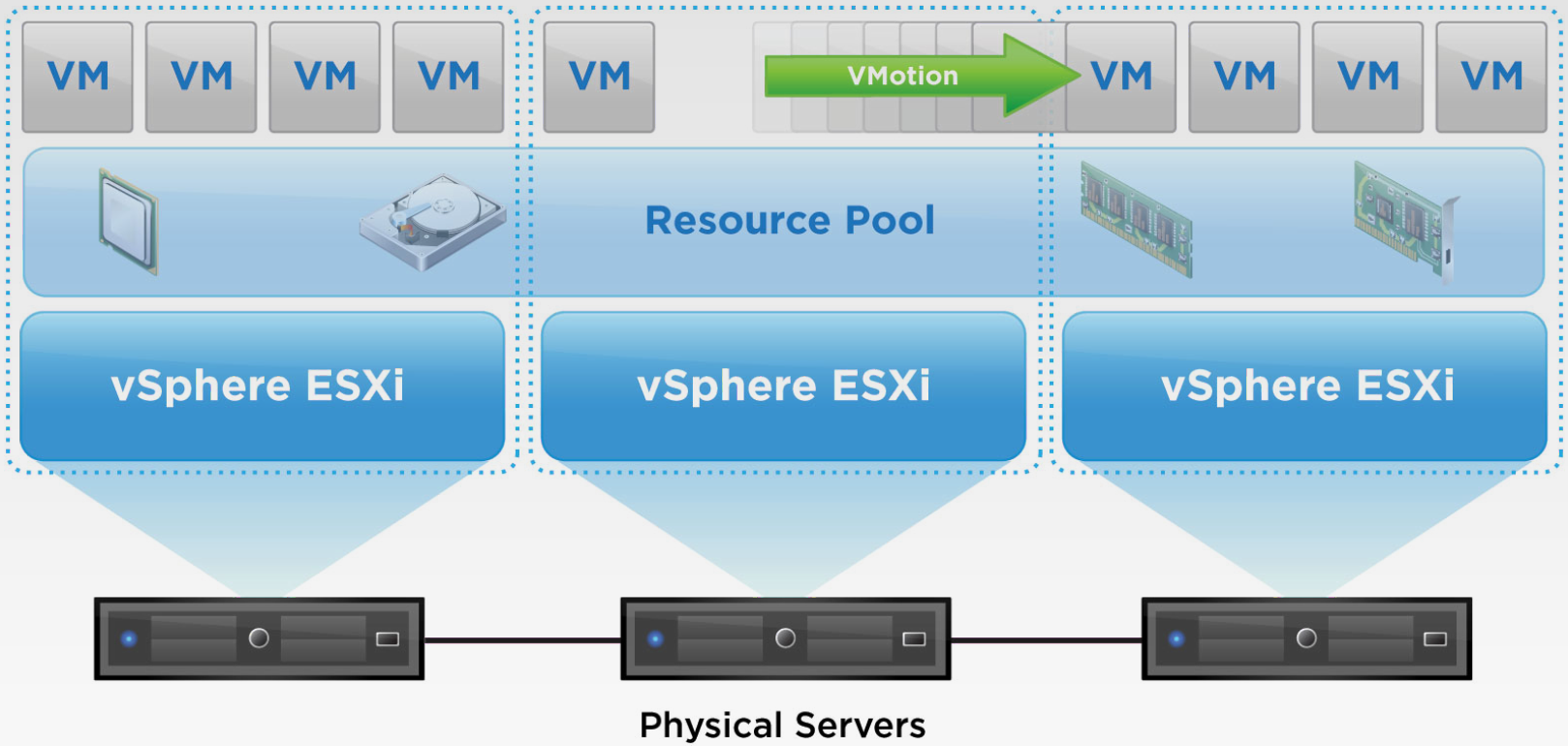

Source: Openclipart



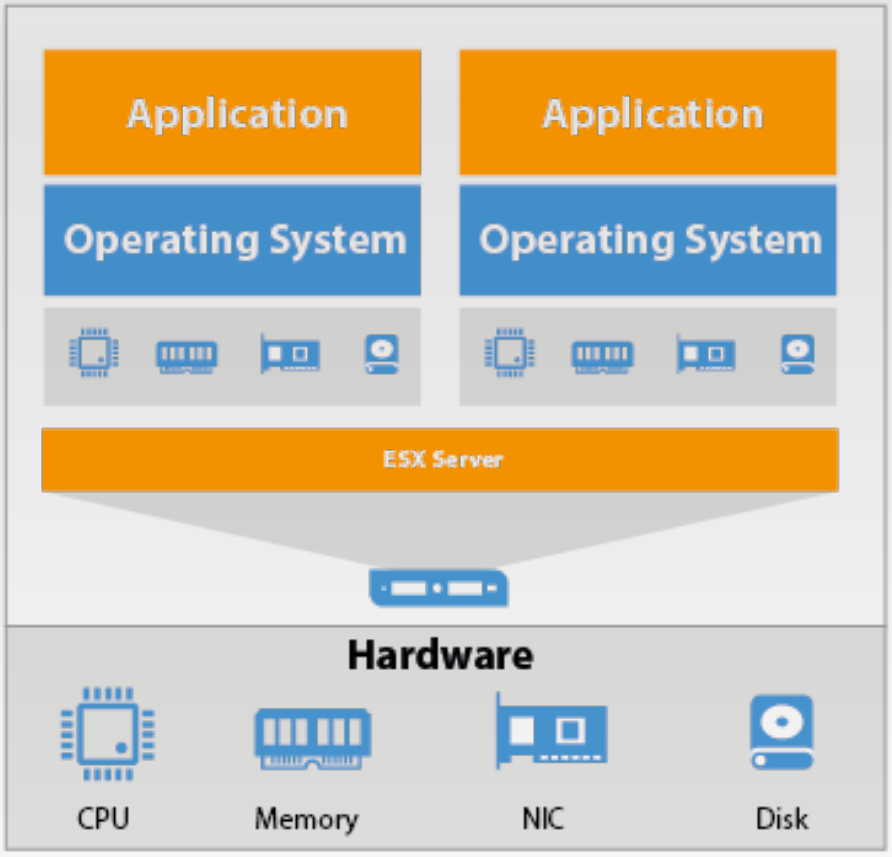

Source: computingtech-247.com



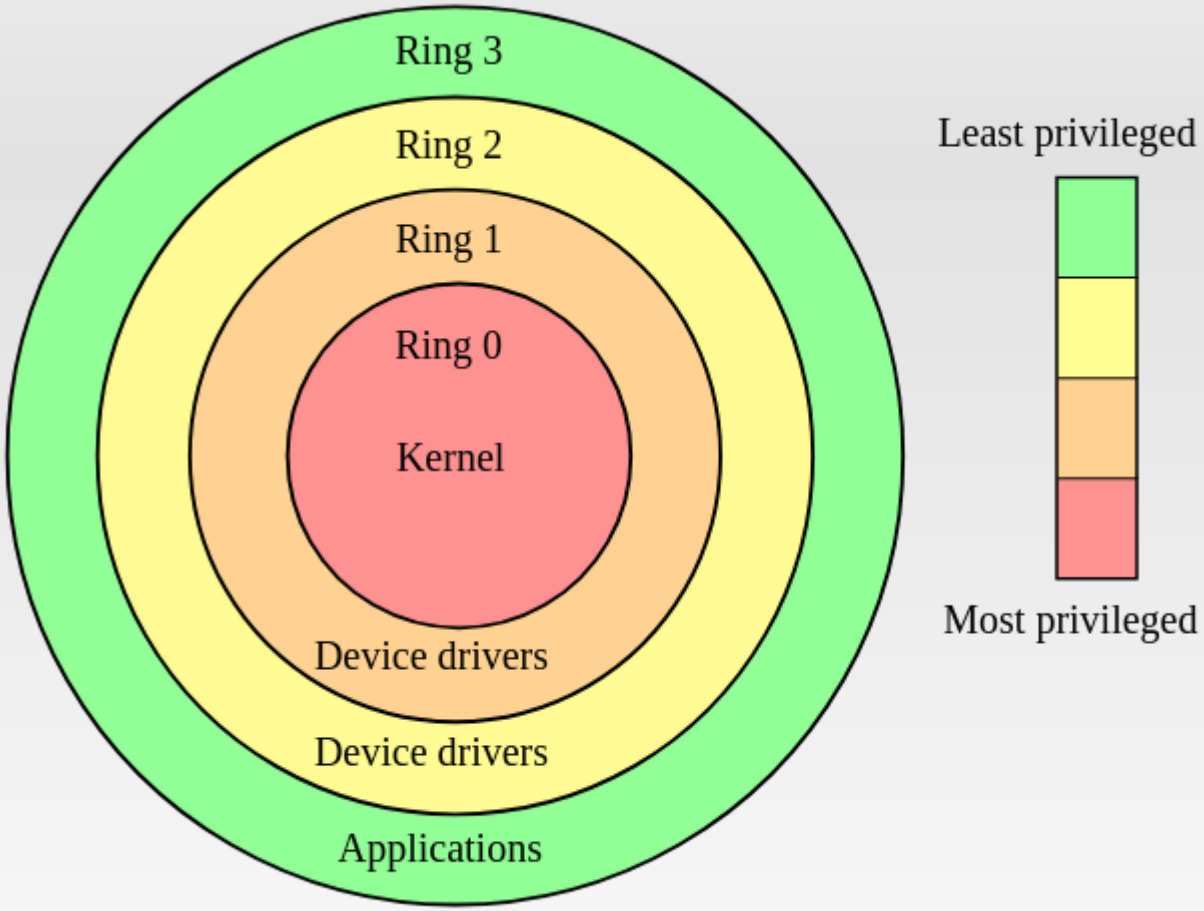

Source: VMware



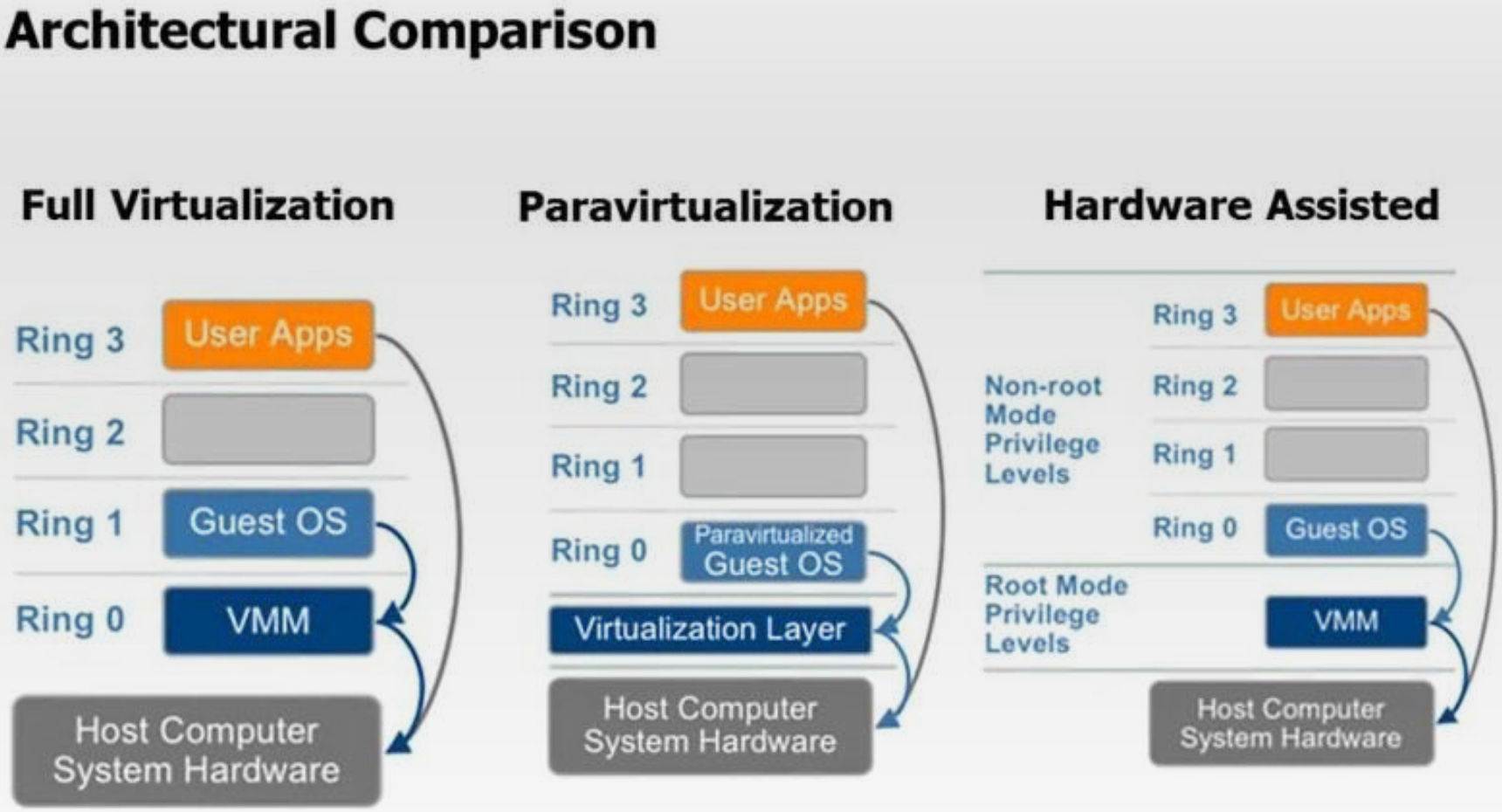

Source: VMware




Source: computingtech-247.com




Source: Wikipedia




Source: computingtech-247.com

# How can I migrate my data and applications from an Amazon Linux paravirtual AMI to a hardware virtual machine AMI?

## Issue

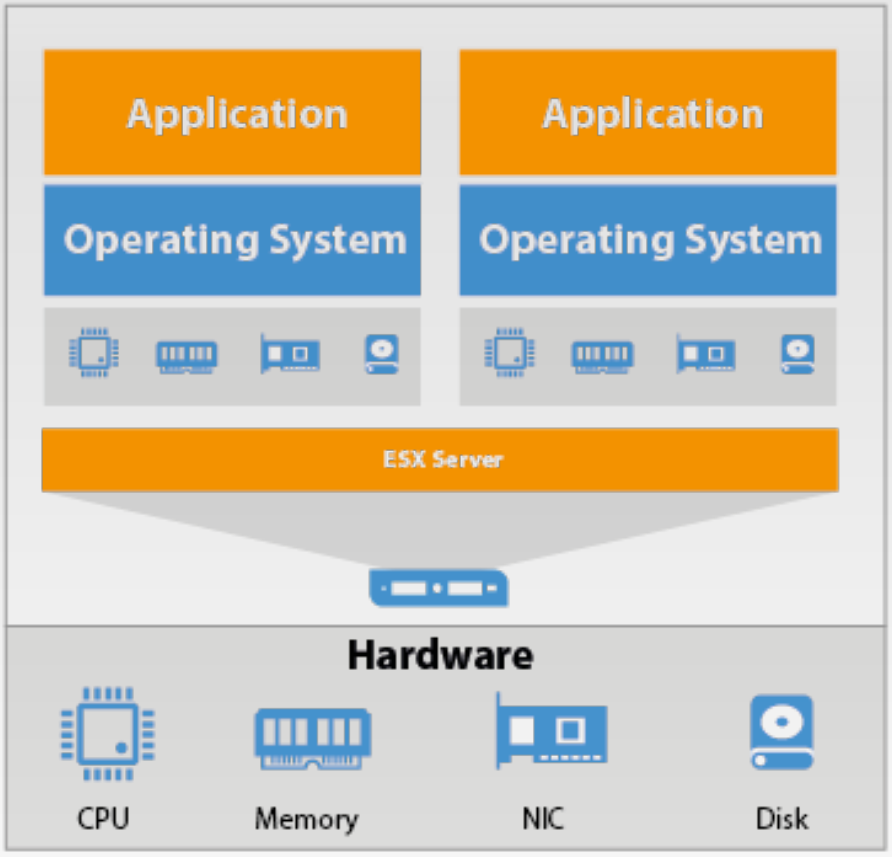
I'm using an Amazon Linux paravirtual (PV) Amazon Machine Image (AMI) on Amazon Elastic Cloud Compute (EC2). How can I migrate to an Amazon Linux hardware virtual machine (HVM) AMI?

## Short Description

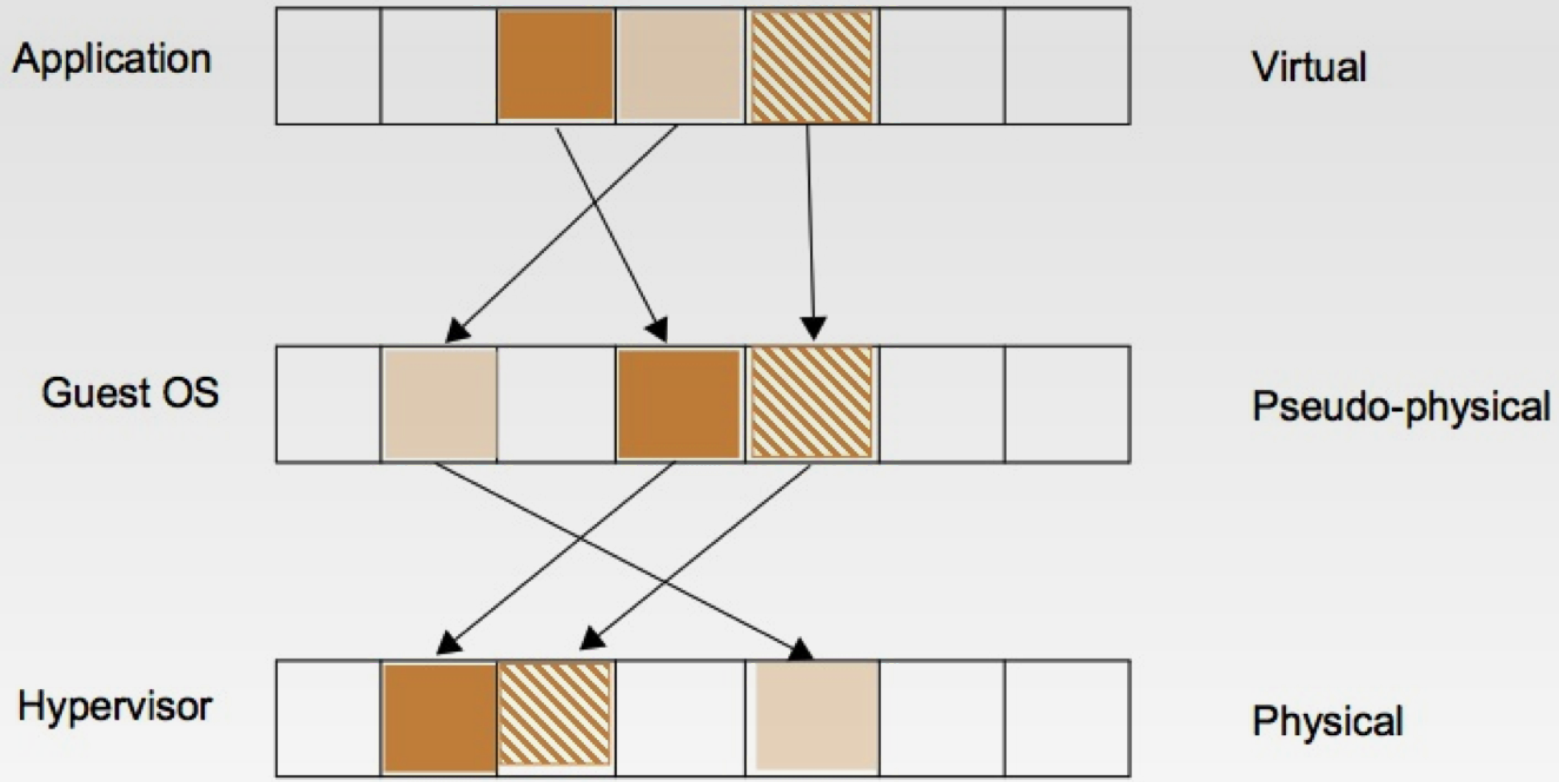
We strongly encourage you to migrate to HVM instances to gain improved security, new features, and performance benefits. For more information on PV and HVM AMIs, see Linux AMI Virtualization Types.

Regarding security, operating system protections are insufficient to address PV instance process-to-process concerns from CVE-2017-5754, as described in AWS Security Bulletin AWS-2018-013. While PV instances are protected by AWS hypervisors from any instance-to-instance concerns, we strongly encourage PV instance users concerned with process isolation (such as processing untrusted data, running untrusted code, or hosting untrusted users) to migrate to HVM instance types for longer-term security benefits.

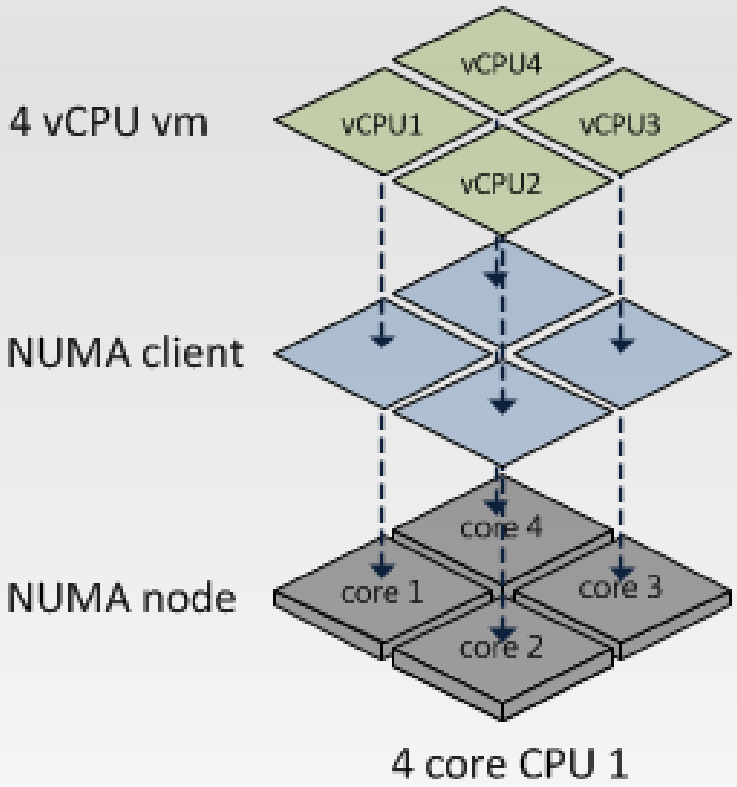
Source: Amazon AWS




Source: computingtech-247.com

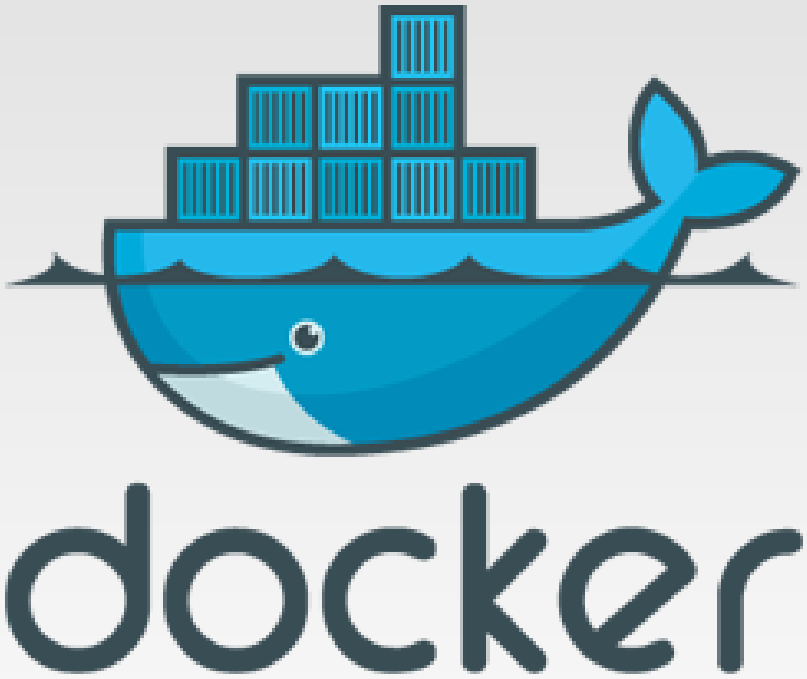


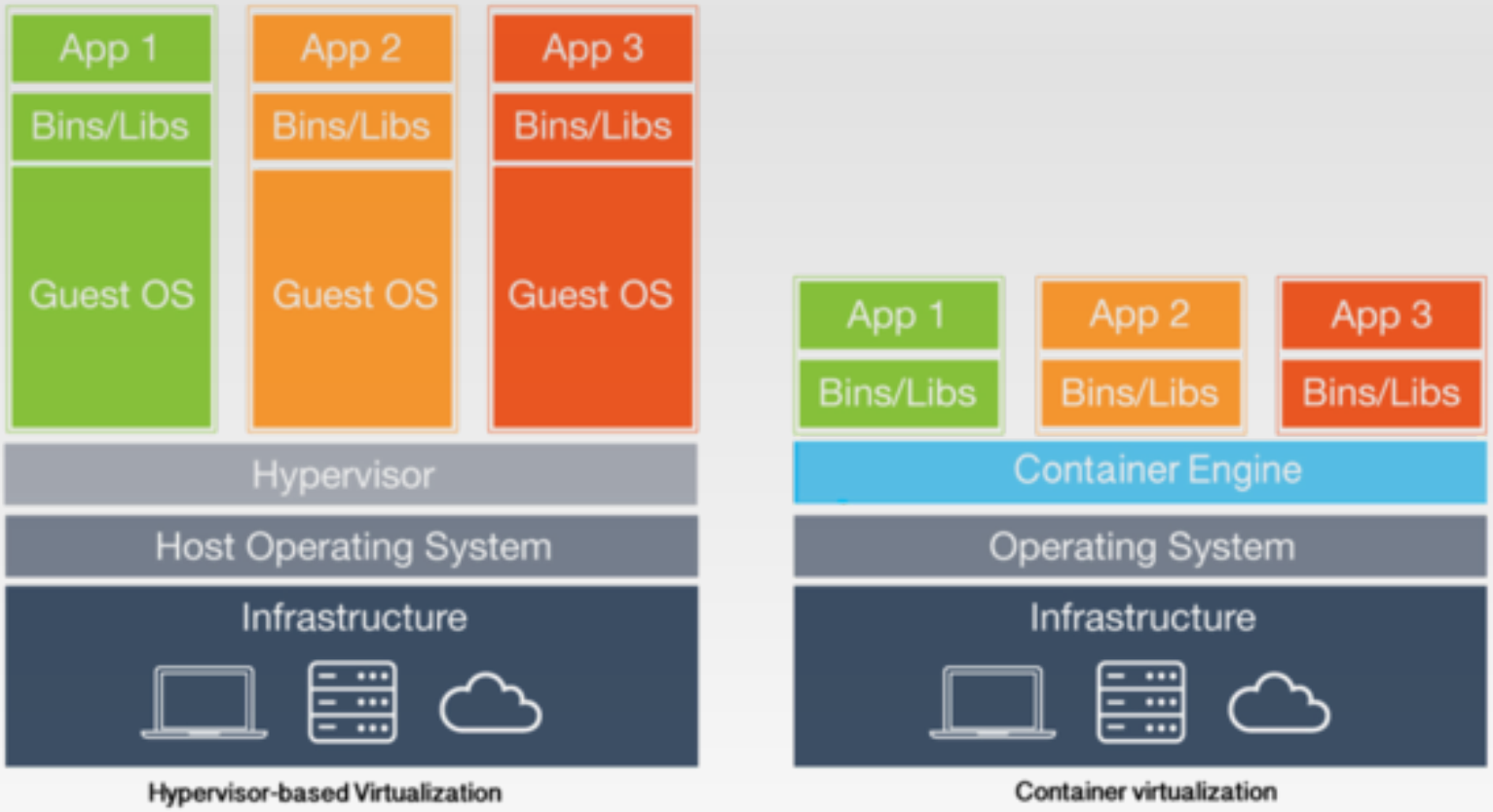

Source: IIC2523 - 2017/2



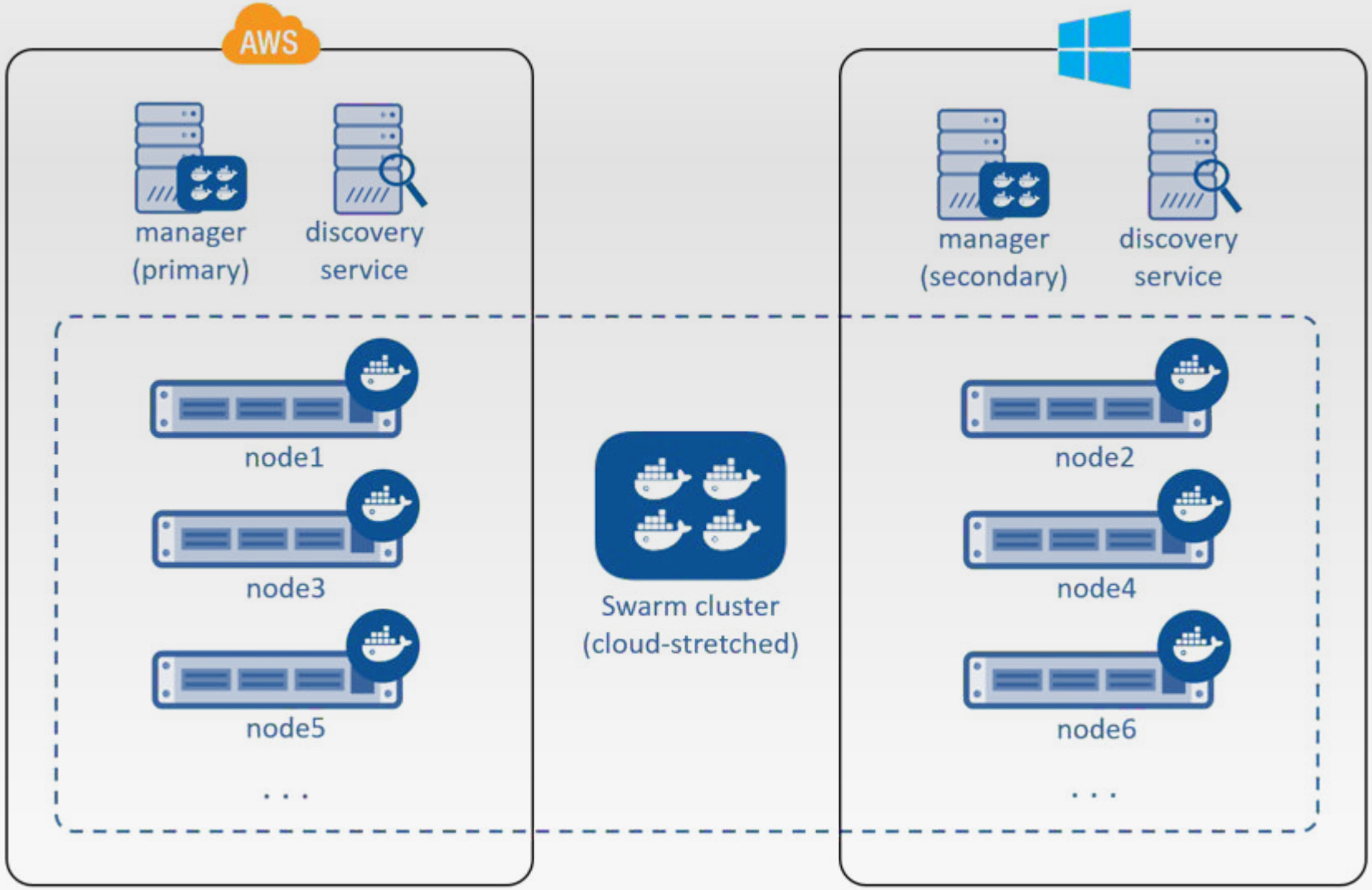

Source: frankdenneman.nl

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación






Source: Hacker Noon




Source: GitHub

enisa

THE EU CYBERSECURITY AGENCY

| VULNERABILITY | MELTDOWN | SPECTRE |
|---|---|---|
| **Processors affected** | Intel, ARM based chips used by Apple | Intel, AMD, ARM, (ARM based chips from used by Apple, Samsung, and Qualcomm) |
| **Method** | Out-of-order execution | Speculative execution, branch prediction |
| **Attack vector** | The attacker must be able to execute code on the target system. | The attacker must be able to execute code on the target system.<br>Remote exploitation is possible through web-based attack using JavaScript, e.g. to attack browsers. |
| **Impact** | Reads kernel memory and physical memory from the user space (privilege escalation), i.e. the attacker can read secret data on the system.<br>In cloud systems, the attack can give access to secret data of other tenants. | Reads the memory of a target/victim process running on the system, i.e. the attacker can leak process specific secret data.<br>The attack needs to be tailored for the target process.<br>Proof-of-concept has suggested that (under certain circumstances) reading kernel memory is possible.<br>The attack can also be carried out in a scenario involving a virtualised environment. |
| **Solution** | Operating system patch specific to Meltdown.<br>Hardware-level fixes in future products. | Software patches for vulnerable processes, e.g. browsers.<br>Bios/firmware updates.<br>Hardware-level fixes in future products. |

**Source:** https://www.enisa.europa.eu/publications/info-notes/meltdown-and-spectre-critical-processor-vulnerabilities


Source: ICO Cloud news