Instituto Tecnológico de Buenos Aires

22.15 - Electrónica V

Trabajo Práctico N°1

Virtualizacion de servidores

Grupo 1:

Matías Agustín Larroque
Leg. 56597

Tomás Agustín González Orlando
Leg. 57090

Lucero Guadalupe Fernandez
Leg. 57485

Manuel Fernando Mollón
Leg. 58023

Ezequiel Vijande
Leg. 58057

Profesores:

Andrés Carlos Rodríguez
Pablo Wündes

Entregado: 16 de Junio de 2020

Índice

1. Definiciones **2**

2. Introduccion **2**

2.1. Terminología . . . 2
2.2. ¿Por qué Virtualización? . . . 3
2.3. Virtualización vs Cloud Computing . . . 3
2.4. ¿Cuándo conviene virtualizar? . . . 4
2.5. Tipos de Virtualización . . . 5
2.6. Ventajas . . . 5
2.7. Desventajas . . . 5

3. Estado actual del mercado de virtualización **6**

3.1. Desarrollo en el ambiente empresarial . . . 7

4. Estado del Arte **7**

4.1. Antecedentes . . . 7
4.1.1. Arquitecturas de Virtualización . . . 8
4.1.2. Anillos de Protección . . . 10
4.2. Beneficios . . . 10
4.3. Inconvenientes . . . 11
4.4. Amenazas de Seguridad . . . 11
4.4.1. Ataques Dos . . . 12
4.4.2. Ataques basados en la comunicación entre VMs huésped y el anfitrión . . . 12
4.4.3. Escape VMM . . . 12

5. Funcionamiento **13**

5.1. Virtualización completa . . . 13
5.2. Virtualización parcial . . . 14
5.3. Virtualización por OS . . . 14
5.4. Caso de ejemplo: Xen . . . 15
5.4.1. Virtualizacion de memoria . . . 15
5.4.2. Virtualizacion de CPU . . . 15

6. Conclusiones y visión de futuro **15**

1. Definiciones

- Workload: Cargas de trabajo.
- Uptime: Tiempo en el que un servidor se mantiene activo durante un tiempo determinado.
- Host: Anfitrión.
- Layer: Capa.
- Dongles: Pequeño dispositivo que se conecta a otro para aportar una función adicional.

2. Introduccion

Se cree que el concepto tiene sus origenes en los 1970s, cuando IBM invirtio mucho tiempo y esfuerzo en desarollar soluciones robustas en cuanto a uso eficiente de los recursos de varias computadoras entre muchos usuarios. Este concepto cambio el paradigma del uso eficietne de la tencologia, llegando a proveer capacidad computacional por un precio mucho menor. Empezamos el artículo con una breve introducción del tema, su definición, beneficios y desventajas.

2.1. Terminología

La palabra virtual proviene del latín «virtus» que significa virtud. Según la RAE, virtual, entre otras cosas, significa "Que tiene existencia aparente y no real". Por lo que cuando se habla de virtualización en el mundo informático/electrónico describe la separación de recursos o solicitud de estos del medio físico que los provee. Esto es decir, que el servicio o recurso utilizado aparenta provenir del medio físico del cual se utiliza. Un ejemplo seria el uso de memoria virtual, donde el software de una computadora gana acceso a mayor memoria de la que físicamente es capaz. Se puede apreciar en la siguiente imagen como cambia el paradigma después de la implementación de una capa de virtualización:

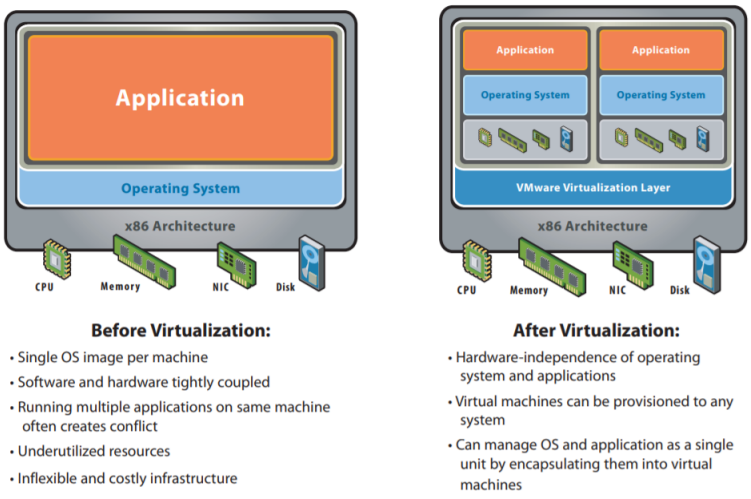

Figura 1: Antes y después de la virtualización

De esta manera se crea una nueva capa de abstracción entre el hardware y el software.

Cuando se habla sobre virtualización en servidores específicamente, hablamos del proceso de dividir un servidor físico en múltiples servidores virtuales por medio de una aplicación de software, donde cada servidor puede correr su propio sistema operativo.

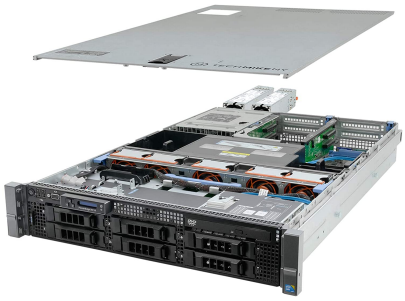

Figura 2: Ilustración de un servidor de virtualización (PowerEdge R710)

2.2. ¿Por qué Virtualización?

Es una solución rentable de proveer servicios de hosting y utilizar efectivamente los recursos de infraestructura. Sin esta virtualización, los servers pueden llegar a usar una pequeña porción de su verdadero poder de procesamiento. Esto nace a raíz de que al no estar bien distribuido el workload, muchos servidores quedan inutilizados a la espera. Esto lleva a desperdicios de recursos y energía. Con el uso de virtualización, cada servidor se divide en múltiples servidores virtuales que utilizan de manera eficiente los recursos y trabajan en conjunto, como varios servidores independientes eficientes.

2.3. Virtualización vs Cloud Computing

La diferencia fundamental es que el cloud computing trabaja con infraestructura como servicio (IaaS), dando acceso on demand a recursos computacionales en una «shared pool» que pueden ser provistos con mínimo esfuerzo del proveedor. Mientras que la virtualización se basa en software como servicio (SaaS). Por lo que la nube es ventajosa para usos públicos, pero para una empresa puede llegar a ser mejor un enfoque por el lado de la virtualización.

A continuación se detallan algunos aspectos claves que diferencian estos dos conceptos:

1. Escalabilidad
   - Cloud Computing: Fácil escalabilidad
   - Virtualización: Limitada en escalabilidad por su configuración
2. Setup
   - Cloud Computing: Proceso tedioso
   - Virtualización: De fácil Setup
3. Flexibilidad
   - Cloud Computing: Flexible para sus usuarios, donde pueden acceder desde cualquier lugar con Internet
   - Virtualización: No es tan flexible en cuanto a acceso, se requiere autenticación
4. Dedicated Hardware
   - Cloud Computing: Múltiples hardware crean el cloud computing
   - Virtualización: Se requiere hardware dedicado para maquina virtual múltiple
5. Integración

- Cloud Computing: Permite expansión futura de usuarios, aplicaciones, etc
- Virtualización: Permite expansión de nuevas maquinas en la misma infraestructura

6. Dependencias
   - Cloud Computing: Múltiples usuarios pueden acceder usando un mismo link
   - Virtualización: Múltiples sistemas operativos pueden ser instalados en un servidor
7. Accesibilidad
   - Cloud Computing: Puede ser accedida desde cualquier parte del mundo
   - Virtualización: Permiso requerido para entrar desde fuera de la red
8. Disaster Recovery
   - Cloud Computing: No dependen se una sola maquina
   - Virtualización: Falla de una maquina puede hacer caer múltiples maquinas virtuales

2.4. ¿Cuándo conviene virtualizar?

Puede no siempre ser beneficiosa la implementación de virtualización. Algunos casos donde es ventajosa la virtualización son:

- Cuando se requiere de tecnología para operar: Si es de vital importancia, la virtualización puede reducir ampliamente los costos.
- Si se tiene una empresa grande: Cuando los servidores aumentan en tamaño la ineficiencia de los mismos tiende a ser mayor y el uso de virtualización se hace esencial para el uso eficiente de recursos.
- Si se pueden cubrir los costos iniciales: Reduce los costos a largo plazo pero requieren une inversión inicial grande si no es una empresa grande.
- Si se necesita espacio: Algunas empresas gastan mucha plata en mantenimiento, espacio y energía de hardware. Con el uso de virtualización se pueden reducir estos problemas de costos.

Algunos ejemplos de cuando NO puede llegar a ser beneficiosa la virtualización son:

- Problemas de licencias: Algunas aplicaciones no permiten ser corridas sobre maquinas virtuales.
- Con el uso de aplicaciones I/O o dongles: Con aplicaciones con características de alto I/O (ej: bases de datos), aplicaciones que requieren uso de gráficos intensivos o dongles se prefiere no utilizar virtualización.
- Cuando tiempos de sincronización son críticos: Las maquinas virtuales corren con su propio clock, lo que significa que diverge del clock del server host. Si estas diferencias son criticas (por ejemplo, aplicaciones que corren en la bolsa en tiempo real o sistemas de control industrial) conviene usar sistemas físicas.
- Capacidad limitada: El uso de maquinas virtuales con un hypervisor no tienen misma performance en cuanto a velocidad que una maquina física. Por lo que si el server esta corriendo a maxima capacidad, puede ser contraproducente el uso de virtualización.

2.5. Tipos de Virtualización

- Full Virtualization
- Para Virtualization
- OS Level Virtualization

2.6. Ventajas

Los beneficios que surgen de esta implementación son:

- Menores costos de operación: Como ya se menciono, la virtualización reduce costos a largo plazo, donde solo se compra la licencia para comenzar a trabajar.
- Mantiene los costos fijos: Se puede tener costos predecibles a la hora de implementarlo, a diferencia de, por ejemplo, cloud computing, donde se tiene que pagar mensualmente y los costos pueden variar.
- Reduce el workload: Proveedores de virtualización hacen actualizaciones automáticas de manera que se reduce el costo y tiempo del equipo IT.
- Mejora el 'uptime': Gracias a técnicas de virtualización, el uptime se puede mejorar drásticamente. Por ejemplo, algunos proveedores ofrecen un uptime de 99.9999 %.
- Reduce costos energéticos: Los costos que generalmente son destinados a los gastos energéticos o costos de cooling, pueden ser redirigidos hacia otro lado.
- Elimina complejidad del servidor: Al virtualizar, se pueden utilizar mejor los recursos y simplificar el servidor de una manera sencilla y eficaz, aprovechando los recursos del mismo.

2.7. Desventajas

- Puede tener altos costos de implementación: Para los proveedores de virtualización, los costos de implementación pueden ser muy altos.
- Tiene sus limitaciones: Como se menciono anteriormente, no todas las aplicaciones y servidores van a ser compatibles con la virtualización a la hora de ser implementada.
- Riesgos de seguridad: Al usar virtualización, los riesgos de seguridad aumentan. El hypervisor introduce una nueva layer de software que puede ser atacada. Ademas, una maquina virtual comprometida puede afectar al resto en un servidor físico. De manera que un ataque a un servidor físico puede llevar a la inhabilitacion de todos los servidores virtuales.
- Problemas de escalabilidad: Cuando se comparten recursos con otras áreas, existe un lag ene el crecimiento de las misma, lo que lleva a usos desproporcionados del espacio en los servidores, esto puede causar problemas de escalabilidad a largo plazo.
- Toma tiempo: Reduce tiempos en cuanto a la implementación, pero cuesta tiempo al usuario a largo plazo comprado con servers locales.

3. Estado actual del mercado de virtualización

- VMware vSphere: VMWare se considera líder en el mercado, dominando el mismo por mucho tiempo. Como desventaja, con el tiempo gano mucha complejidad lo que la convierte en una opcion poco atractiva para negocios chicos. Tambien se piensa que para entornos Linux, se prefieren otras opciones.
- Red Hat Virtualization: Opcion atractiva para entornos Linux. Ratings levemente inferioires al de VMWare a costos mas bajos.
- Proxmox VE: Opcion de bajo costo para entornos Linux. Compite cercamente con Virtuozzo
- Microsoft Hyper-V: Opcion mas economica que VMWare para entornos Windows. Se tiene que tener cuidado con la compatibilidad.
- Citrix Hypervisor: Lidera el mercado en industiras de graficos 3D y maneja entornos tanto Windows como Linux
- Oracle VM Server: Primera opcion para uso con aplicaciones Oracel. Aunque tiene bajo rating de satisfaccion de usarios.
- IBM PowerVM: Primera opcion para uso con apliaciones AIX, IBM Linux y clientes IBM i. Mejor para empreas grnades con mucno presupuesto.
- Virtuozzo: Creada para proveer soporte comercial a la plataforma KVM (Kernel based Virual Machine)

Prod.	Platform	Scalability	Overhead %	Markets	Cost	Migration	Key Differentiator
Vmware vSphere	x86	1,024 VMs per host	5 to 25	SMB-large enterprise	$995 per CPU, plus $273 per year support	Drag and drop or command line	Market leade in virtualizatic
Red Hat Virtualization	x86	up to 400 hosts	5 to 20	highly-scaled deployments with budget constraints.	$999/per managed hypervisor socket pair each year	Manually or auomated	Strong in Linu environments
Proxmox VE	x86/AMD64	Up to 32 nodes per cluster	5 to 10	Hyperconverged infrastructure, Ceph Storage cluster, software-defined data center, cloud computing.	€74.90 per CPU	One click in Web interface	Lower cost provider in Linux environment
Microsoft Hyper-V	x86	240 vCPUs per VM	9 to 12	Windows Server users, Microsoft/Azure customers	$1,323 for up to 16 cores, free with MSC	Import/export enables easy VM move	Top offering Windows da centers
Citrix Hypervisor	X86	64 VMs per host	5 to 10	Citrix Virtual Apps and Desktops users, data center server consolidation, high-performance 3D graphics.	$1149 per CPU socket, free to users of Citrix Virtual Apps and Desktops	Can move a running VM from one host to another	Lower cost alternative, popular amo SMB
Oracle VM Server	X86, SPARC	256 vCPUs per guest	5 to 10	Oracle app users	Free	Move over secure SSL links	Geared for Oracle customers
IBM PowerVM	AIX, Linux and IBM i clients	1000 VMs on a single server	10 to 15	Virtualization for AIX, Linux and IBM i clients running IBM Power platforms	$590 per core	Move active or inactive VMs	Very well suited for IBI environment
Virtuozzo	x86	About 50 virtualization instances per server	5 to 20	KVM users, open source users, SMBs	$990 per month per business	Command line interface	Focused on open source

Figura 3: Tabla de comparacion

3.1. Desarrollo en el ambiente empresarial

La virtualización de servidores es una tecnología adoptada por muchas empresas debido a sus beneficios, mencionados en este artículo. Esto da a lugar a una competencia entre los proveedores de los servicios de virtualización.

Para conocer estos proovedores y cómo se situan en el mercado, a continuación se muestra una imagen extraída de una página de Gartner Group que representa un "magic quadrant" actualizado al año 2016:

Figure 4: Magic Quadrant - Empresas proovedoras de virtualización como servicio

Este cuadrante generado por Gartner Group, que es una prestigiosa empresa consultora e investigadora de tecnología, plasma un análisis cuantitativo para mostrar tendencias sobre las empresas de un mercado en particular.

Se puede ver que la empresa "VMware", por ejemplo, Se situa como la más visionaria y como la líder en el mercado. También en el cuadrante se plasman varias empresas con actividad de nicho.

4. Estado del Arte

4.1. Antecedentes

La práctica de la virtualización surgió en la década de 1960 cuando IBM quiso mejorar el particionado de los mainframes (o computadoras centrales) para mejorar la utilización del CPU, de manera que los programadores pudieran estar utilizando recursos del mainframe al mismo tiempo. Los científicos de IBM observaron que estas particiones lógicas permitían que varios procesos y aplicaciones pudieran estar ejecutándose al mismo tiempo, lo que aumentaba la eficiencia. En ese tiempo, reinaban los costosos mainframes, por lo que tenía sentido aprovechar este escaso recurso para múltiples procesos, mediante VMM (Virtual Machine Monitor).

Tiempo después, con el inicio de la década de 1980 y 1990, la arquitectura x86 (que comprendía los microprocesadores compatibles con el juego de instrucciones Intel 8086) empezó a prevalecer y surgieron las minicomputadoras y luego las PCs (computadoras personales), al punto de que esta arquitectura se empezó a utilizar para implementar servidores y los mainframes junto a VMM pasaron a ser una curiosidad histórica. A modo de ejemplo, era más costoso tener un mainframe que dividiera recursos para una cantidad de tareas que tener varios equipos que realizaran cada uno una de esas tareas, además que ocupaban un menor espacio.

Irónicamente, en los '90, las capacidades de las computadoras modernas y su bajo costo (la combinación que había hecho tan prolífero el uso de VMM en la década pasada) empezaron a causar problemas que los investigadores pensaron que las máquinas virtuales podrían resolver. Como ya mencionamos, los bajos costos de las PCs hicieron que su uso se masificara, pero la CPU se encontraba generalmente infrautilizada, al igual que el almacenamiento. Además, la cantidad de funcionalidades agregadas en los sistemas operativos hacían que éstos fueran más frágiles y vulnerables. Poder mover aplicaciones que antes corrían en muchas máquinas físicas a máquinas virtuales y consolidar las mismas en algunas pocas físicas permitía incrementar la eficiencia y el uso de la CPU, como así también gestionar mejor el almacenamiento. En el presente, VMM no es tanto un vehículo para multitarea, como se pensó originalmente, sino más una solución para confiabilidad y seguridad.

4.1.1. Arquitecturas de Virtualización

Como ya mencionamos, el software de virtualización se conoce como hipervisor o Virtual Machine Monitor (VMM) cuyo propósito es alojar los recursos físicos a cada sistema operativo o a cada aplicación que se está ejecutando sobre un sistema operativo. Una vez definido, el hipervisor emula un dispositivo físico para cada sistema operativo virtual y maneja las comunicaciones entre este SO y los recursos físicos.

El software del hipervisor puede instalarse de manera independiente o como parte de un sistema operativo. Como consecuencia, la manera en la que el hipervisor es instalado define dos arquitecturas de virtualización, como se puede observar en la figura (5) [1].

El Tipo I de hipervisor, también conocido como virtualización *bare-metal*, refiere a que no hay sistema operativo anfitrión porque la VMM se sitúa directamente sobre el hardware físico e intercepta las comunicaciones entre las múltiples máquinas virtuales y los recursos físicos.

La segunda arquitectura, o el Tipo II de hipervisor, se conoce como *hosted*, donde el VMM se encuentra sobre el sistema operativo anfitrión y se ejecuta como una aplicación más. En este caso, es el SO anfitrión el encargado de proveer los drivers de entrada/salida y es quién gestiona las máquinas virtuales huéspedes. Un claro ejemplo de esta arquitectura es el software VirtualBox. La principal desventaja de la arquitectura *hosted* es que, al funcionar sobre un sistema operativo, gasta más recursos; sin embargo como punto positivo, cuenta con mucha compatibilidad con el hardware, ya que el SO anfitrión controla los drivers.

[1] Imagen extraída de: https://www.how2shout.com/how-to/hyper-v-vs-virtualbox-basic-comparison.html

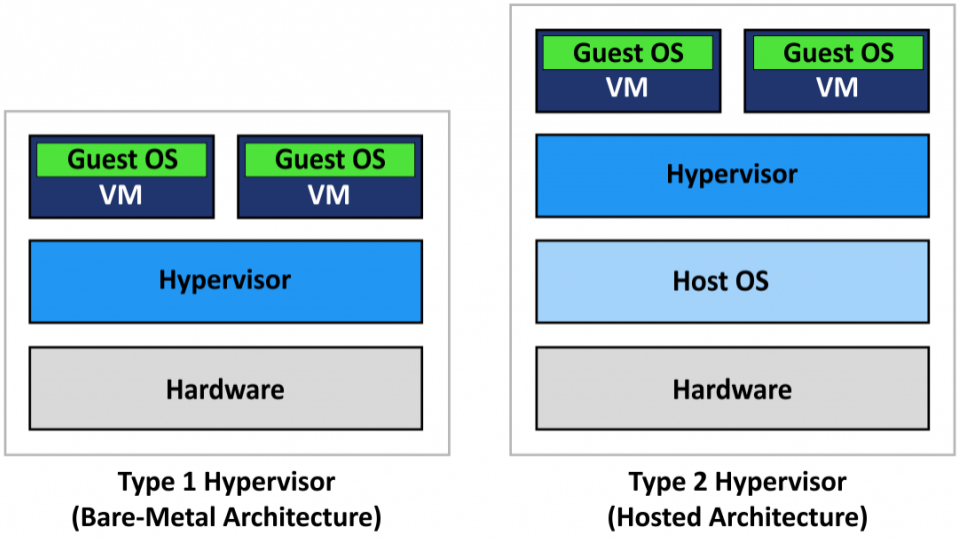

Figure 5: Arquitecturas de virtualización.

La característica principal del VMM es que remueve la dependencia del sistema operativo con los recursos físicos, con el hardware. En otras palabras, los recursos son controlados por el hipervisor y no por el SO anfitrión o el hardware. Debido a aquello, múltiples sistemas operativos pueden correr con el mismo hardware al mismo tiempo, estando aislados entre sí. Como resultado, el hardware físico es particionado en unidades lógicas conocidas como máquinas virtuales (VM).

Con esto, podemos definir los tres principales atributos de los VMM:

Aislamiento Sólo el hipervisor tiene la responsabilidad de controlar y monitorear las máquinas virtuales huéspedes que residen en el hardware físico, y también tiene la responsabilidad de alojar y gestionar los recursos físicos que requieren las VMs. Se puede decir entonces, que el VMM provee aislamiento, es decir, cada máquina virtual está aislada de las otras máquinas virtuales que corren desde el mismo hardware. Esto es lo mismo que decir que las aplicaciones que se están ejecutando en una máquina virtual no pueden ver ni interactuar con otras aplicaciones que están corriendo en otra máquina virtual. Cabe aclarar, cada máquina virtual está a su vez aislada del sistema operativo anfitrión de la misma manera.

Interposición Como ya mencionamos, el hipervisor es quien gestiona las instrucciones que requieren privilegios sobre el hardware. El sistema operativo huésped comunica las interrupciones (*interrupts*) al hipervisor que en su debido momento procesará los eventos interactuando en favor del SO huésped. También, intercepta las solicitudes del periféricos del sistema operativo huésped y las mapea de manera adecuada con los periféricos físicos correspondientes.

Inspección El hipervisor tiene acceso al estado de todas las máquinas virtuales que están corriendo, como el estado del CPU, o de la memoria. Poder acceder a estas variables es necesario para que el VMM pueda por ejemplo, reestablecer una máquina virtual a un estado previo (*rollback*), o poder realizar una 'fotografía' del estado actual de la máquina (*check pointing*). Además permite que los administradores puedan mover, o instanciar entornos de virtualización desde un anfitrión físico hacia otro.

4.1.2. Anillos de Protección

La arquitectura x86 ofrece cuatro niveles de privilegios, en forma de anillos, que se pueden observar en la figura (6)[2]. Estos anillos permiten varios niveles de aislamiento y abstracción de privilegios dentro de la misma arquitectura de la computadora. Se acomodan de manera jerárquica de más privilegiado (más confiable y menos restricciones para acceder a recursos - Ring-0) a menos privilegiado (menos confiable y con más restricciones para acceder a recursos - Ring-3), como se pueden observar en la figura (6). El anillo-0 (Ring-0) es el que tiene más privilegios e interactúa directamente con los recursos físicos del hardware.

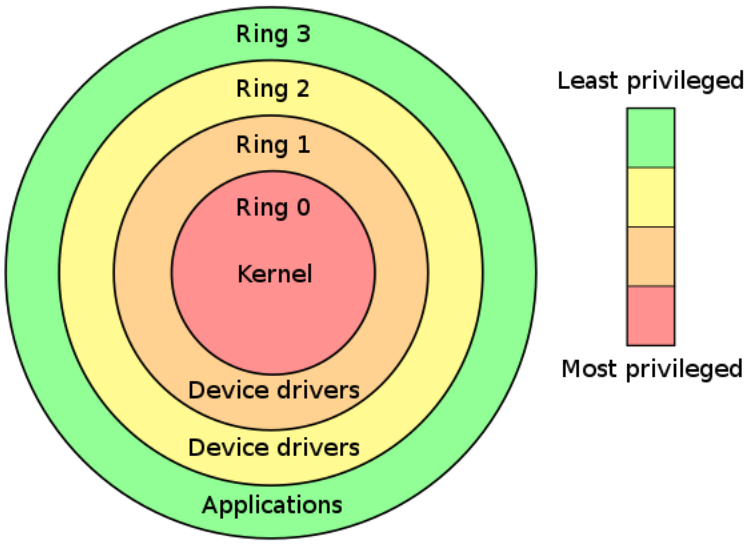

Figure 6: Anillos de protección en CPU de arquitectura x86.

Los anillos menos privilegiados no pueden acceder a los anillos del interior sin instrucciones que expliciten y permitan ese acceso. Y son los anillos exteriores los que tienen estas restricciones para resguardar y proteger la información y funcionalidades internas de malos usos, malware, y demás.

En un entorno de virtualización, el hipervisor corre en modo kernel (*Ring-0*) porque es su responsabilidad asignar recursos de hardware y alojar memorias de dirección a las máquinas virtuales huéspedes. Ergo, estas VMs corren en un anillo con menos privilegios que el anillo-0, entonces el kernel de las máquinas virtuales cuenta con menos privilegios para acceder a recursos o referenciar direcciones de memoria sin el consentimiento del hipervisor.

4.2. Beneficios

La virtualización lleva consigo beneficios e inconvenientes intrínsecos de esta tecnología. En esta parte del artículo se intenta agrupar los beneficios en tres factores, y también luego se mencionarán los inconvenientes.

El primer beneficio se lo puede etiquetar como "consolidación". Esta consolidación, o unificación, permite combinar todas las cargas de trabajo en un número reducido de plataformas físicas, lo cual incrementa el uso de los recursos y la optimización a la hora de utilizarlos. Además, poseer en funcionamiento una plataforma de virtualización que admita compatibilidad y permita administrar distintos sistemas independientes, favorece la migración de sistemas antiguos e incompatibles con tecnologías emergentes por otros más actuales, ya que no hace falta cesar la actividad de aquellos sistemas que no sean necesario cambiar, lo cual reduce el impacto en estas migraciones de sistemas.

[2]Imagen extraída de: https://es.wikipedia.org/wiki/Anillo_(seguridad_informática)

En segundo lugar, se cuenta con la "fiabilidad". Se puede afirmar esto ya que esta tecnología mantiene funcionalidades y disponibilidades de operación en distintas maquinas virtuales, de manera aislada, lo cual permite que alguna de las maquinas falle, sin que esta falla tenga efectos sobre otras maquinas, aunque estás esten funcionando en el momento de la falla. Por otra parte, a las maquinas virtuales les son asignados recursos a medida que estas los necesitan, sin que tengan que encargarse de la obtención, configuración e instalación de los mismos.

Como tercer y último lugar, se identifica al beneficio de la "seguridad". Este beneficio se da en el sentido del aislamiento entre maquinas virtuales, ya que si la seguridad de una maquina está comprometida, el riesgo se detiene en esa maquina y no se propaga a las demás, debido a la capa de virtualización.

4.3. Inconvenientes

En cuanto a los inconvenientes de la tecnología de virtualización, se identifican:

1) Pérdida de performance/rendimiento en algunos casos específicos en los que se requiera un hardware único para mayor eficiencia, o para cálculos que lleven mucho tiempo y que requieran mucha capacidad de una central de procesamiento especial.

2) Necesidad de redundancia en el caso de que falle el hardware que implementa la virtualización. Al fallar este, todas las particiones pierden sus datos, excepto que se tenga una redundancia para este hardware.

3) Costos operativos. En una organización, se debe tener en cuenta la necesidad de personal experto para poder encargarse de mantener y manejar el entorno virtual, dado sus complejidades, licencias que hay que tener en cuenta, y actualizaciones.

4.4. Amenazas de Seguridad

En una organización, los aspectos clave a tener en cuenta a la hora de garantizar la seguridad de la información son:

- Confidencialidad: Los datos no deben poder ser accedidos de forma no autorizada.
- Integridad : Los datos no deben poder ser modificados, dañados, o eliminados mediante acceso no autorizado. access
- Disponibilidad: Los datos deben poder ser accedidos por quien esté autorizado a hacerlo en el momento en que lo desee.
- Autenticación: Debe haber procesos para verificar la identidad de un usuario con respecto al acceso a la información.
- Autorización: Cada usuario autorizado deberá tener una serie de privilegios y permisos determinados y limitados acorde a su usuario.
- Responsabilidad: Se deberán establecer y realizar controles y auditorías para monitorear los permisos de acceso de los usuarios autorizados.

Migrar los recursos de una empresa a un ambiente virtual no solo implica contraer todos las amenazas y vulnerabilidades de seguridad de un servicio o sistema operativo de cada huésped a un sólo sistema físico, sino que además introduce nuevas amenazas y vulnerabilidades de seguridad al sistema, que deberán ser tenidas en cuenta, invirtiendo en personal experto y en procesos (de parcheo, actualizaciones, etc) adicionales.

A continuación mencionaremos algunos ejemplos de posibles ataques de ciber seguridad en relación a la virtualización.

4.4.1. Ataques Dos

Un ataque DoS o Denial of Service es una clase de ciber-ataque en el cual el atacante bloquea los recursos de la máquina atacada para que sus usuarios no puedan utilizar sus servicios.

Un ataque DoS en el contexto de la virtualización puede tener lugar en aquellos casos en los que un VM rompa el principio de aislamiento y tenga control sobre los recursos físicos de otro huésped VM o del anfitrión físico, corrompiéndolos o deshabilitándolos.

4.4.2. Ataques basados en la comunicación entre VMs huésped y el anfitrión

Como fue mencionado anteriormente, el aislamiento entre VMs es un atributo de importancia significativa dentro del contexto de la virtualización. Este atributo permite a cada huésped confinar todas sus acciones a su propio espacio de direcciones, por lo que, configurando de forma cuidadosa y correcta a dicho aislamiento, se lograría evitar problemas como:

- Interferencia de otras VMs huésped, así como también por parte del anfitrión en tareas que deberían estar ya aisladas.
- Acceso a información sensible por parte de otra VM.

A pesar del atributo de aislamiento característico de toda virtualización, hay sin embargo oportunidades de comunicación entre distintas VMs a través de características agregadas como el uso de un portapapeles compartido que permita copiar y pegar contenido desde una VM a otra. Situaciones como las mencionadas anteriormente pueden permitir la inyección de código malicioso entre los sitemas operativos de distintas VMs y con el anfitrión, y mantener un monitoreo permanente de las configuraciones del ambiente de virtualización juega por lo tanto un rol importante en la seguridad del sistema.

Algunos tipos de virtualización remueven la capa de aislamiento al permitir correr un sistema operativo dentro de otro. Estos casos plantean un desafío de seguridad.

4.4.3. Escape VMM

Una VM huésped no debería poder tener en su conocimiento que la misma es efectivamente una VM dentro de un ambiente de virtualización. El proceso a través del cual una VM obtiene esta información y logra interactúar con la VMM es conocido como “escape VMM”. A través de este escape VMM, una VM podrá acceder a otras VMs del anfitrión físico. El hecho de que un VMM se vea comprometido debido a un escape VMM exitoso se conoce como “hyperjacking”.

Security Threats	Security Components	Safeguards
Virtualization Based Malware	Integrity	1. Hypervisor security & integrity checks. 2. Guest OS security & hardening. 3. Virtualized network security & isolation. 4. Zero-day real-time detection of malicious activities. 5. Security policies and controls in place 6. Automatic restoration of guest VMs to a clean state.
Denial of Service	Availability	
Communications Attack	Confidentiality Authentication Authorization	
VM Escape	Authentication Authorization Accountability	
Inter-VM Attacks and Network Blind Spots	Authentication Authorization	

Figure 7: Impacto de amenazas de seguridad en aspectos cruciales de seguridad y sus salvaguardas requeridos

5. Funcionamiento

A grandes rasgos el funcionamiento de los servidores virtuales puede entenderse como la siguiente serie de pasos:

- Un Layer dedicado separa la capa fisica del host del guest
- Este software divide y maneja los rescursos fisicos a los guests.
- El usuario utiliza directamente las aplicaciones e interfaces que corren en los guests.
- El Layer se encarga de entregar recursos de la capa fisica a un guest cuando el usuario los solicita asi como tambien efectuar los cambios necesarios en la capa fisica.

Los servidores virtuales pueden dividirse en tres categorias principales. Estas son virtualización completa, virtualización parcial y virtualización por sistema operativo(OS).

5.1. Virtualización completa

En este tipo de virtualización se tiene que cada guest se comporta de manera independiente de los demás y no hay interacción entre ellos. Los guests pueden utilizar distintos sistemas operativos y distintos formas de manejo de

archivos. Sin embargo, todo los guests corren en el mismo servidor físico, por lo que comparten los recursos físicos de este.

Con el fin de cada guest se abstraiga completamente de los demás, se utiliza un software denominado hypervisor el cual se encarga de interactuar directamente con los recursos del host como el disco y la CPU.

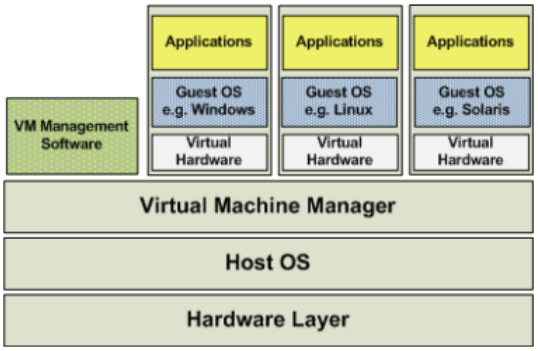

Figura 8: Esquema de virtualizacion completaa

Algunos ejemplos comerciales que siguen este esquema son VMware Workstation[3] , Parallels[4] y Virtual PC[5]

5.2. Virtualización parcial

A diferencia de la virtualización completa, se puede pensar como que en este tipo de virtualización se "delegan" tareas sobre los guests. En este caso los guests saben de la existencia de los demás y también que recursos necesitan utilizar. Por lo que, si bien en este esquema también hay un hypervisor, el mismo necesita menos procesamiento ya que cada guest esta enterado de las demandas de recursos de los demás.

5.3. Virtualización por OS

Finalmente, la virtualización por OS se distingue en que no hay hypervisor sino que la funcionalidad de virtualización es empleada completamente por el OS del host. En este caso se tiene la limitación de que todos los guests deben utilizar el mismo OS. Tiene en comun con la virtualización completa el hecho de que cada guest es independiente del otro y no sabe de la existencia de los demás.

[3] https://www.vmware.com/es/products/workstation-player.html
[4] https://www.parallels.com/
[5] https://www.microsoft.com/es-ar/download/details.aspx?id=3702

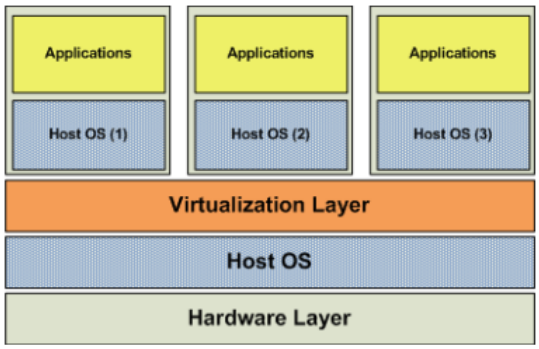

Figura 9: Esquema de virtualizacion por software

Algunos ejemplos que siguen este esquema son OpenVZ[6] , y Linux VServer[7]

5.4. Caso de ejemplo: Xen

Xen es una tecnologia de vitrualizacion de codigo abierto desarrollada por la universidad de Cambridge. Esta tecnologia sigue el equema de virtualizacion parcial y a continuacion se daran detalles de como el mismo realizaba las tareas de virtualizacion.

5.4.1. Virtualizacion de memoria

Para las lecturas, Xen automatiamente otorga permiso de read-only, de acceso directo a los OS de los guests para acceder a las paginas del host.Mientras que las actualizaciones de paginas se realizan por Xen mediante 'hyperllamadas'.Las hyperllamadas consisten en un medio de comunicacion sincronico entre los guests y Xen. Para evitar overhead los OS de las maquinas virtuales pueden acumular actualizaciones tandas y hacer una sola hyperllamada que se encargue de todas las actualizaciones y asi evitar tener que realizar una hyperllamada por actualizacion.

5.4.2. Virtualizacion de CPU

Para este caso el hypervisor hace uso del CPU directamente por lo que es necesario que Xen tenga mayor prioridad que el OS propio del host.Esto convierte a Xen en la funcion con mayor prioridad de todo el sistema por lo que para correr instrucciones privilegiadas es necesario virtualizarlas y ejecutarlas directamente mediante Xen.

6. Conclusiones y visión de futuro

La virtualización es una tecnología ampliamente utilizada a través del tiempo, que permite aprovechar recursos de hardware de manera eficiente y promueven la expansión de servidores en empresas. La independencia y el aislamiento que se brinda entre los servidores es la pieza escencial de esta tecnología.

Virtualización de servidores sigue estando notablemente vigente en el mercado, y continúa en crecimiento, a pesar de haber surgido en los principios de los 70s, y habiendo hoy en día otras opciones que pueden llegar a ser competencia, como los contenedores o el cloud service. Sin embargo, la robustez de la virtualización es tal que se complementa

[6] https://openvz.org/
[7] http://linux-vserver.org/Welcome_to_Linux-VServer.org

con estas herramientas. Esto es lo que nos permite afirmar que es altamente probable que la virtualización continúe implementandosé en el mercado.

Referencias

[1] Daniels, Server virtualization architecture and implementation. 2009.

[2] F. Bazargan, C. Y. Yeun, and M. J. Zemerly, "State-of-the-Art of Virtualization, its Security Threats and Deployment Models," International Journal for Information Security Research, vol. 3, no. 3, pp. 335–343, Jan. 2013.

[3] D. Marinescu and R. Kroger, "State of the art in autonomic computing and virtualization". Wiesbaden, Germany, 2007.

[4] G. Aljabari, "Virtualization of IT infrastructure for small and medium businesses," 2012 International Conference on Communications and Information Technology (ICCIT), 2012.

[5] Virtualization overview. 2006. https://www.vmware.com/pdf/virtualization.pdf

[6] M. Rosenblum and T. Garfinkel, "Virtual machine monitors: current technology and future trends," Computer, vol. 38, no. 5, pp. 39–47, 2005.

[7] "Server Virtualization," VMware. [Online]. Available: https://www.vmware.com/topics/glossary/content/server-virtualization. [Accessed: 16-Jun-2020].

[8] "Why choose virtualization?," TechAdvisory.org. [Online]. Available: https://www.techadvisory.org/2014/05/why-choose-virtualization/. [Accessed: 16-Jun-2020].

[9] L. Gaille, "14 Advantages and Disadvantages of Virtualization," Vittana.org, 16-Dec-2019. [Online]. Available: https://vittana.org/14-advantages-and-disadvantages-of-virtualization. [Accessed: 16-Jun-2020].

[10] "Top 10 Reasons Not to Virtualize," ServerWatch. [Online]. Available: https://www.serverwatch.com/server-trends/top-10-reasons-not-to-virtualize.html. [Accessed: 16-Jun-2020].

[11] "Top 10 Useful Comparison Between Cloud Computing vs Virtualization," EDUCBA, 13-Apr-2020. [Online]. Available: https://www.educba.com/cloud-computing-vs-virtualization/. [Accessed: 16-Jun-2020].