# Problemas de procesamiento

2 estrategias: Ambiente virtual:

* Virtualizar un chip y proveer acceso a este recurso.
* No aplica virtualización, durante ‘tiempos’ provee segmentos de procesamiento en el procesador físico (pCPU) de cliente virtualizado hacia el procesador virtual de l sanfitriones de máquinas virtuales en el servidor físico.

‘Es la manera de como los hipervisores virtuales proveen recursos o sus clientes’

\*\*Parámetros de un servidor

El número de procesadores.

* Es una medición ‘critica’, en un ambiente virtual que en uno físico.

Servidor físico: En el sistema toda la configuración de recursos de computo es de un exclusivo para aplicaciones.

* Ej: Server con procesadores quad-core en donde la aplicación usa 16 cores disponibles.

Servidor virtual: migración App Web a Virtualización:

* Mejora las capacidades de procesamiento por medio de la virtualización.

Ley Moore: Proveer procesadores puede incluso ser mejor y mucho más rápido, que proveer un recurso con un servidor físico.

\*\*Configuración de Maquinas Virtuales ‘procesador, memoria, red y almacenamiento I/O’

## Buenas prácticas.

1. Regla Básica de crear VM: Un único vCPU y configuración de aplicación en monitor.
2. No ubicar la misma cantidad de vCPU y pCPU.
   * El hypervisor ocupa los pCPU para la virtualización de los anfitriones en beneficio de la VM.

### \*\*Administración de hardware para Sistemas Operativos nativos

Como intermediario entre solicitudes de condigo en aplicaciones y hardware se debe dar respuesta a la información y procesamiento. El Sistema Operativo traslada las solicitudes al dispositivo ‘drivers’ que corresponda hacia los controladores físicos, hacia los dispositivos de almacenamiento I/O de retorno.

El Sistema Operativo es el Reuter central de información y accesos de control a todos los recursos físicos del hardware.

Una función clave de un OS es ayudar en prevención maliciosa o llamadas de sistemas accidentales.

\*\***Anillos de protección**: Nivel de acceso o privilegios dentro de un sistema de computador.

Ring 0: Capa más confiable.

* Es donde el kernel del OS trabaja.
* Interactúa directamente con el hardware.
* Se ejecutan los hipervisores, acceso de control físico a los VM.

Ring 1 y 2:

* Se encuentran los drivers físicos.

Ring 3:

* Las aplicaciones se ejecutan en esta área.
* Ocupa al OS para ejecutar a su beneficio en el R0.

# Administración de memoria

Como un numero de vCPU, el almacenamiento de memoria en una maaquina virtual es uno de las configuracinoes mas impoiortantes a elegir: en cambio, l;os recursos de memoria son usualmente el filtro que pasa la infraestructura virtual conforme crece,. Incluso como los procesos de virtualizacion la memoria utilizada en los ambientes virtuales es mas como la administración de recursos físicos que la creación de las entidades virutales.

Para procesos similares, los creadores de aplicaciones preguntan por ubicaciones de memoria de espejo en la infraestructura física de donde migraron, sin importar si el tamaño de la ubicación es garantizado o no.

“Tamaño correcto” La base de las máquinas virtuales en su caracterizada configuración actual, hay características generadas dentro del hypervisor que ayuda el uso de memoria óptimo. Un ejemplo es **page sharing.** Es similar la duplicidad de datos, técnicas de almacenamiento que reduce el numero de bloques de almacenamiento al ser usado.

En los clientes en donde los anfitriones son ejecutados en donde el sistema operativo es el mismo y las mismas aplicaciones entre 10% y 40% de la memoria física actual puede ser reclamada. El 25% en un servidor de 8GB puede agregar adicional dos clientes en 1GB máquinas virtuales. Dado que el hypervisor administra el compartimiento de páginas, el sistema operativo de la maquina virtual no conocen que está pasando en el sistema físico. Otra estrategia del uso eficiente de memoria es parecida a un provisionamiento leve de administración de almacenamiento.

El proceso de reservación es ejecutado mediante el balloning (globo). El hypervisor activa un controlador balloon que (virtualiza) infla y presiona al sistema operativo anfitrión a mover las páginas al disco.

Existen técnicas de administración de memoria que provee un manejo de recursos mejores. En todos los casos, el Sistema operativo ve en la máquina virtual y tiene acceso a un conjunto de memoria que sido ubicadas a él. El hypervisor administra el acceso a la memoria física para asegurar contra asegurar las solicitudes ubicadas en servicio en una manera temporal sin la necesidad de impactar en las máquinas virtuales.

# Administration de I/O

El rendimiento de la aplicación puede suele estar directamente relacionada con el ancho de banda asignado de un servidor. Si el acceso del almacenamiento está siendo filtrado o restringiendo trafico hacia la red, el caso incluso puede causar a una aplicación ser percibida de bajo rendimiento. De esta manera, durante la virtualización de procesos, virtualización I/O es un item crítico. La arquitectura de como I/O es administrada en un ambiente virtual

is straightforward (see Figure 14.8). In the virtual machine, the operating system makes a call to the device driver as it would in a physical server. The device driver then connects with the device; though in the case of the virtual server, the device is an emulated device that is staged and managed by the hypervisor.

This virtual device plugs into the hypervisor’s I/O stack that communicates with the device driver that is mapped to a physical device in the host server, translating guest I/O addresses to the physical host I/O addresses. The hypervisor controls and monitors the requests from the virtual machine’s device driver, through the I/O stack, out the physical device, and back again, routing the I/O calls to the correct devices on the correct virtual machines.

The advantages of virtualizing the workload’s I/O path are many. It enables hardware independence by abstracting vendor-specific drivers to more generalized versions that run on the hypervisor.

This abstraction enables of one of virtualization’s greatest availability strengths: live migration.

. In more mature solutions, capabilities exist to granularly control the types of network traffic and the bandwidth afforded to individual VMs or groups of virtual machines to insure adequate performance in a shared environment to guarantee a chosen Quality of Service level.

A faster processor enables the hypervisor to perform its I/O management func tions more quickly, and also speeds the rate at which the guest processor processing is done. Explicit hardware changes for virtualization support also improve performance.

TCP Offload Engine (TOE) removes the TCP/IP processing from the server proces sor entirely to the NIC. Other variations on this theme are Large Receive Offload (LRO), which aggregates incoming packets into bundles for more efficient process ing, and its inverse Large Segment Offload (LSO), which allows the hypervisor to aggregate multiple outgoing TCP/IP packets and has the NIC hardware segment them into separate packets.

# VMware ESXi

## Provee un Tipo 1 a los usuarios

Conjunto de diferencias fundamentals en el la arquitectura ESXi en comparación con otras soluciones disponibles.

El Kernel Virtual (VMKernel) es el core del hypervisor y configura todas las funciones de virtualización.

VMware restructure por complete a ESX para su instalación y administración sin el servicio de consola. La nueva arquitectura doblega a ESXi (I por integración) tiene todo el servicio de gestión como parte del VMkernel. Provee paquete de menor tamaño y seguro en comparación al anterior.

VMware ESXi provee unas características avanzadas y sofisticadas por su disponibilidad, escalabilidad, seguridad, disponibilidad en administración y configuración. Las disponibilidades adicionales son introducidas con cada lanzamiento, proveyendo las capacidades de la plataforma.

**VMotion** Almacenamiento: Permite la reubicación de los archivos de información que compone una maquina virtual, mientras la máquina virtual está en uso.

**Tolerancia** a fallos: Crea una copia en cada momento en un cliente diferente. Si el cliente original sufre de un fallo, Las conexiones de la maquina virtual restauran la copia, sin interrumpir ls usuarios o la aplicación en uso.

**Administrador** de recuperación del sitio: Se usan varias técnicas de copiado, para selecciona la maquina virtrual de copia a un sitio secundario en caso de un desastre en el datacenter. El sitio secundario puede ser levantado en cuestión de minutos.

**Control I/O** de red y almacenamiento: Permite al administrador de especificar el ancho de banda de la red en una red virtual de una manera muy granular.

**Programador** de recursos distribuidos (DRS): Ubica inteligentemente en los clientes las maquinas virtuales para el levantamiento y puede de balancear de manera automática los flujos vía la base VMotion en políticas de negocios y uso de recursos.

-----------------------------------------------------------------------------------------------------------------------------------

Microsoft Hyper-V and Xen VARIANTS

Xen, an open-source hypervisor.

Xen requires a dedicated operating system or domain to work with the hypervisor, similar to the VMware service console.

Guests on Xen are unprivileged domains, or sometimes user domains, referred to as DomU. Dom0 provides access to network and storage resources to the guests via BackEnd drivers that communicate with the FrontEnd drivers in DomU.

Dom0 provides access to network and storage resources to the guests via BackEnd drivers that communicate with the FrontEnd drivers in DomU. Unless there are pass-through devices configured (usually USB), all of the network and storage I/O is handled through Dom0. Since Dom0 is itself an instance of Linux, if something unexpected happens to it, all of the virtual machines it supports will be affected. Standard operating system maintenance like patching also can potentially affect the overall availability.

Microsoft has had a number of virtualization technologies, including Virtual Server, a Type 2 hypervisor offering that was acquired in 2005 and is still available today at no cost. Microsoft Hyper-V, a Type 1 hypervisor.

Hyper-V has a parent partition that serves as an administrative adjunct to the Type 1 hypervisor (see Figure 14.11). Guest virtual machines are designated as child partitions. The parent partition runs the Windows Server operating system in addition to its functions, such as managing the hypervisor, the guest partitions, and the devices drivers. Similar to the FrontEnd and BackEnd drivers in Xen, the parent partition in Hyper-V uses a Virtualization Service Provider (VSP) to provide device services to the child partitions.

### Java Virtual Machine

Hypervisors support one or more virtual machines on a host. These virtual machines are self-contained workloads, each supporting an operating system and applications, and from their perspective, have access to a set of hardware devices that provide compute, storage, and I/O resources.

can support multiple threads and each thread has its own register and stack areas, though the heap and method areas are shared among all of the threads. When the JVM is instantiated, the runtime environment is started, the memory structures are allocated and populated with the selected method (code) and variables, and the program begins.

LINUX VSERVER VIRTUAL MACHINE ARCHITECTURE