Fundamentos de virtualización

¿Qué es la virtualización?

La virtualización es la creación de una representación virtual de recursos físicos y lógicos mediante software. Esto incluye servidores, almacenamiento, redes, sistemas operativos y aplicaciones. Esta práctica permite un mejor aprovechamiento de los recursos disponibles, mayor flexibilidad y escalabilidad en entornos de TI.

¿Qué es un hipervisor?

Es el corazón de la virtualización, es el intermediario que existe entre las máquinas virtuales y un servidor físico, esto permite la correcta asignación de recursos. Existen 2 tipos de hipervisores:

Hipervisor de tipo 1 o bare-metal

Se instala directamente sobre el hardware físico, sin necesidad de un sistema operativo, es más eficiente. Suele usarse en entornos empresariales. Algunos ejemplos son: VMware ESXi, Microsoft Hyper-v, Xen o KVM.

Hipervisor de tipo 2 o hosted

Se ejecuta sobre un sistema operativo ya existente como un programa más, lo que lo hace más sencillo de instalar pero menos eficiente. Algunos ejemplos son VMware Workstation, VirtualBox o QEMU

Entornos virtualizados

La virtualización es una práctica que beneficia a las organizaciones a disminuir la cantidad de máquinas físicas necesarias en el entorno de TI. Existen diferentes elementos que pueden conformar un sistema virtual:

Máquinas virtuales (VM)

Son sistemas operativos completos virtualizados que se ejecutan sobre un hipervisor. Es importante mantenerlas actualizadas y protegidas, ya que comparten hardware y se ejecutan con privilegios elevados. Si una VM es comprometida, el host también podría estar en riesgo.

Contenedores

Son entornos ligeros que incluyen una aplicación y sus dependencias, compartiendo el kernel del sistema operativo anfitrión. Docker es una de las plataformas más utilizadas para este tipo de virtualización. Aunque son más eficientes, si un contenedor con privilegios elevados es comprometido, el sistema operativo subyacente también podría verse afectado.

Infraestructura de equipo de escritorio virtual (VDI)

Los entornos de escritorio de los usuarios se pueden almacenar de manera remota en un servidor utilizando thin client o escritorios virtuales. Esto hace que sea mucho más fácil el crear, eliminar, copiar, archivar o descargar rápidamente configuraciones por medio de la red. Este requiere alta disponibilidad y capacidad de almacenamiento.

Tipos de virtualización

Virtualización de servidor

Es la virtualización donde se busca conseguir varios servidores virtuales partiendo desde un servidor físico, esto sirve para ejecutar múltiples sistemas operativos de forma independiente y de forma simultánea si se necesita. Consta de los siguientes elementos: Servidor, hipervisor y finalmente, máquinas virtualizadas.

Virtualización de escritorio

Permite a los usuarios trabajar sobre una máquina con todos sus procesos y aplicaciones, pero sin la necesidad de contar con esa máquina de forma física.

Virtualización de recursos hardware

Es la simulación de recursos hardware de forma lógica, esto incluye la virtualización de: la memoria principal (Memoria RAM), unidades de almacenamiento e interfases de red.

Virtualización de red

Separa la red física en varias redes virtuales o une varias redes físicas en una sola red virtual. También puede implementar tecnologías como SDN (Software Defined Networking) para gestionar redes de forma programable.

Virtualización de aplicaciones

Permite ejecutar aplicaciones desde un servidor remoto sin instalarlas directamente en la máquina física del usuario.

Tipos de redes en hipervisores

NAT

Comparte la conexión de red del sistema anfitrión, permitiendo el acceso a internet y a dispositivos de red local. Las máquinas virtuales poseen una IP privada, lo que la hace inaccesible desde el exterior. Ideal para entornos de pruebas o laboratorios.

Adaptador Puente

Conecta la máquina virtual directamente a la red física, asignándole su propia IP publica, lo que la hace visible al exterior. Útil para simulaciones de entornos de producción.

Interna

Permite únicamente la comunicación solo entre máquinas virtuales en la misma red interna, creada por el hipervisor. Sin conexión al sistema anfitrión ni a la red física externa. Adecuada para laboratorios aislados y entornos de prueba.

Protección de máquinas virtuales

Las máquinas virtuales al igual que una computadora física, requiere parches, actualizaciones y medidas antimalware para protegerlas de amenazas externas. Dependiendo de las herramientas especificas disponibles en una plataforma, la nube ofrece opciones de seguridad adicionales para proteger las máquinas virtuales, entre las cuales están:

Ubicación de la subred

Destinar cuidadosamente la subred para cada instancia para que solo tenga el acceso necesario al mundo exterior.

Deshabilitar los puertos y servicios

Habilitar únicamente los servicios y puertos necesarios para reducir la exposición innecesaria al exterior.

Gestión y políticas de las cuentas

Desactivar las cuentas de usuario predeterminadas y crear cuentas de usuario con políticas de administración de cuentas recomendadas, como: complejidad de la contraseña y acceso con privilegios mínimos.

Instalar software antivirus/antimalware

Instalar software que protejan la máquina virtual es crucial, en algunas ocasiones puede estar disponible como servicio desde la plataforma en la nube.

Implementar firewall basado en host/software IPS/IDP

Configurar firewalls basados en host y utilizar servicios de IPS/IDS para monitorear y proteger las máquinas virtuales contra amenazas externas. En algunas plataformas de la nube se puede encontrar como servicio.