

Hálózatba kapcsolt erőforrás platformok és alkalmazásaik

Maliosz Markosz

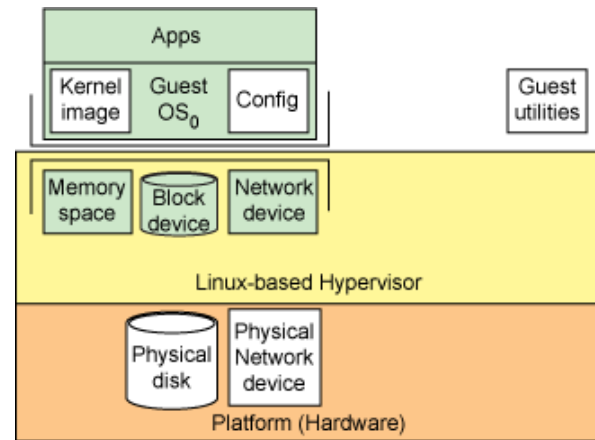
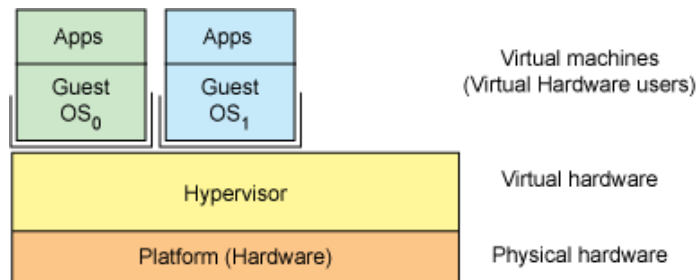
TMIT

2020

Virtuális hálózatkezelés alapok

Virtuális gép (Virtual Machine - VM)

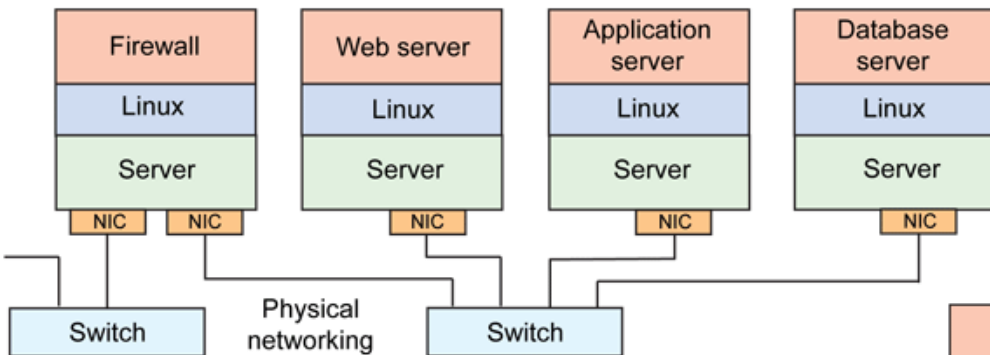
- CPU, memória, háttértár és ezen felül a hálózat virtualizálás kulcsfontosságú!
- több, különböző operációs rendszer ugyanazon a hardveren
- hibák izolálása: egy VM hibája nem teszi tönkre a többit
- operációs rendszer szintű állapot mentés/visszatöltés
- szerver terhelés (workload) optimalizálás
- felhő infrastruktúra szolgáltatás



Virtualizálás

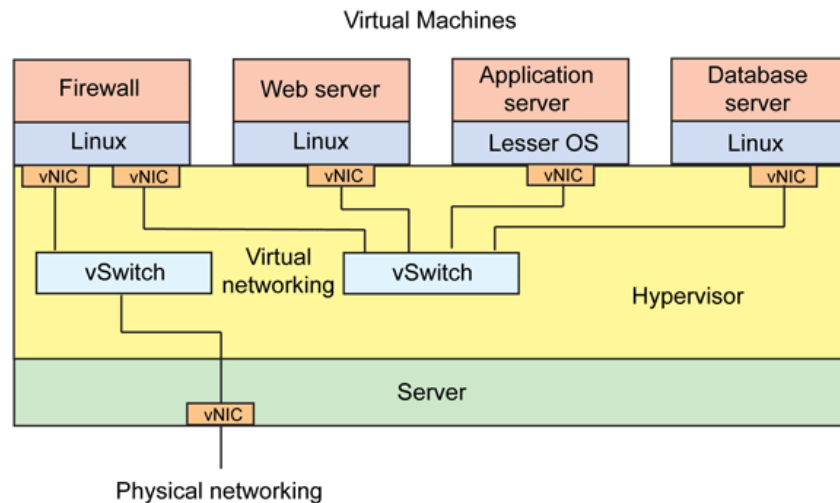
- CPU időbeli megosztása a vendég rendszerek között
- Memória „térbeli” megosztása a vendég rendszerek között
- Lemez, hálózati és egyéb eszközök szimulálása

Hálózatok: fizikai - virtuális



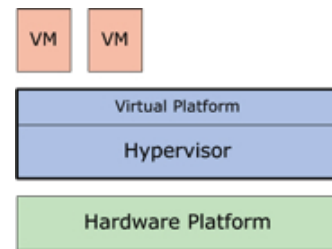
NIC: Network Interface Card
vNIC: virtual NIC

- virtuális kapcsoló
 - a lokális kommunikáció sebessége a memóriaátvitel sebességétől függ
- implementációk
 - Linux bridge
 - Open Virtual Switch (OVS)

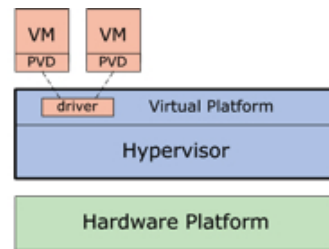


Hálózati kártya virtualizálás

- QEMU: Quick Emulator
 - szoftveres platform emulátor
 - szoftveres NIC emuláció
 - KVM: Kernel-based VM
 - hardveres gyorsítás
- virtio
 - input/output para-virtualizáció
 - módosított vendég rendszer
 - egyszerűbb és gyorsabb
 - blokk, általános PCI és hálózati eszközök számára
- TAP: (Test Access Point)
 - Ethernet szintű (L2) virtuális hálózati meghajtó
- TUN: tunnel
 - IP szintű (L3) virtuális hálózati meghajtó



Full Virtualization



Para-Virtualization

VirtualBox hálózatkezelés

- Virtualizált NIC hardver
- Hálózati módok
 - nincs csatlakoztatva
 - NAT (default)
 - kimenő forgalom engedélyezett, VM kívülről és más VM-ből elérhetetlen, külső hozzáférés port továbbítással beállítható
 - NAT hálózat (v4.3-tól)
 - kimenő forgalom engedélyezett, VM kívülről elérhetetlen, hálózaton belül a VM-ek kommunikálhatnak, külső hozzáférés port továbbítással beállítható
 - Bridge-elt kártya
 - mintha a vendég rendszer a fizikai hálózaton lenne
 - Belső csatoló
 - hálózaton belül a VM-ek kommunikálhatnak
 - Host-only kártya
 - hálózaton belül a VM-ek és a hoszt kommunikálhatnak
 - Általános driver

Linux bridge

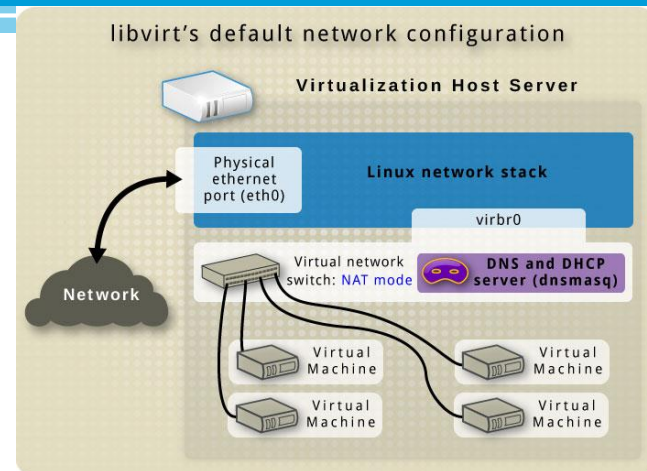
- kernel modul
- konfigurálás
 - `brctl`
 - `ip link`
- példák
 - `sudo brctl show`
 - `sudo brctl addbr br1`
 - `sudo brctl addif br1 eth0`

Linux virtualizáció

- hypervisor: qemu / kvm, Xen, stb.
- libvirt
 - virtualization API
 - is a toolkit and API to manage virtualization hosts
- libvirt GUI: virt-manager

Libvirt hálózat: NAT

- `virsh net-list --all`
 - név: `default`
- default virtual network: NAT
 - `virbro`
 - nincs hozzá csatolva fizikai interfész, mivel NAT + forwarding segítségével kapcsolódik a külvilághoz
 - ip forwarding engedélyezve
 - `/etc/sysctl.conf : net.ipv4.ip_forward = 1`
 - iptables szabályok: ki/be forgalom engedélyezése a virbro-hoz kapcsolódó VM-ek számára (INPUT, FORWARD, OUTPUT és POSTROUTING láncok)
 - DHCP (dnsmasq program)
 - külső hozzáférés port továbbítással beállítható
 - név alapján csatlakoztatható hozzá VM
- különbségek a VirtualBox NAT módhoz képest
 - kimenő forgalom engedélyezett, VM kívülről elérhetetlen, **hálózaton belül a VM-ek illetve a hoszt kommunikálhatnak**
 - kb. NAT hálózat + Host only vegyítése



További Libvirt hálózati módok

- Bridge-elt
 - full bridging, a vendég rdsz. közvetlenül a LAN-hoz kapcsolódik
 - shared physical device: a hoszt fizikai interfésze csatolva a virtuális bridge-hez
 - megj.: vezeték-nélküli interfész nem csatlakoztatható hoszt bridge-hez, csak Ethernet
 - bridge név alapján csatlakoztatható hozzá VM
- Routed
 - ha bridge-elt nem kivitelezhető
 - statikus útvonalbeállítás, nincs NAT
 - hálózat név alapján csatlakoztatható hozzá VM
- Izolált
 - VM-ek egymással és a hoszttal kommunikálhatnak, de a külvilággal nem

