

A decorative graphic consisting of a light gray circle on the left side, partially overlapping a horizontal bar. The bar has a dark gray gradient on the left and a light gray gradient on the right. Large black square brackets are positioned on the left and right sides of the bar, framing the title text.

Virtualios infrastruktūros sauga

1 paskaita

Įvadas į virtualizaciją

[Apie kursą]

Dėstytojas

Prof. dr. Dalius Mažeika

Informacinių sistemų katedra

e-paštas Dalius.Mazeika@vgtu.lt

Kab. L413, tel. 2744830

<http://dma.vgtu.lt>

Vertinimas

Egzamino pažymys kaupiamasis.

- 20% referatas
- 20% savarankiško darbo užduotis
- 60% teorijos egzaminas

[Turinys]

IT Infrastruktūros virtualizacija

- Virtualizacija
- Virtualios infrastruktūros komponentai
- Bendrosios realizacijos (Vmware ESX, MS Hyper-V, Citrix XenServer)
- Virtualios aplinkos valdymas

Virtualizacijos taikymai

- Debesų kompiuterija
- Duomenų centrų virtualizacija
- Virtualių darbo vietų infrastruktūra (VDI)

[Turinys]

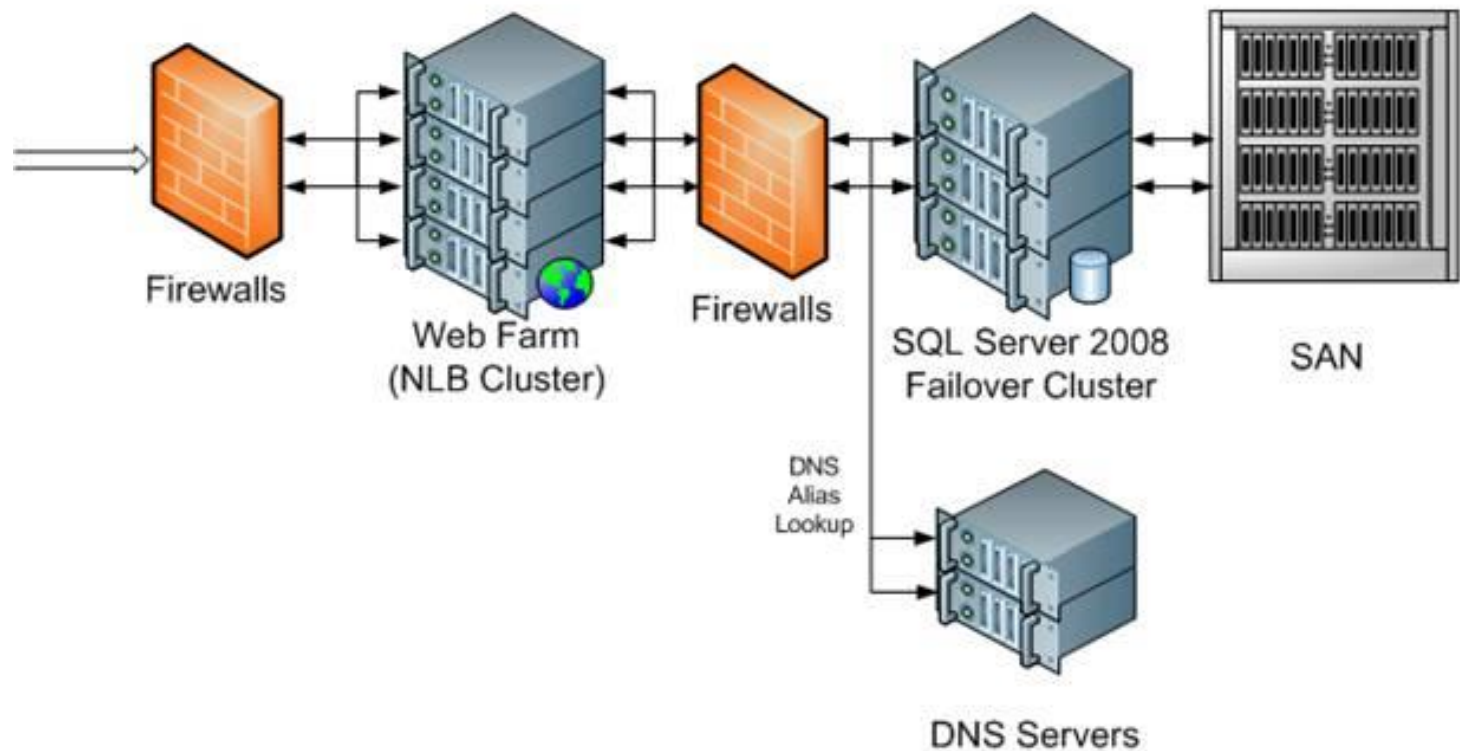
Virtualios infrastruktūros sauga

- Hipervizorių sauga
- Duomenų saugyklų ryšiai virtualioje aplinkoje (SAN, NAS, iSCSI, Virtual Storage Appliance) ir naudojimas virtualioje aplinkoje
- Duomenų saugyklų saugumas
- Klasterizavimas ir sauga
- Diegimo ir valdymo sauga
- Eksploatacijos (operation) sauga
- Virtualiaus tinklo sauga
- Virtualių darbo vietų infrastruktūros sauga

[Duomenų centro IT infrastruktūra]

Duomenų centro tipinę IT infrastruktūrą sudaro fiziniai:

- Serveriai
- Tinklo įrenginiai
- Duomenų saugyklos
- IT saugos įrenginiai

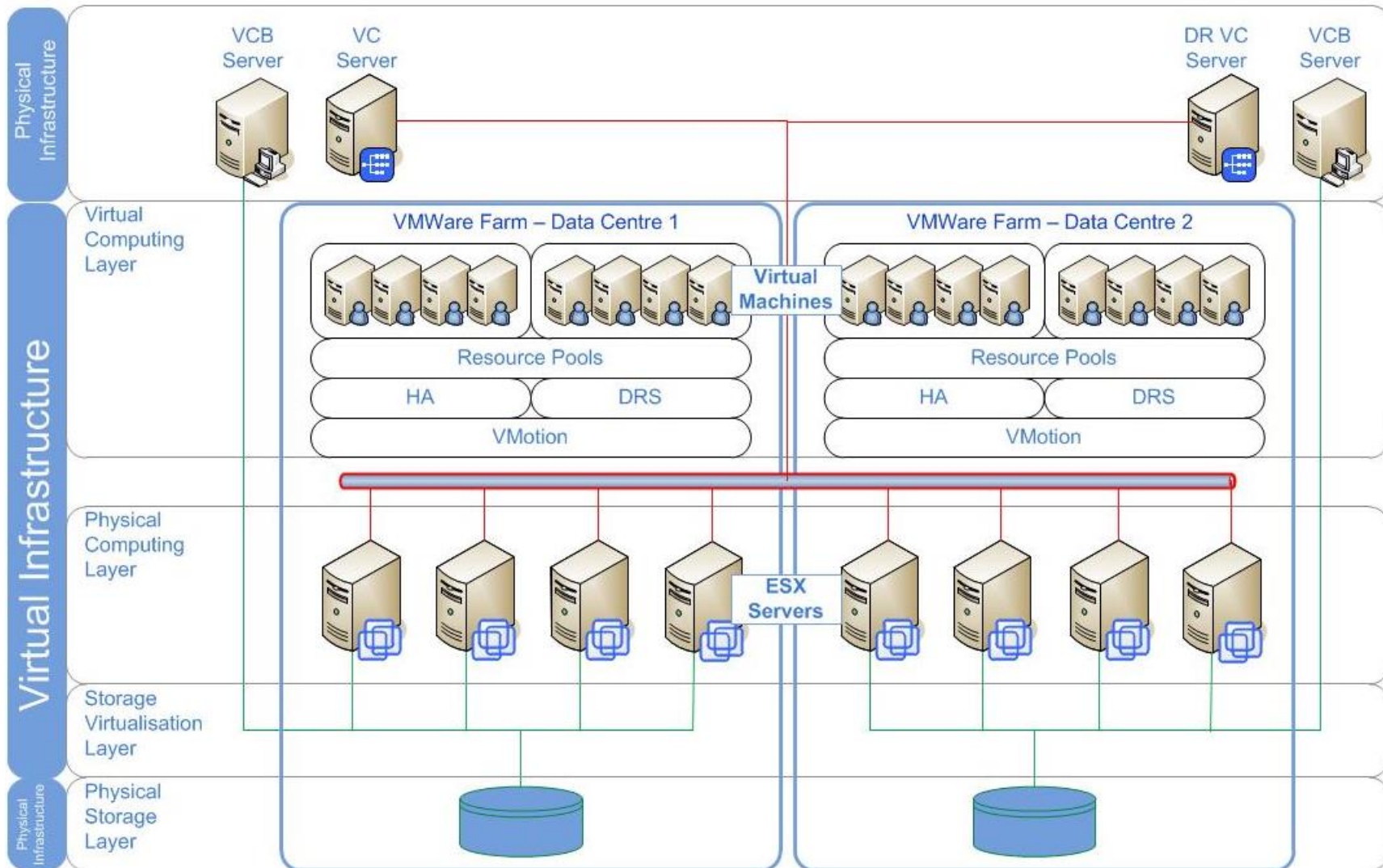


[DS sauga]

Duomenų centro **fizinės IT infrastruktūros** sauga apima:

- **Fizinė sauga**
 - Praėjimo kontrolė, patalpų stebėjimas, energijos tiekimas, kondicionavim.
- **Tinklo sauga**
 - Ungiansienės, IPS/IDS, maršrutizatorių ACL, monitoringas, auditavimas
- **Serverių sauga**
 - OS stiprinimas, autentifikavimas, žurnalai, antivirusinės programos, anti-spam, monitoringas
- **Programų sauga**
 - Autentifikavimas, saugos stiprinimas, patch/update savalaikis instaliavimas
- **Vartotojų sauga**
 - Slaptažodžiai, kortelės, monitoringas, socialinė inžinerija

Virtuali infrastruktūra



[VI sauga]

Virtualizuoto DS IT infrastruktūros sauga apima:

- **Fizinė sauga**
 - Ta pati, kaip fizinės IT infrastruktūros atveju + įrenginių pajungimas prie VM
- **Tinklo sauga**
 - Virtualaus tinklo sauga (L2: MAC flooding, STP, VLAN ir t.t.)
- **Serverių sauga**
 - Hipervizoriaus sauga

[VI sauga]

- **Virtualių mašinų sauga**
 - Tas pats kaip serverių sauga fiziniu atveju
- **Programų sauga**
 - Ta pati, kaip fizinės IT infrastruktūros atveju + atvejai, kaip virusų skenavimas vienu metu
- **Vartotojų sauga**
 - Ta pati, kaip fizinės IT infrastruktūros atveju + prieiga VM tvarkymo atveju, fizinio įrenginio pajungimas ir t.t.

[SDDC]

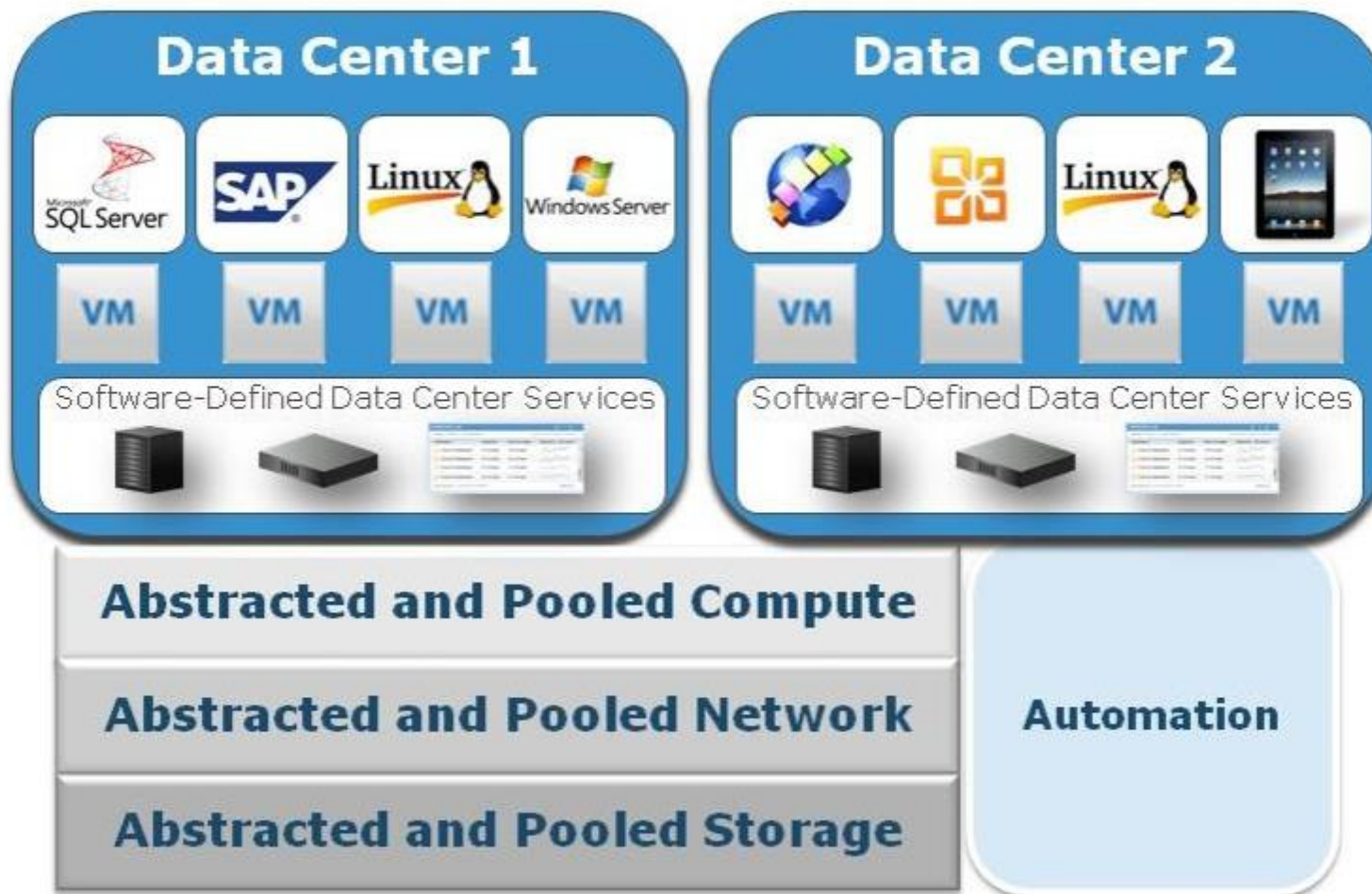
Software-defined data center (SDDC) (arba virtual data center (VDC)) – tai ateities duomenų centrų vizija, kuri praplečia virtualizacijos koncepciją ir teikia **ITaaS**.

SDDS koncepcija apima visų duomenų centro resursų abstrakciją, skirstymą (pooling) ir automatizavimą.

SDDS visi infrastruktūros elementai - tinklai (SDN), saugyklos (SDS), CPU (virtualizacija), IT sauga – yra virtualizuoti ir teikiami kaip paslauga.

[SDDC]

The Software-Defined Data Center



[Debesų valdymo platforma]

The screenshot displays the VMware vRealize Automation web interface. The browser address bar shows the URL: https://vra-01a.corp.local/vcac/org/vsphere.local/?code=hl16Ny9XNMtvS8rZaTh7YF8Ni7rh3v0Te&userstore=Userstore_a3fb3ed3-b41d-4c0b-b253-f359821c26d0#com.vmware.vca. The page title is "New Blueprint: MSBU App 1.0".

The interface is divided into several sections:

- Categories:** A sidebar on the left lists categories such as Machine Types (10), Software Components (22), Blueprints (14), Network & Security (7), and XaaS (5).
- Design Canvas:** The main workspace shows a grid with components for "SGWebTierProd", "SGDBTierProd", "Web_IS", and "DB_SQL". The "Web_IS" component is expanded to show "Win2k12_R2_Base" with sub-components "Microsoft_Inter..." and "Microsoft_NET...". The "DB_SQL" component is also expanded to show "Win2k12_R2_Base" with sub-components "Microsoft_SQL..." and "Microsoft_NET...".
- Web_IS-Win2k12_R2_Base:** A configuration panel at the bottom shows tabs for General, Build Information, Machine Resources, Network, Security, and Properties. The "Network" tab is active, displaying a table with columns: ID, Network, Assignment Type, Address, Load Balancing, and Custom Properties.

ID	Network	Assignment Type	Address	Load Balancing	Custom Properties
0	NSXRTD10101016	Static IP			

At the bottom of the configuration panel, there is a "Maximum network adapters:" field set to "Unlimited".

The footer of the interface includes the copyright notice "Copyright © 2012-2015 VMware, Inc. All rights reserved.", a "Play" button, system tray icons for ControlCenter, vRealize Automati..., and vcsa-01a.corp.loc..., and the version information "version 7.0.0 (build 3282778)". The system clock shows "6:11 PM 1/27/2016".

[Virtualizacijos prielaidos]

- Šiuolaikiniai kompiuteriai yra pakankamai galingi:
 - 2, 4, 8, 32 branduolių procesoriai
 - operatyviosios atminties dydis matuojamas TB
 - 24 HDD viename kompiuteryje (vidiniai)
 - > PB duomenų saugyklos (SAN, NAS)
- Maža CPU utilizacija (fiziniuose serveriuose apkrova 10 – 30 %)
- Padidėjęs sistemų saugumo ir izoliuotumo poreikis
- Resursų padalinimas tarp nesusijusių vartotojų
- Operacinės sistemos saugumo ir patikimumo problemos

[Sprendimas]

Sprendimas – kurti viename fiziniame kompiuteryje **virtualias mašinas (VM)**, turinčias savarankiškas operacines sistemas.

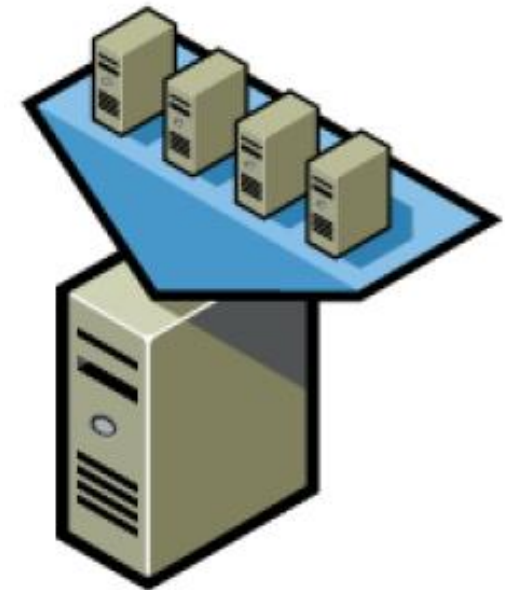
Toks sprendimas leidžia spręsti visas anksčiau minėtas problemas.

Galimi VM darbo režimai:

- Fizinio procesoriaus ISA **sutampa** su VM ISA
 - x86 procesoriuje leidžiama VM su MS Windows, Linux, OpenSolaris (x86)
- Fizinio procesoriaus ISA **nesutampa** su VM ISA (naudojama ISA emuliacija)
 - Pavyzdžiui IBM Power procesoriuje leidžiame VM su AIX, x86 OS, ARM procesoriaus OS (Android, Chrome OS)

[Kas yra virtualizacija?]

- **Virtualizacija** – tai technologija, leidžianti kompiuterio aparatūrinę dalį pateikti kaip programinę įrangą.
- **Virtualizacija** sudaro galimybę keletai operacinių sistemų veikti vienu metu viename kompiuteryje.
- Kiekviena operacinė sistema yra individuali ir veikia lyg būtų instaliuota atskirame fiziniame kompiuteryje.



[Kas yra virtuali mašina?]

- **Virtuali mašina** – tai programa, kurioje lyg fiziniame kompiuteryje, instaliuojama operacinė sistema ir vartotojų programos.
- Fiziškai virtuali mašina yra tik failų rinkinys:
 - Konfigūracinis failas
 - Virtualus kietojo disko failas
 - Atminties failas
 - Tarnybinių įrašų failas



[Virtualizacijos technologijos]

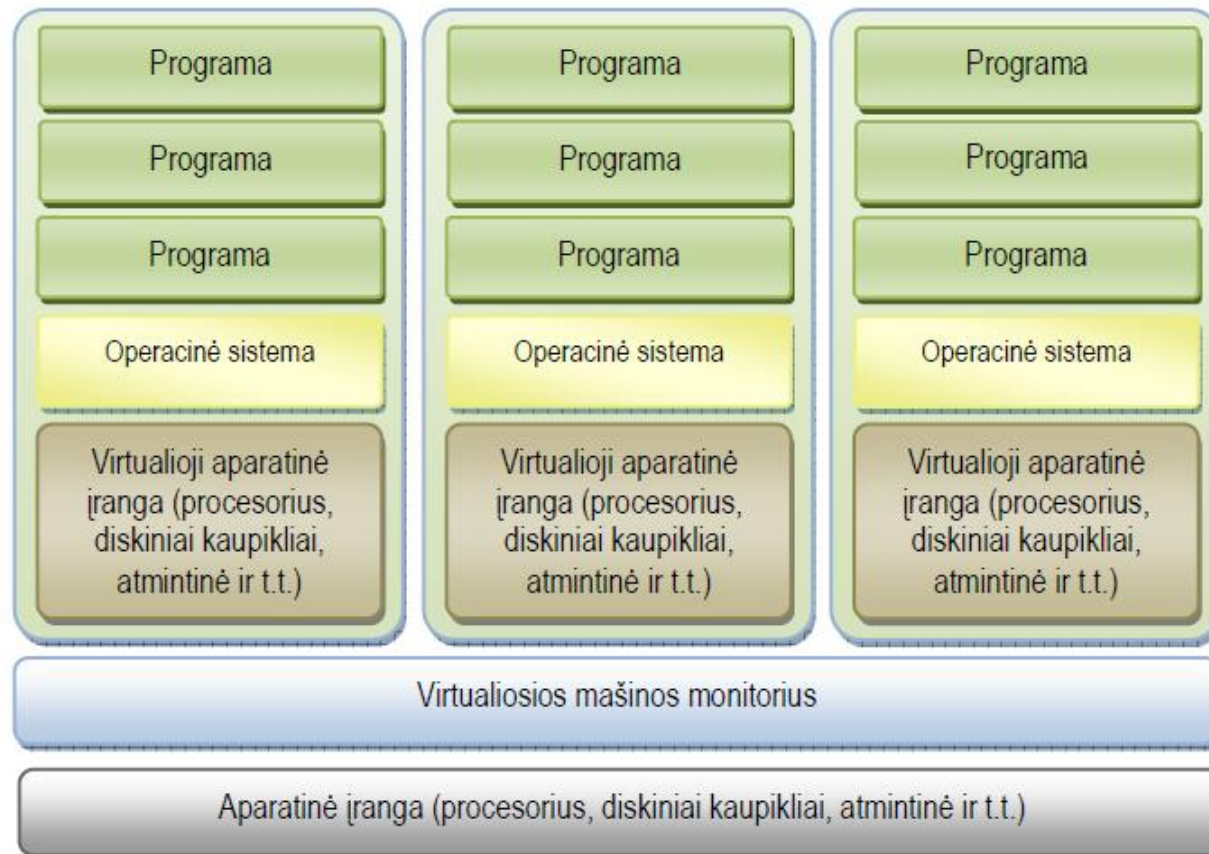
Virtualizacijos technologijos skiriamos į tris grupes:

- **Resursų virtualizacija**, kai sujungiama arba atskiriama tik tam tikra kompiuterinės įrangos dalis (kietieji diskai, tinklo plokštės)
- **Platformų virtualizacija** – tai technologija, kuomet atskiriama operacinė sistema nuo aparatūrinės kompiuterio dalies ją simuliuojant.
- **Programų virtualizacija** – tai technologija, kai programos vykdymas tampa nepriklausomas nuo aplinkos, kurioje ji vykdoma.

Platformų virtualizaciją dar skirstoma:

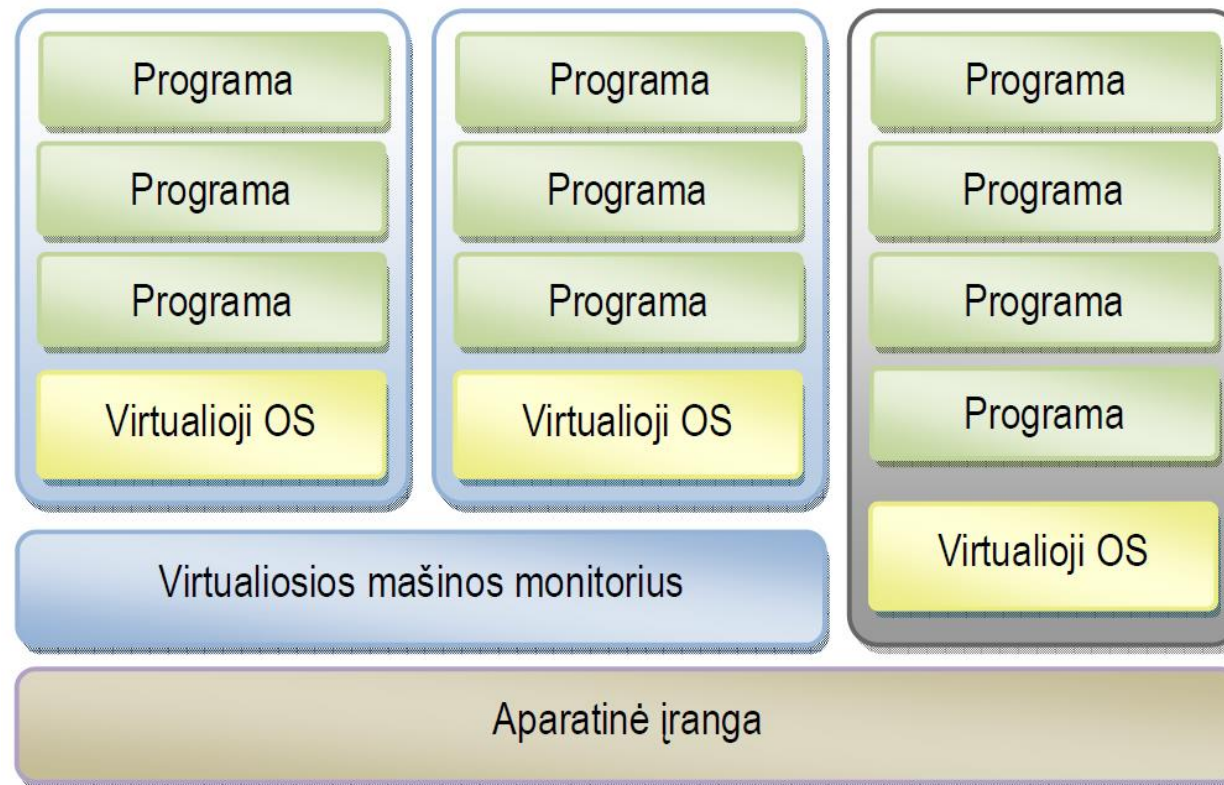
- Aparatinės įrangos imitavimas
- Visiška virtualizacija
- Paravirtualizacija
- Operacinės sistemos lygmens virtualizacija

[Visiška virtualizacija]



Visiška virtualizacija vadinama tokia virtualizacijos technologija, kai specialus **virtualios mašinos monitorius** (*hypervisor*) pateikia virtualioms mašinoms priėjimą prie kompiuterio aparatūrinės įrangos.

[Visiška virtualizacija su COS]



Visiška virtualizacija su konsolės operacine sistema (COS).

COS dalinasi taip pačiais aparatiniais resursais kaip ir hipervisorius => :
dviejų 2 OS branduoliai dalinasi aparatūriniais resursais. Pvz. Hyper-V

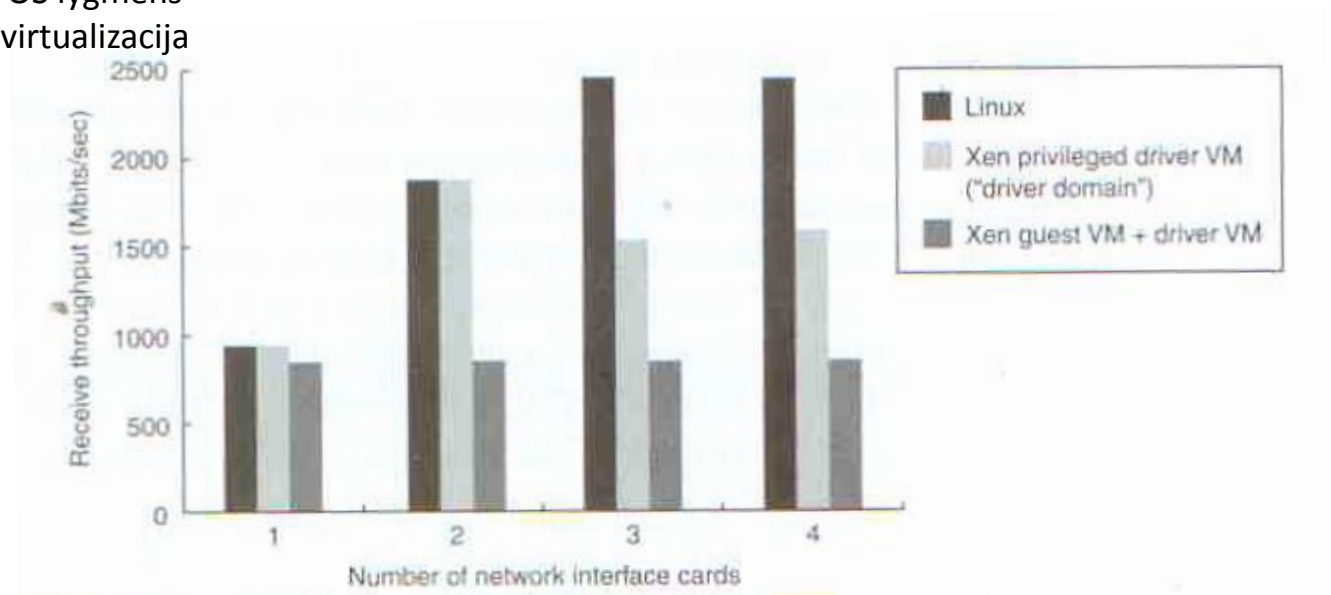
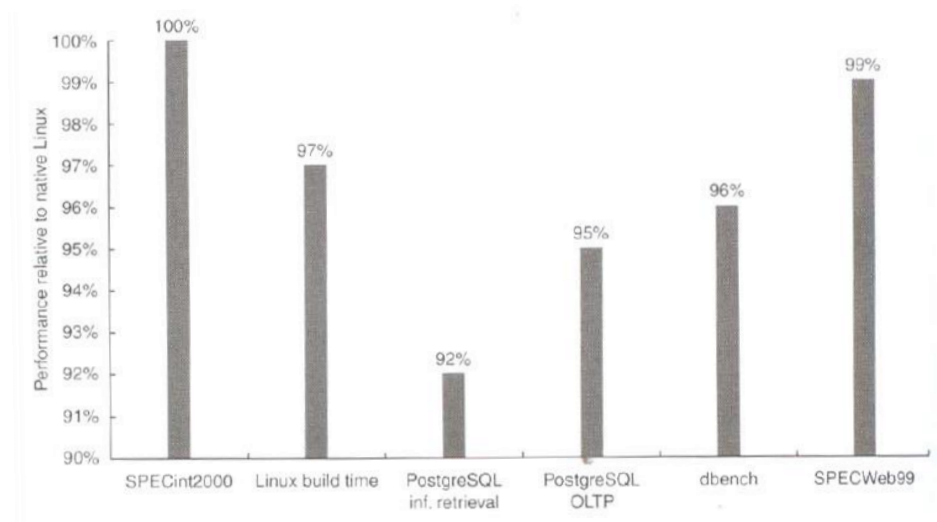
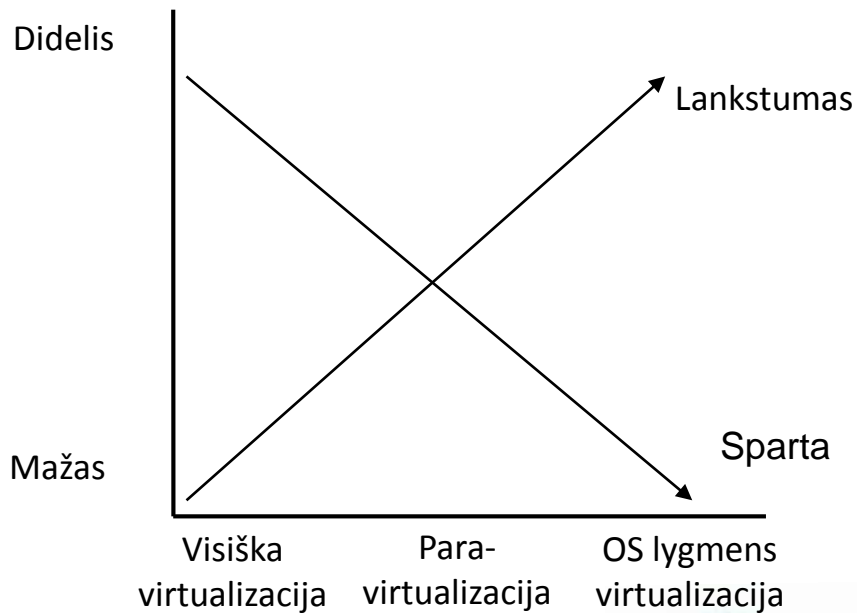
OS lygmens virtualizacija



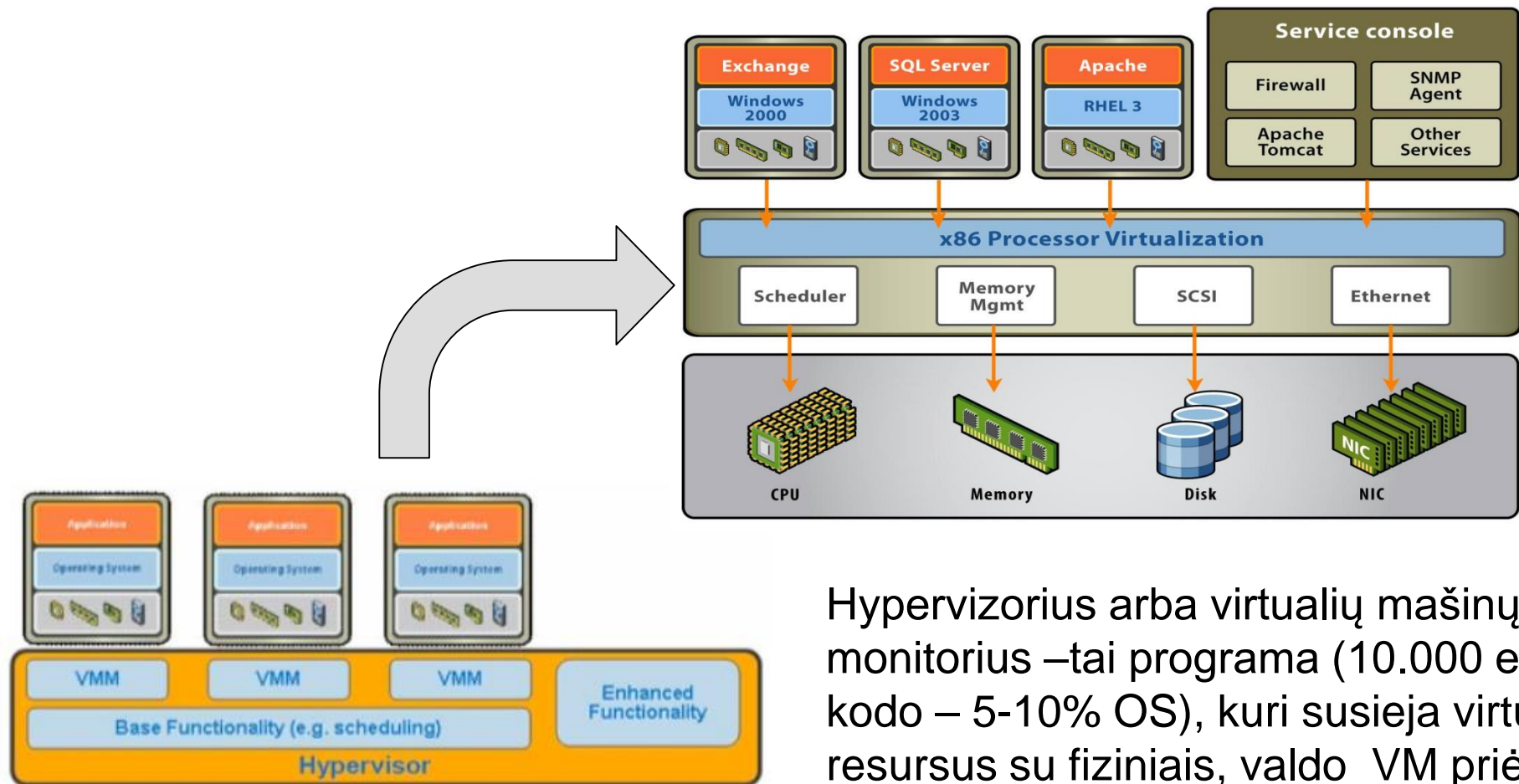
Operacinės sistemos lygmens virtualizacija – tai virtualizacijos sprendimas, kai virtualių mašinų monitorius instaliuojamas jau egzistuojančioje operacinėje sistemoje (Windows, Linux) ir veikia kaip atskira programa. Pavyzdžiui:

- VMware Server, VMware Workstation, VMware Player
- Microsoft virtual PC
- SUN (Oracle) xVM VirtualBOX

Virtualizacijos naudojimas



[Hypervizorius]



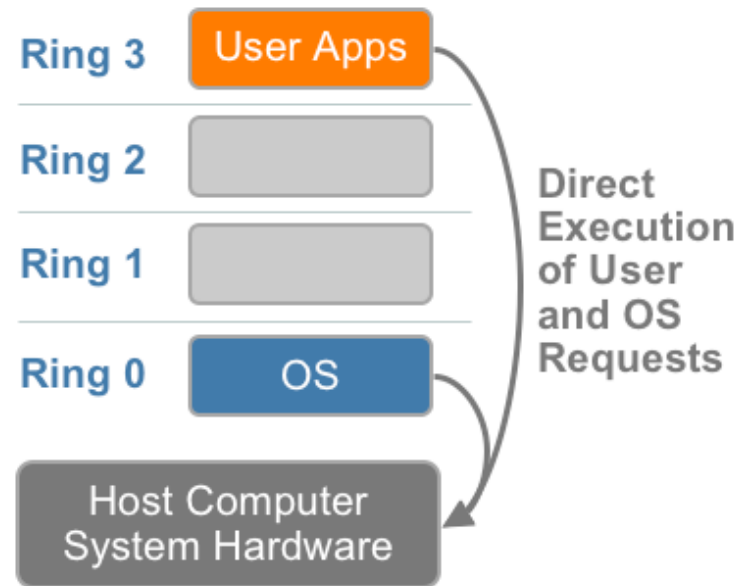
Hypervizorius arba virtualių mašinų monitorius –tai programa (10.000 eilučių kodo – 5-10% OS), kuri susieja virtualius resursus su fiziniais, valdo VM priėjimą prie fizinių resursų *time-shared*, *partitioned* ar emuliacijos principu.

[Hypervisorius (VMM)]

VMM atliekamos funkcijos:

- Pateikia virtualius aparatinius resursus VM'ams ir juos valdo
- Kontroliuoja VM priėjimo privilegijų režimus prie CPU
- Izoluoja VM vieną nuo kito
- Vykdo fizinių resursų monitoringą

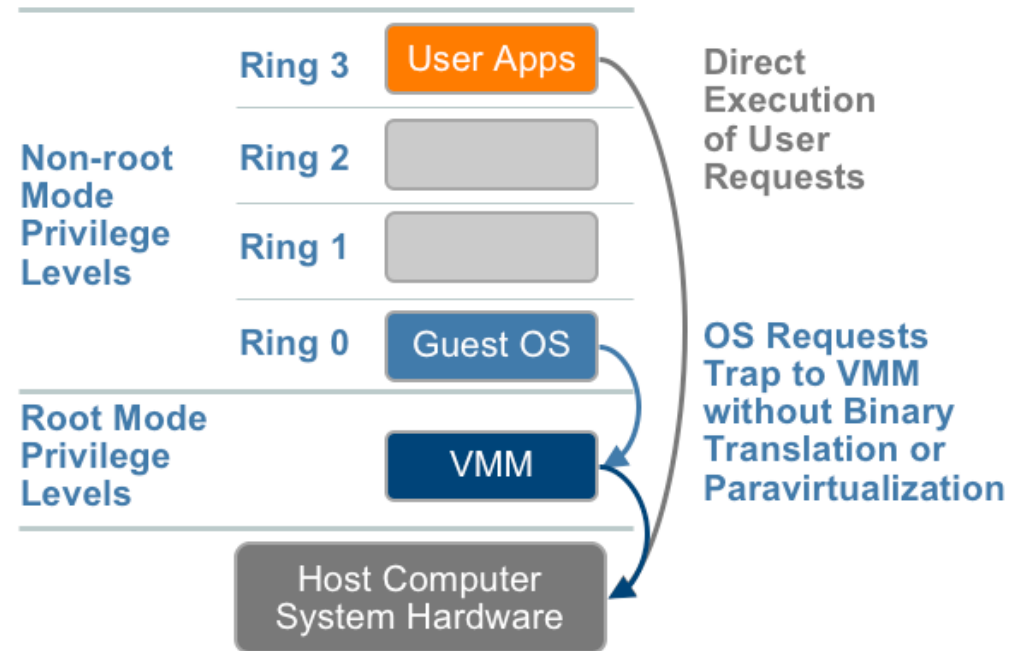
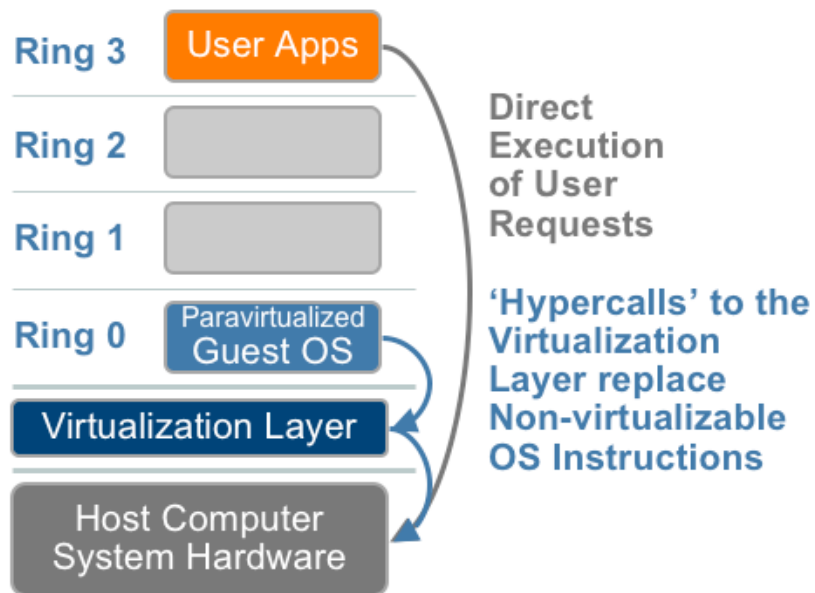
[Procesoriaus x86 virtualizacija]



x86 ISA procesoriuose naudojamos technologijos, palaikančios aparatinę virtualizaciją:

- Intel VT (Intel Virtualization technology)
- AMD-V (AMD virtualization)

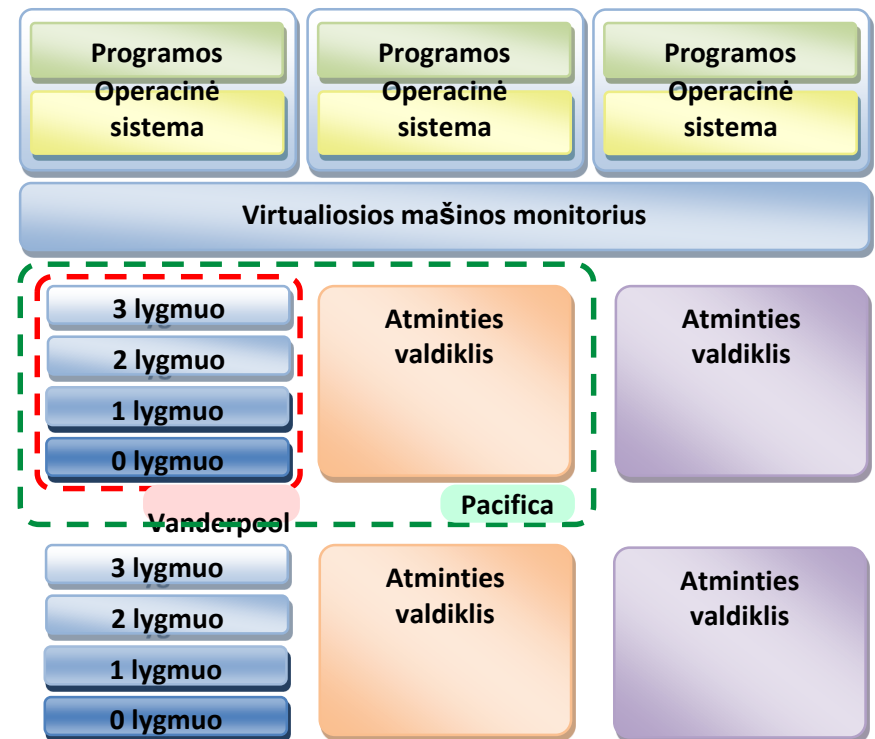
[Procesoriaus x86 virtualizacija]



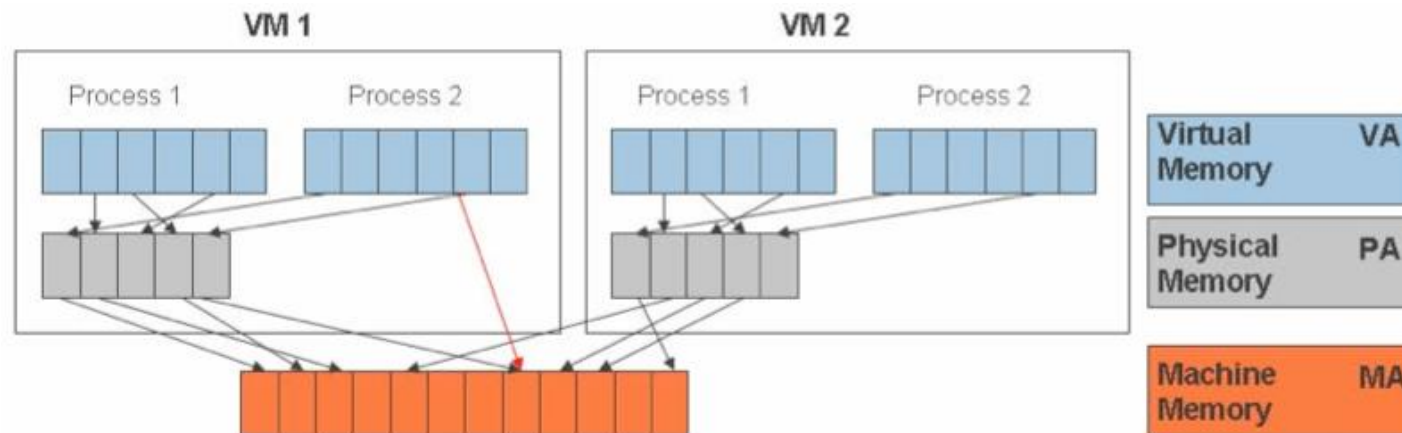
[CPU virtualizacijos palaikymas]

VM programinė įranga palaikanti „Intel VT“ ir AMD-V“ technologijas:

- Kernel-based Virtual Machine (KVM)
- Microsoft Virtual PC
- Microsoft Server 2008 Hyper-V
- Parallels Workstation
- Sun VirtualBox
- Virtual Iron
- VMware Workstation, ESX, Server
- Xen



[Atminties virtualizacija]



Atminties virtualizacija turi užtikrinti bendrą fizinės ir dinaminės atminties naudojimą VM. Virtualios atminties išskyrimas VM, primena virtualios atminties naudojimą įprastoje oper. sistemoje. t.y.

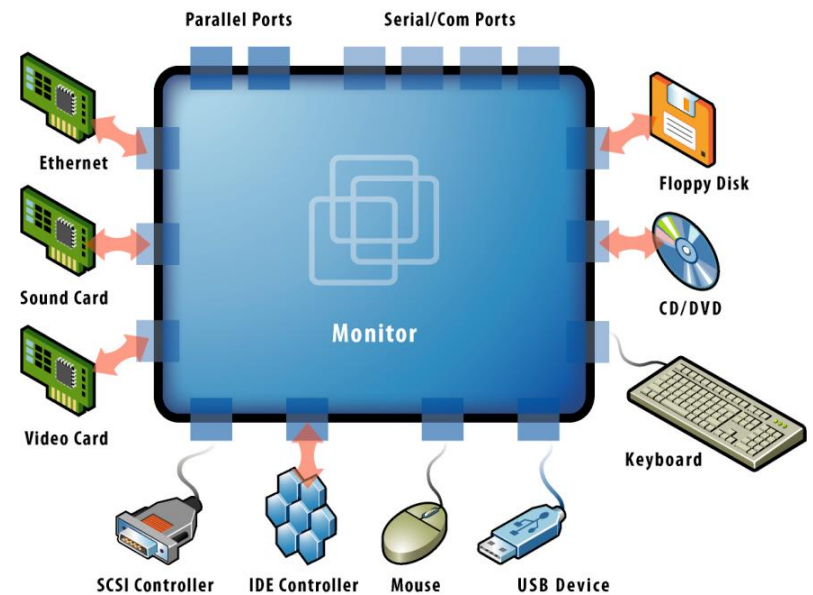
Aplikacijos mato atminties adresus, kurie nebūtinai susiję su fizine atmintimi. Sąryšis užtikrina OS lygyje.

x86 CPU turi *memory management unit* (MMU) ir *translation lookaside buffer* (TBL) priėjimui prie atminties optimizuoti.

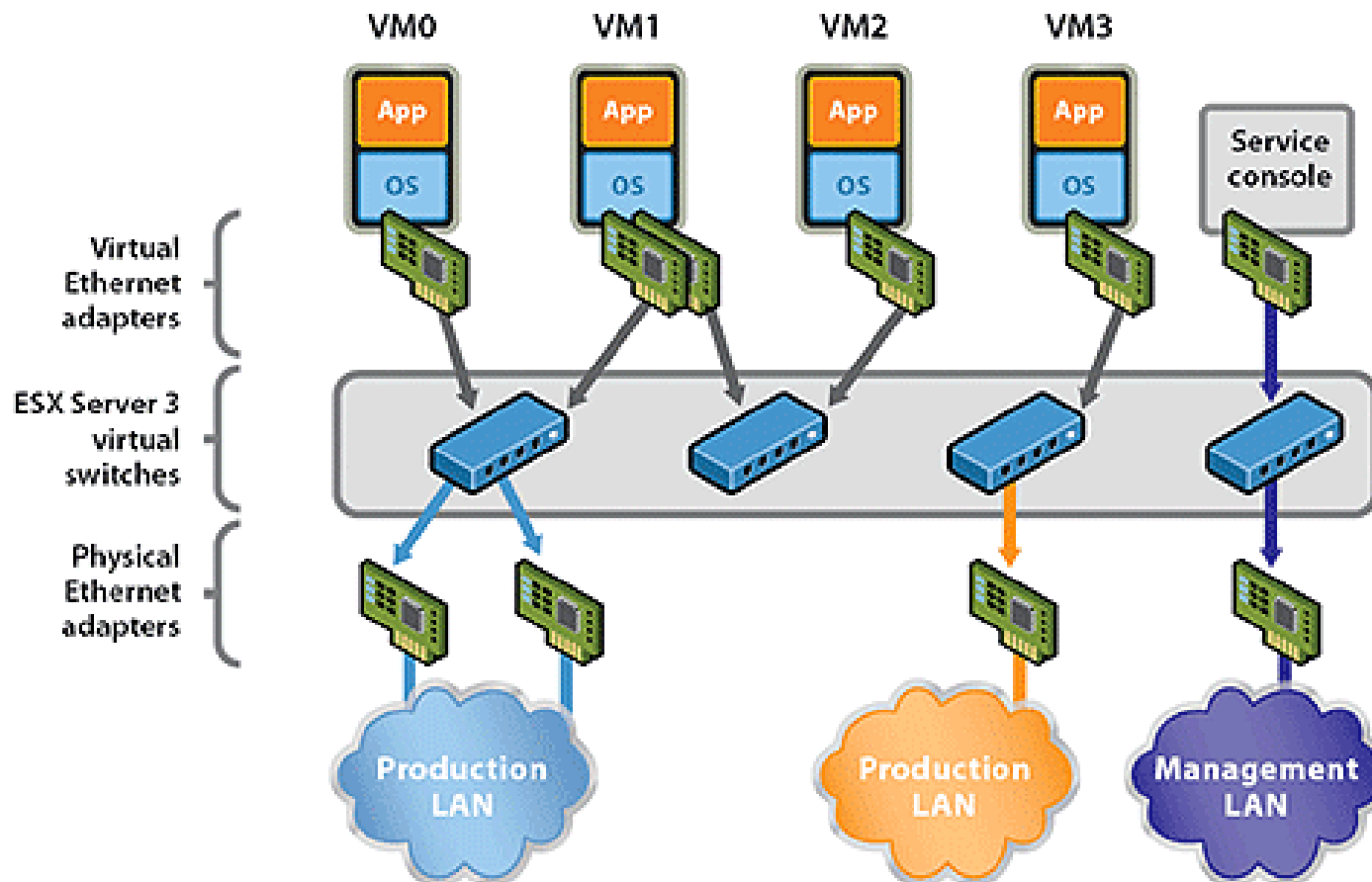
[I/O ir įrenginių virtualizacija]

VMM pateikia VM standartinius virtualius įrenginius juos emuliuojant.

Toks principas suteikia galimybę VM naudotis keliais virtualiais įrenginiais, realizuoti tinklus tarp VM naudojant virtualius NIC ir komutatorius, fiziškai nenaudojant fizinio įrenginio.



Virtualus tinklas



[Virtualus tinklas]

- VM susietos su išoriniu tinklu per virtualų komutatorių, kuris imituoja tradicinį fizinį Ethernet tinklo komutatorių, dirbantį duomenų perdavimo **kanalo sluoksnyje L2**.
- Hipervizorius palaiko keletą virtualių komutatorių, turinčių iki 1000 portų (pvz. ESX, 248 vkomutatorius).
- Dažniausiai hipervizorius palaiko kelias dešimtis fizinių tinklo portų (pvz. 24 portus, ESX).
- Virtualus tinklo komutatorius gali sujungti keletą vNIC kartu sudarydamas jų grupę (agregaciją, NIC teaming), taip padidindamas VM tinklo pralaidumą.

[Virtualus komutatorius]

- vKomutatoriai kuriami realiuoju laiku ir palaiko:
 - 2 lygmens persiuntimus (forwarding)
 - VLAN segmentavimą portų lygmenyje ir filtravimą
 - 2 lygmens saugumą, kontrolines sumas (checksum) and segmentavimo nukrovimą.
- Savybės:
 - Nesidalina ARP lentelėmis. Tai padeda sumažinti Denial of Service atakos.
 - Daro siunčiamų paketų kopiją, ją analizuoja ir priimama sprendimus dėl filtravimo.
 - vKomutatorių topologija išvengia kaskadavimo problemų.

[Virtualizacijos privalumai]

Lankstumas. Viename fiziniame kompiuteryje gali veikti daugiau nei viena skirtingos architektūros operacinė sistema. Tokią virtualizuotą instanciją galima lengvai perkelti iš vieno klasterio mazgo į kitą ir keisti jos aparatinę įrangą (operatyviosios atminties kiekį, standžiojo disko talpą ir kt.) nesustabdant pačios virtualiosios mašinos.

Pasiekiamumas. VM gali išlikti pasiekiamos ir veiksnius net ir išjungus fizinį klasterio mazgą (pavyzdžiui, aparatinės įrangos keitimo arba taisymo atveju). Paslaugos lieka pasiekiamos, kadangi jas galima laikinai perkelti į kitą veikiančią tarnybinę stotį ir vėl sugrąžinti į sutvarkytą senąją. Šis privalumas leidžia tvarkyti fizinių klasterių mazgų aparatinę įrangą nestabdant pačių paslaugų.

[Virtualizacijos privalumai]

Plečiamumas. Padidėjus aparatinės įrangos išteklių poreikiui, labai paprastai galima į klasterį įdiegti naujus mazgus, panaudojant tik nesudėtingą klasterio valdymo PĮ konfigūravimą ir paleidžiant virtualiąsias mašinas, teikiančias atitinkamas paslaugas. Šiuo atveju klasteris gali lengvai plėstis pagal organizacijos poreikius.

Aparatinės įrangos panaudojimas. Kelios virtualiosios mašinos viename fiziniame klasterio mazge žymiai geriau panaudoja jo aparatinės įrangos resursus, nei viena OS tame pačiame mazge. Tai yra todėl, kad virtualioji mašina išnaudoja „*idle*“ išteklius.

Saugumas. Visas teikiamas paslaugas galima išskirstyti skirtingoms virtualiosioms mašinoms. Šis procesas dar kartais vadinamas „izoliavimu“. Jei viena paslauga taptų pažeidžiama, kitos išliktų saugios.

[Virtualizacijos privalumai]

Laikas

Laikas, sugaištamasis virtualiam serveriui pateikti labai mažas, lyginant su laiku, fiziniam serveriui pateikti ir paruošti (1-3 mėn.).

Trūkumai

- Hypervizorius naudoja 10 - 15 % resursų (overhead)
- Stipriai padidėja VM poreikis, nes lengva gauti

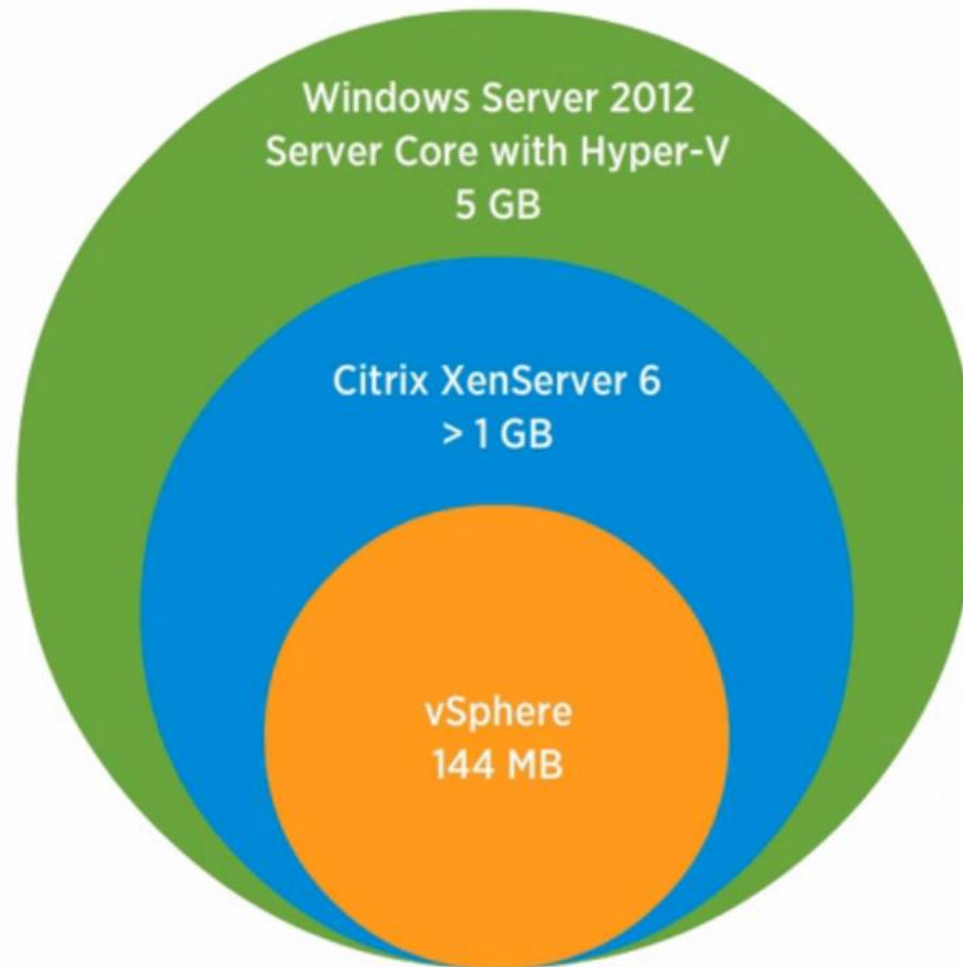
Virtualizacijos sprendimai (x86)

Resursų virtualizacijos programinė įranga x86 procesoriams

- VMware ESXi
- MS Server Hyper-V
- Citrix XenServer
- KVM
- Oracle VirtualBox
- Vmware Workstation, Player



Hypervisorių palyginimas

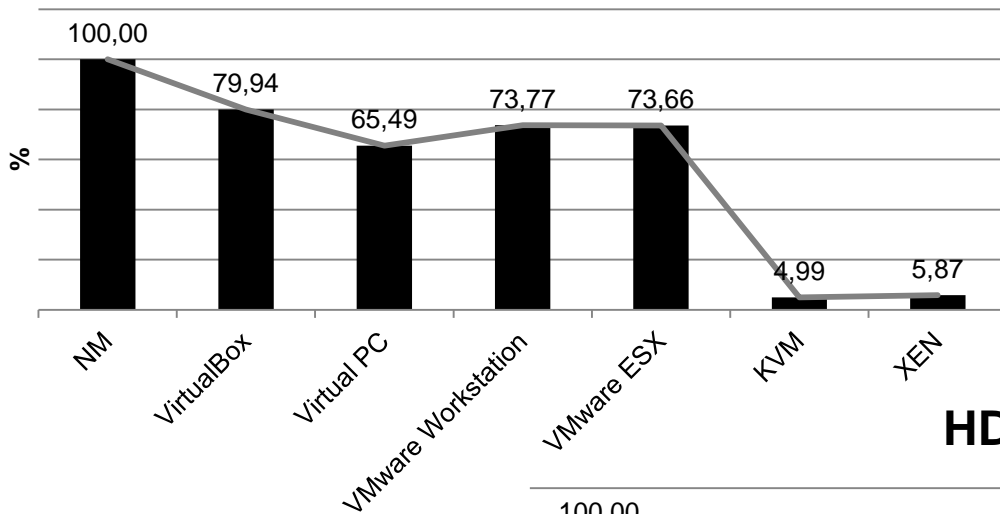


Funkcionalumo lyginimas

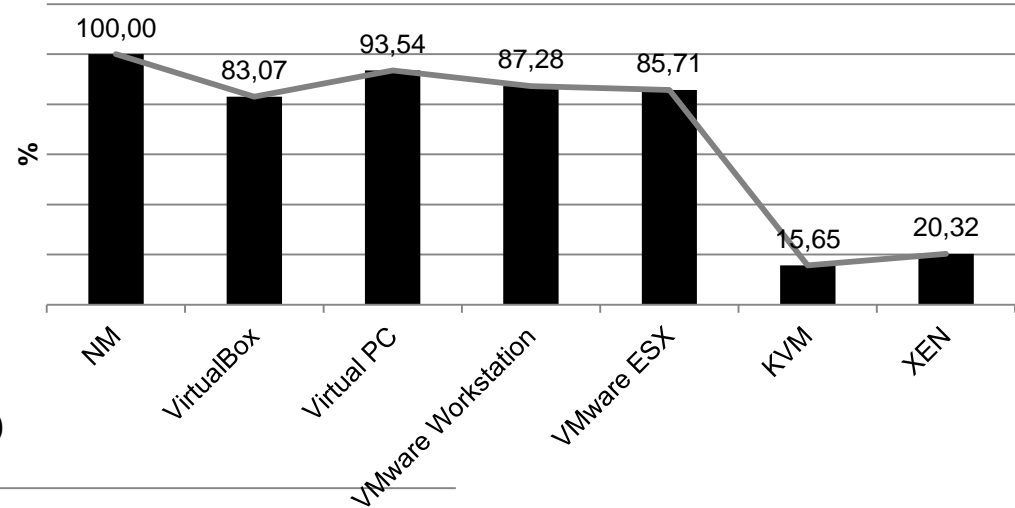
	Windows	LINUX	MacOS	Nuotolinis valdymas	Daugiau nei 1 VM	Nemokamas produktas	32bit sistemos palaikymas	64bit sistemos palaikymas	Video 3D palaikymas	Linux NTFS	Pilnas suderinamumas visose byly sistemose	Daugiakalbė aplinka	USB 2.0 palaikymas	CPU Hot-plug	Valdymas per Virt-manager	Vartotojo sąsaja lietuvių kalba
VMware Workstation	X	X			X	X	X	X	X		X	X	X			
VMware ESX		X		X	X		X	X								
Virtual Box	X	X			X	X	X	X	X	X	X	X	X			
VirtualPC	X		X		X	X	X	X	X			X	X			
XEN		X			X	X	X	X		X				X	X	
KVM		X			X	X	X			X					X	

VM testavimo rezultatai

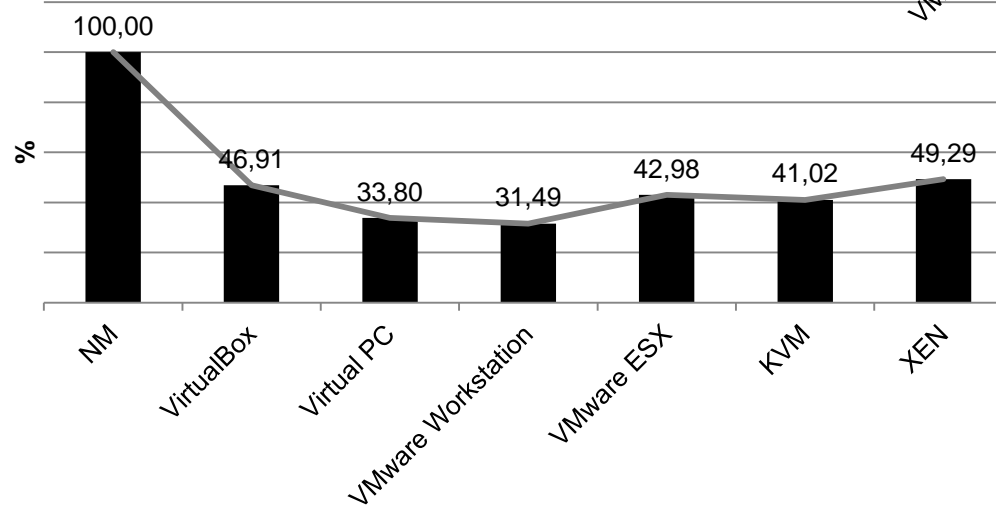
CPU



RAM



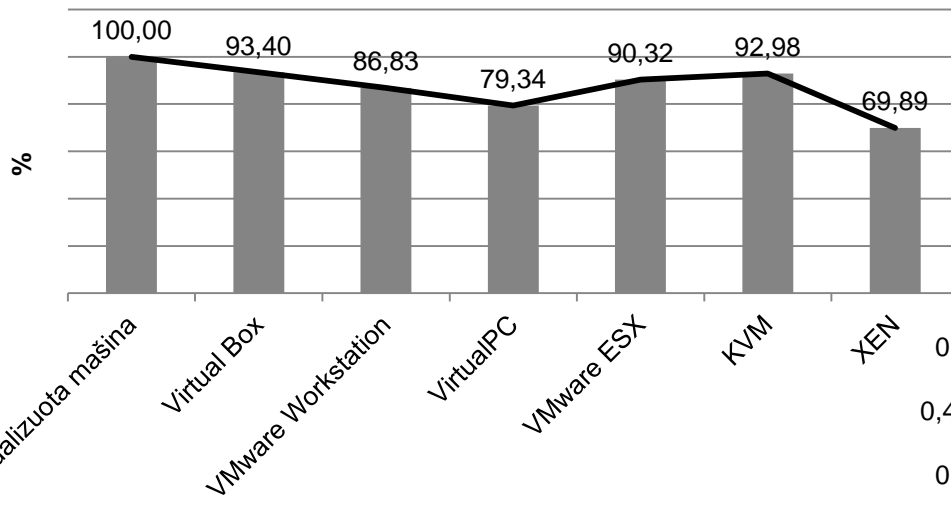
HDD



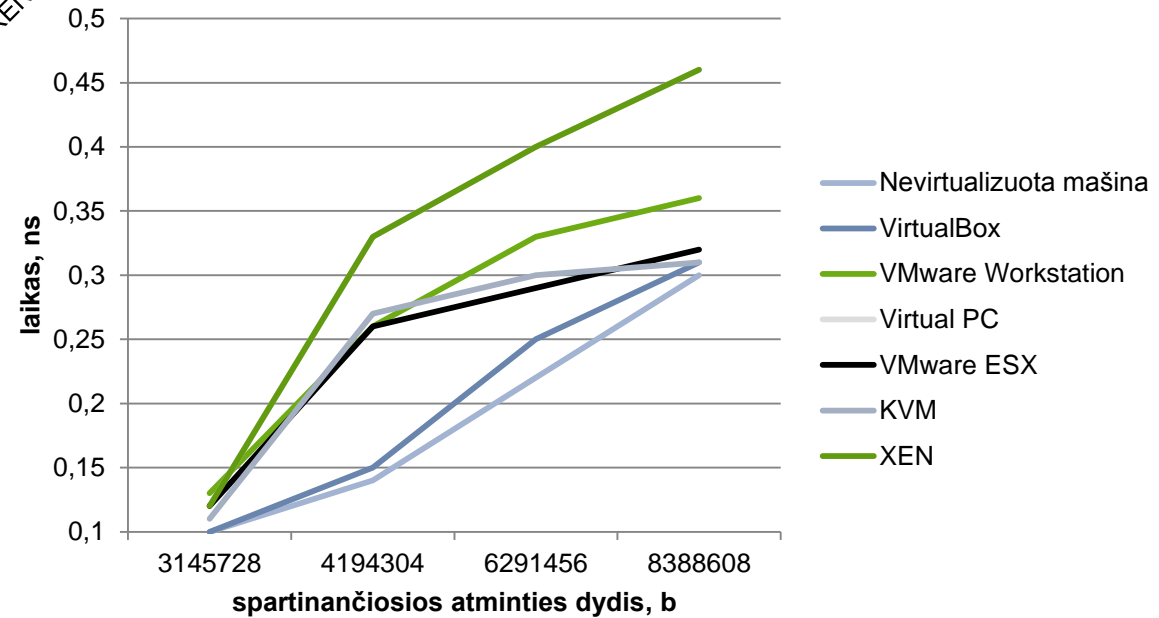
VM operacinė sistema: Windows XP

VM testavimo rezultatai

CPU



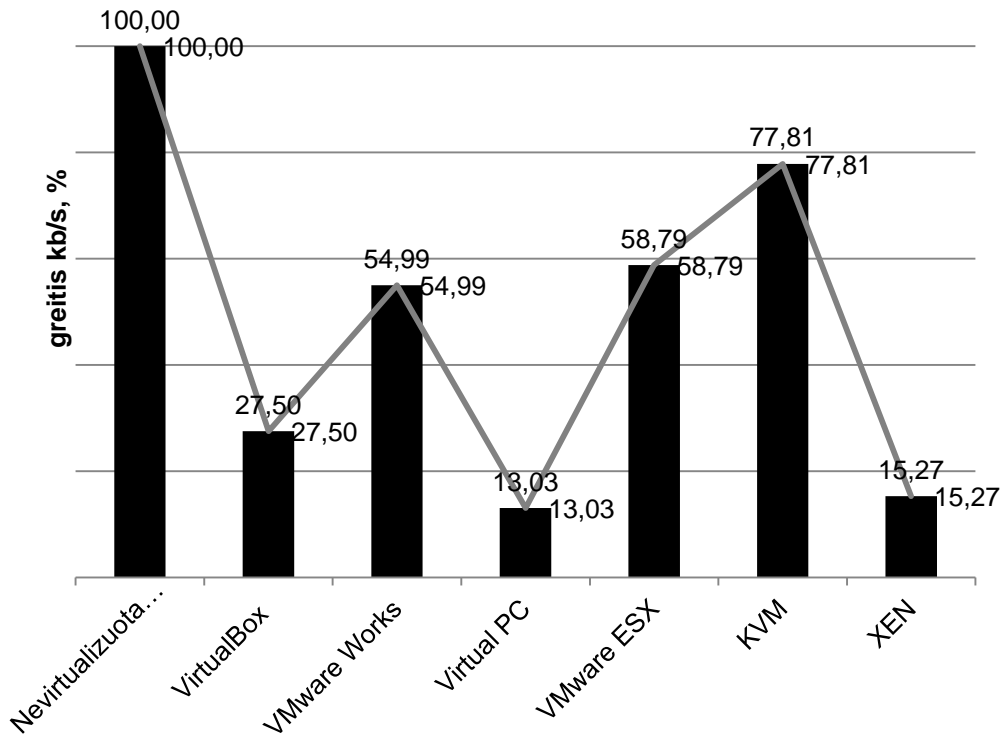
Atminties priskyrimas



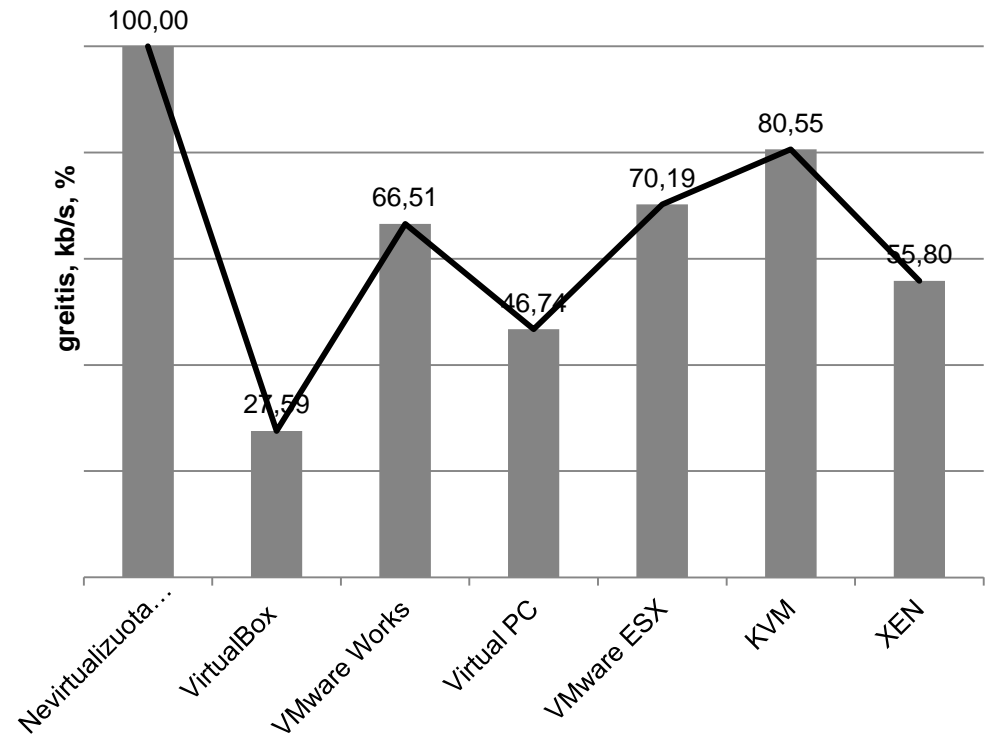
VM operacinė sistema Linux Ubuntu

VM testavimo rezultatai

VM rašymo rezultatai



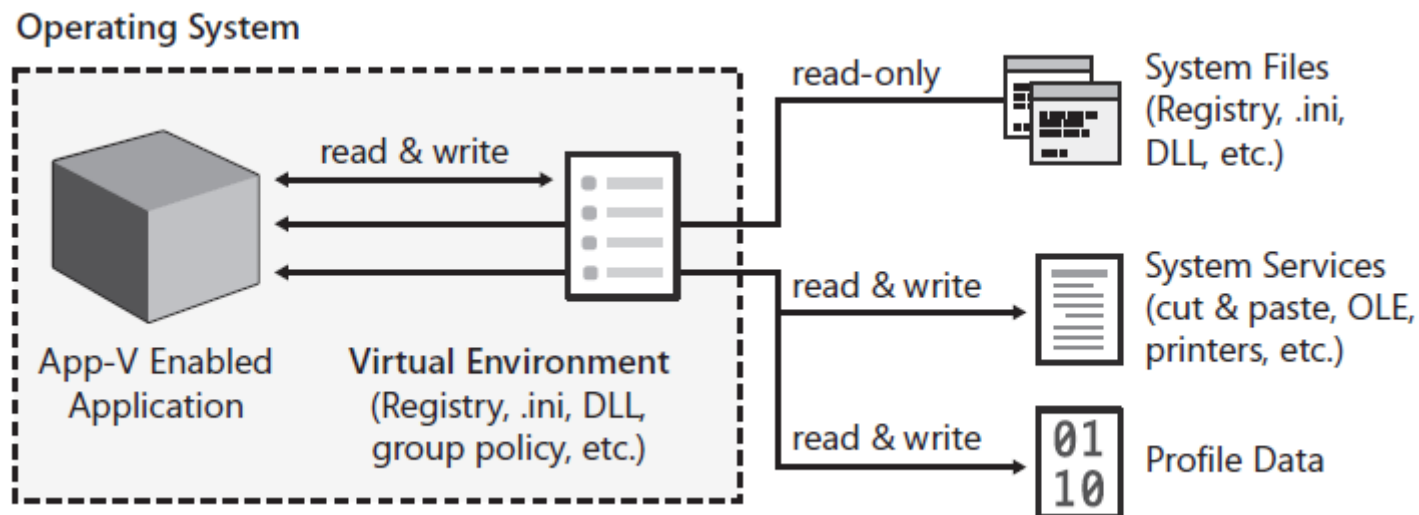
VM skaitymo rezultatai



VM operacinė sistema Linux Ubuntu (HDD skaitymo/rašymo testas)

[Programų virtualizacija]

Programų virtualizacija – tai virtualizacijos technologija, kuri inkapsuliuoja programos failus ir registrus į vieną paketą, kuris gali būti diegiamas, valdomas, atnaujinams nepriklausomai nuo operacinės sistemos. Virtualizuota programa nedaro jokios įtakos operacinei sistemai, o susikuria savo aplinką “sandbox”, kurioje ji dirba.



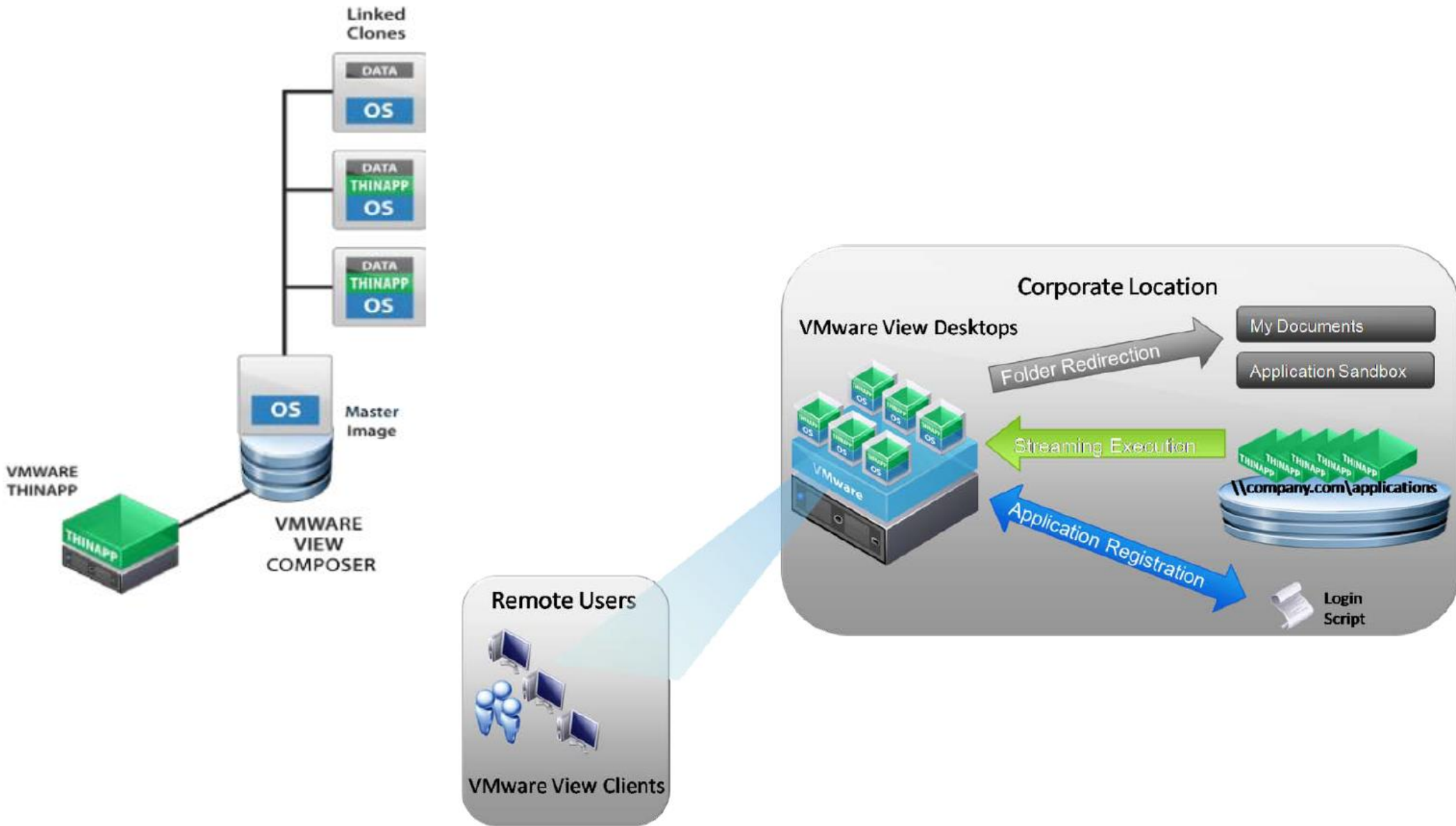
[Virtuali programų aplinka]

Virtuali programų vykdymo aplinka – tai *runtime* konteineris, kuris nustato kokius resursus prieinami programoms, paleidžiamoms iš paketų.

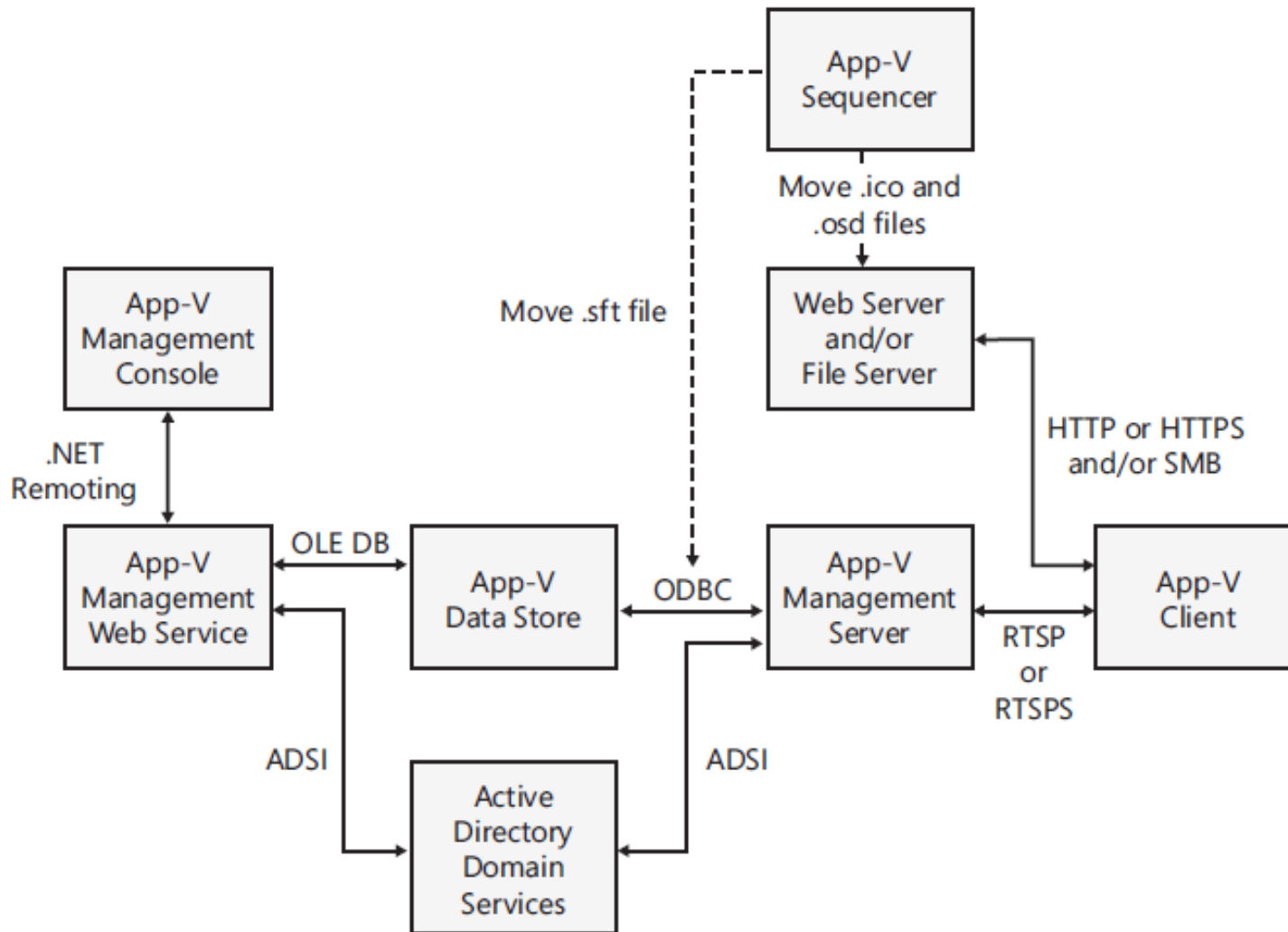
Resursai apima:

- Virtualią direktoriją
- Virtualius failus
- Virtualią failų sistemą
- Virtualų registrą
- Virtualius servisus

VMware ThinApp



Microsoft App-V



[Linux konteineriai]

Linux Containers - tai OS lygmens virtualizacija, skirta Linux sistemų izoliavimui (konteineriavimui) vienoje Linux fizinėje mašinoje.

Linux branduolys pateikia funkcionalumą, leidžiantį riboti ir prioritizuoti resursus (CPU, atmintis, block I/O, tinklas) be hypervizoriaus ir VM. Vardų erdvės izoliavimas leidžia pilnai izoliuoti programų sistemas ir jų aplinką įskaitant procesų medį, tinklą, vartotojus, failines sistemas.

Daugelis konteinerių dalinasi tuo pačiu Linux branduoliu, bet kiekvienam konteineriui galima apriboti resursų naudojimą CPU, RAM I/O.

Pagrindinis privalumas – programų izoliavimas be resursų švaistymo virtualizacijos sluoskniui (no overhead).

[OpenVZ]

- OpenVZ sukuria keletą saugių, izoliuotų Linux konteinerių grupę (virtualių privačių serverių, VPS).
- Kiekvienas konteineris veikia taip, lyg veiktų atskira operacinė sistema.
- Konteineris turi savo naudotojus, IP adresus, atmintį, procesus, failus, aplikacijas, sistemines bibliotekas bei konfigūracijos failus, tačiau realiai veikia tik vienas operacinės sistemos branduolys, kuriuo dalijasi OS šeimininkė su konteineriais – svečiais.
- Konteinerio tinklo srautas yra izoliuotas nuo kitų konteinerių o taip pat ir nuo fizinio tinklo adapterio. Konteineryje yra ugniasienės ir atskiros jų konfigūracijos.

[OpenVZ]

Virtualus diskas

- Fizinio serverio administratorius nustato kietojo disko kvotas kiekvienam virtualiam konteineriui.
- Konteinerio administratorius gali nustatyti standartines disko kvotas taip, kaip jos yra nustatomos UNIX sistemose (naudotojų bei grupių disko sunaudojimo kvotos).
- Jeigu yra poreikis skirti daugiau vietos konteineriui, tiesiog yra padidinama kvota, nereikia didinti disko skirsnio (angl. partition).

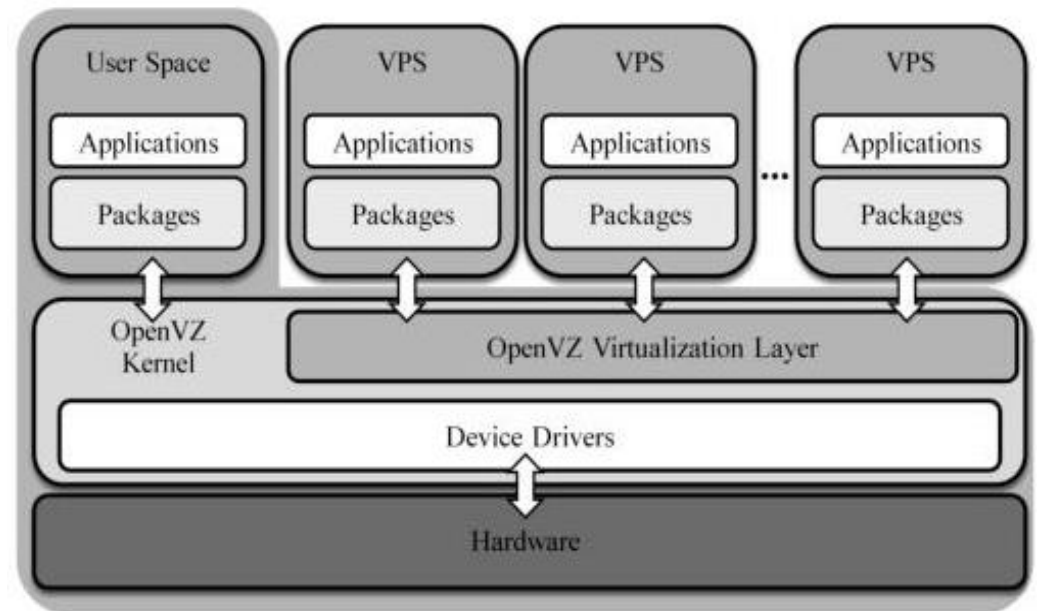
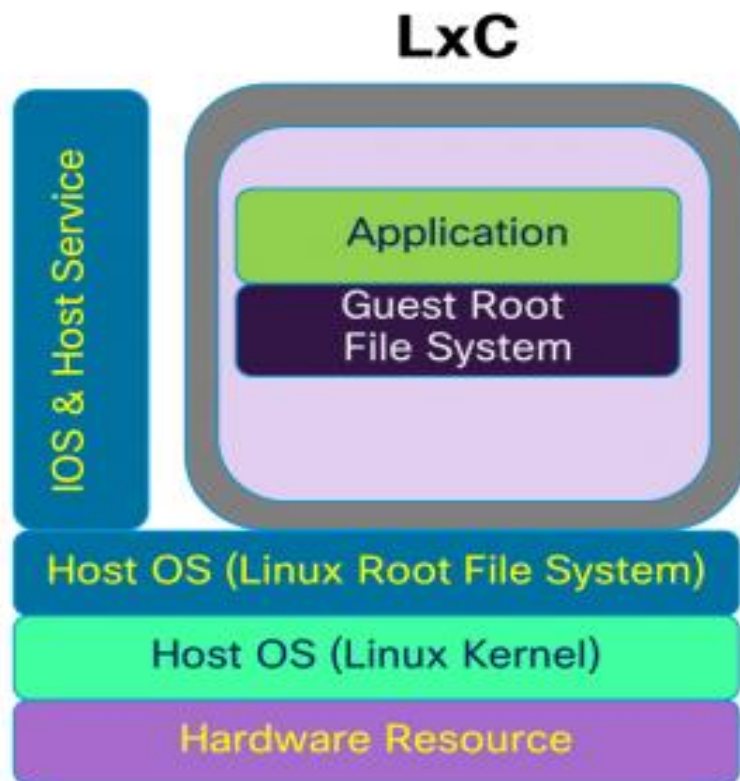
[LXC

LXC sukuria kuo labiau panašią aplinką standartinei Linux aplinkai be reikalavimo atskirti OS branduolius, t.y. laikomasi konteineriavimo principo ir visi LXC konteineriai veikia viename OS šeimininkės branduolyje.

LXC privalumas tai, kad konteinerius galima grupuoti bei valdyti grupėmis, tai labai palengvina administratoriaus darbą, kadangi vietoje kiekvienos virtualios mašinos (konteinerio) savybių keitimo, galima keisti ir kitų panašių, ar tokių pačių konteinerių savybes.

Patogesniam konteinerių kūrimui valdymui yra sukurta API.

[OpenVZ ir LXC]



[Docker]

Docker – tai programų sistema, kuri automatizuoja aplikacijų diegimą konteineriuose, sudarydama papildomą abstrakcijos sluoksnį Linux OS.

Docker naudoja resursų izoliavimo funkcionalumus Linux OS t.y. cgroups ir branduolio namespace kurti konteinerius.

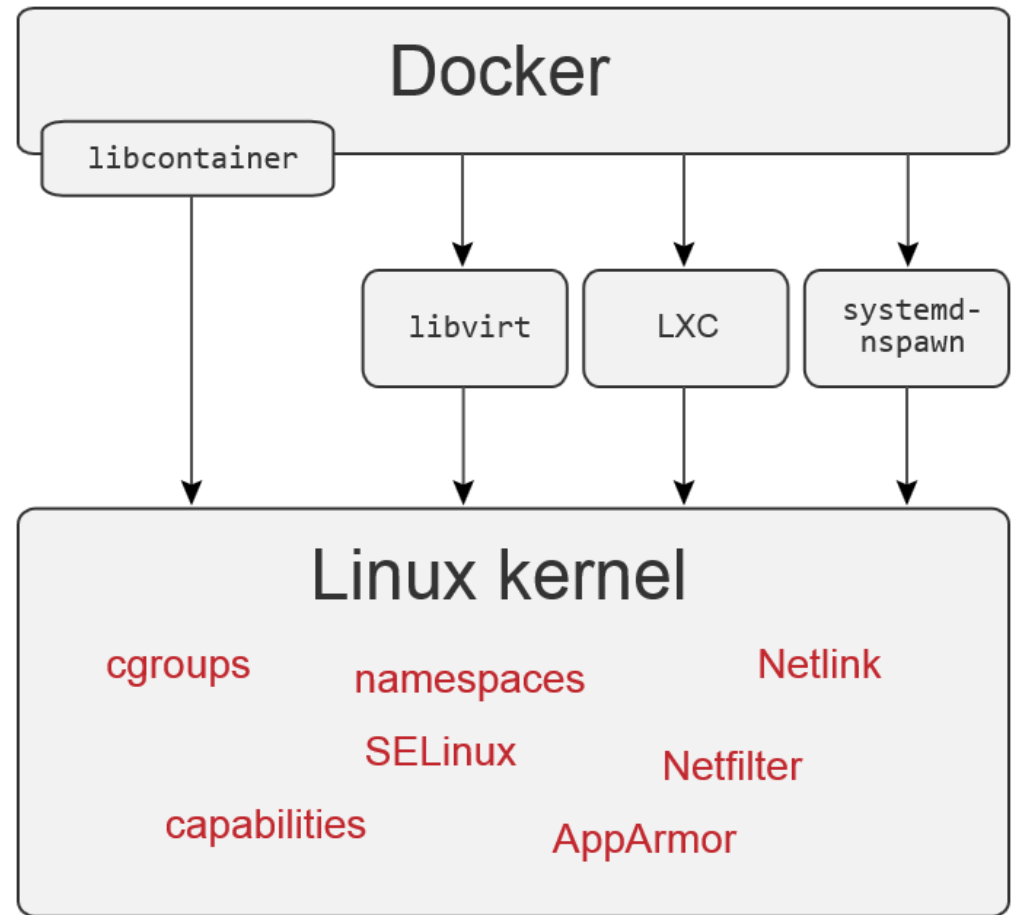
Docker sudaro **libcontainer** biblioteka, per kurią tiesiogiai naudojamos virtualizacijos savybės, palaikomos Linux branduolio. Taip pat naudojama **libvirt** (abstracted virtualization interface) virtualizacijos sluoksniui ir **LXC** (Linux Containers).

Pagrindinis privalumas – platus virtualizacijos platformų palaikymas (driverių kiekis).

[Docker]

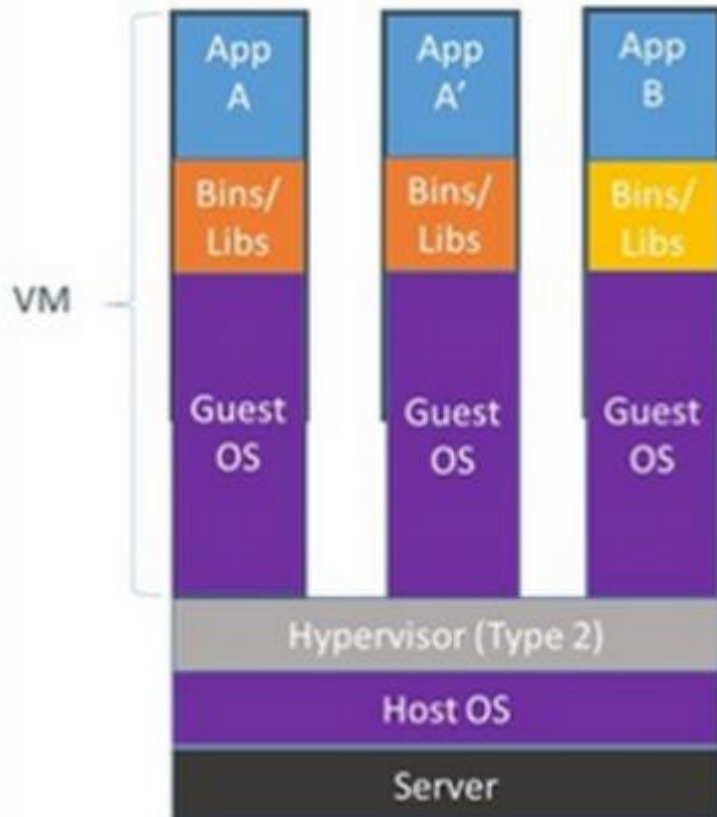
Docker integruojamas į įvairias tokias platformas:

- Amazon Web Services, Google Cloud Platform,
- IBM Bluemix,
- Microsoft Azure,
- OpenStack Nova,

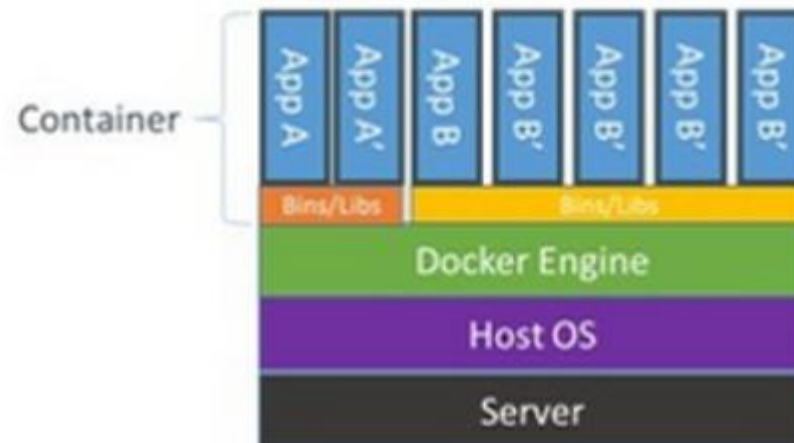


[Docker]

Containers vs. VMs



Containers are isolated, but share OS and, where appropriate, bins/libraries



[Debesų kompiuterija]

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. (*Wikipedia*)

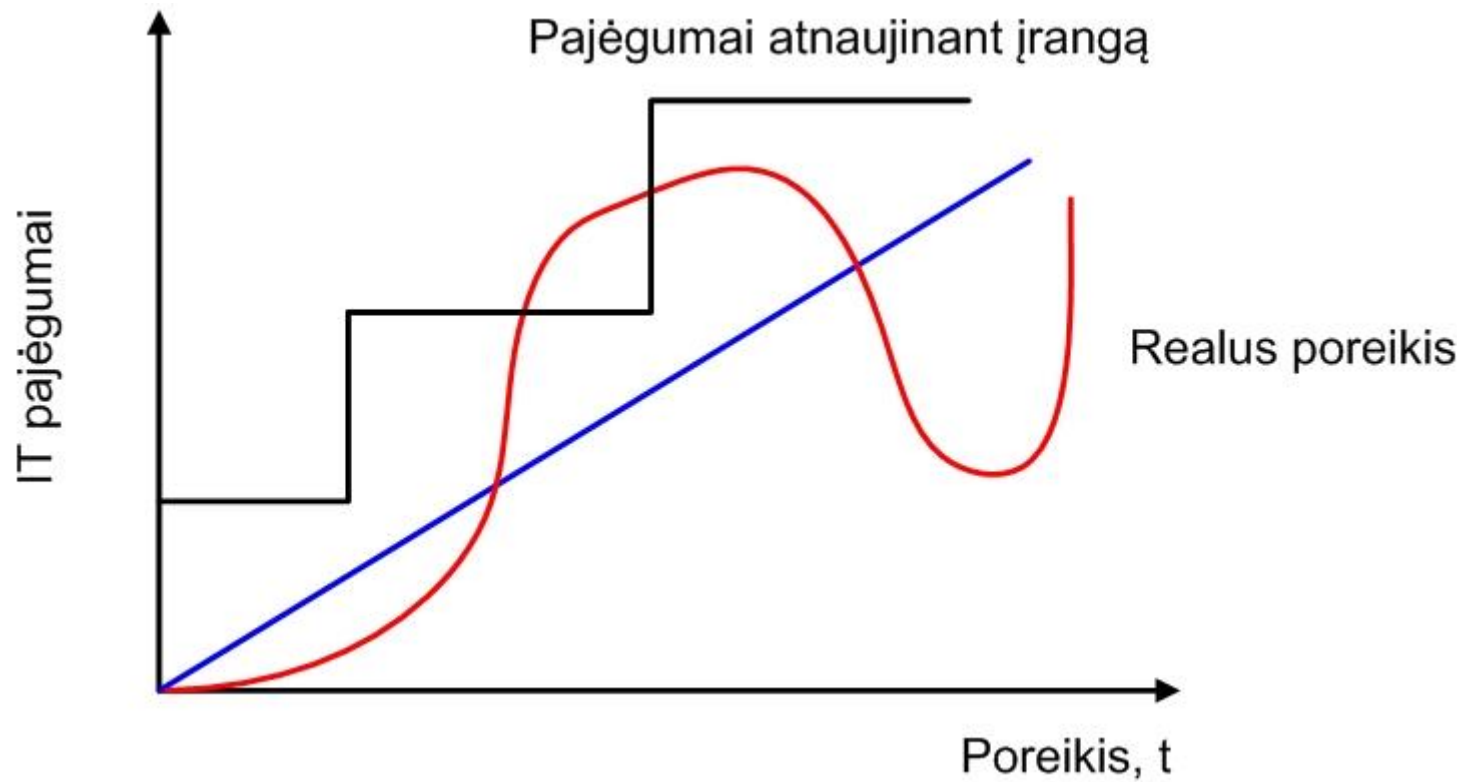
Debesų kompiuterija teikia paslaugas t.y.:

priėjimą prie bendro pobūdžio verslo aplikacijų ir skaičiavimo Resursų per web naršykles (pvz. Google Docs), kai programinė įranga ir duomenys saugomi serveryje.

Debesų kompiuterija resursų tipai:

- Privatūs (organizacijos ribose)
- Vieši (prieinami bet kuriam vartotojui)
- Mišrūs (organizacijos/privačių ir viešų resursų sąjunga)

[Infrastruktūros naudojimas]

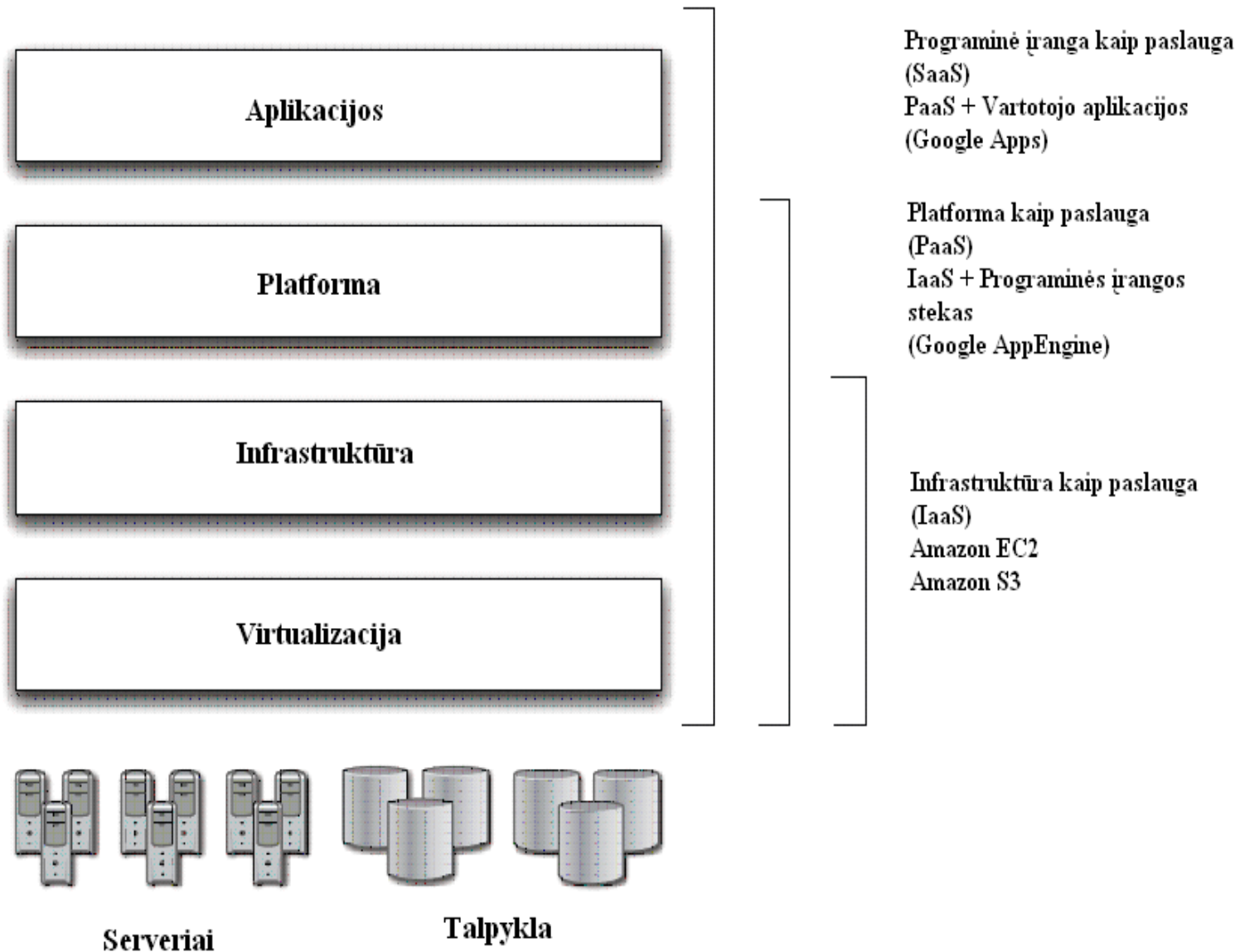


[Kada tikslinga naudoti debesis?]

Debesų kompiuteriją tikslinga naudoti kai:

- IT resursų poreikis yra nenuolatinis (naudojama – nenaudojama)
- IT resursai turi neperiodinius išaugančių pajėgumų pikus
- Cikliškai kinta IT resursų išaugančio pajėgumo poreikis
- Neprognozuojamas IT resursų augimo poreikis
- Norima greitai dinamiškai keisti serverių kiekį (testavimas)

Debesų kompiuterijos struktūra



Debesų kompiuterijos tiekėjai



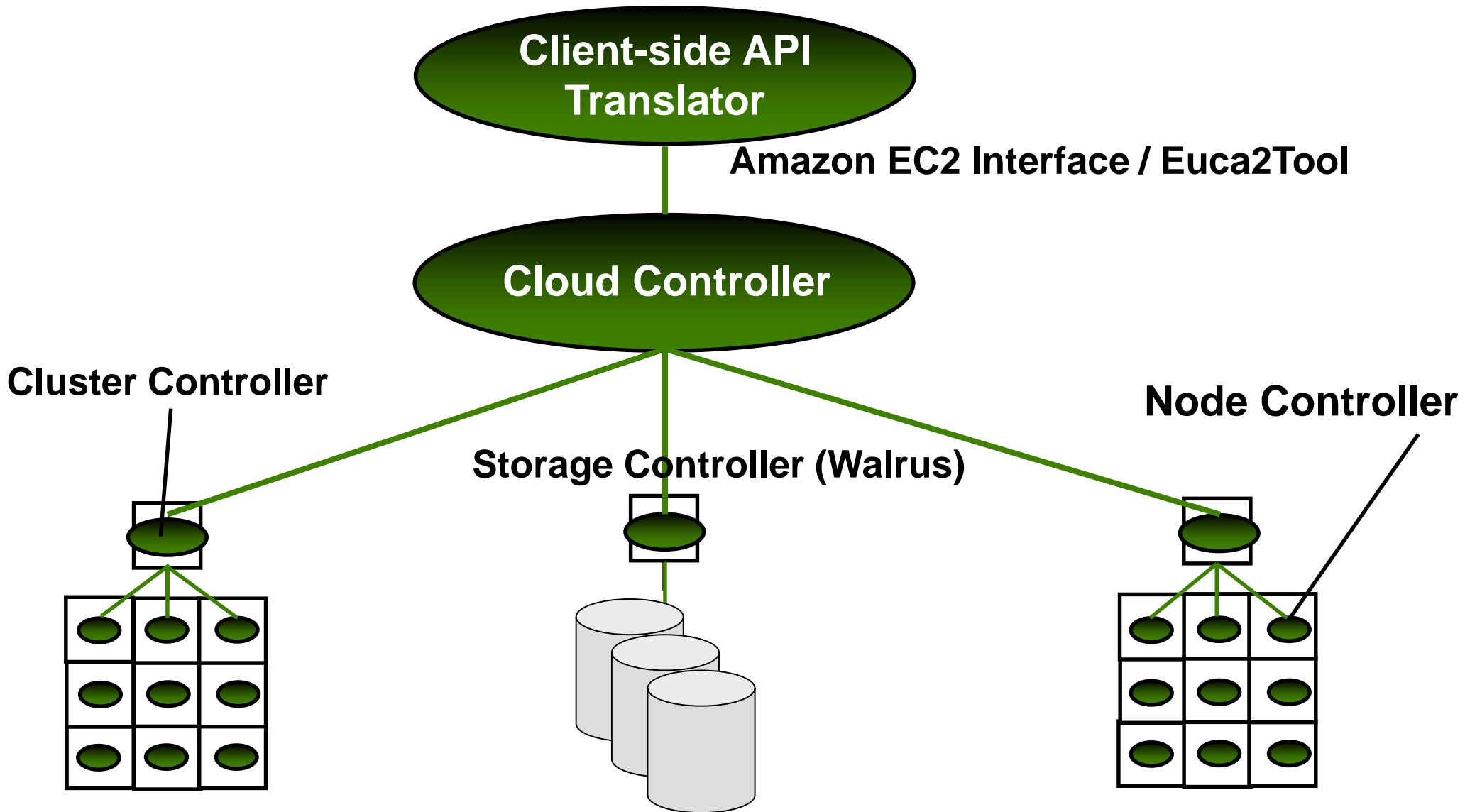
Amazon Elastic Compute Cloud (Amazon EC2) - Beta



MOSSO
the hosting cloud



[Eucalyptus sistemos architektūra]



[Kontroleriai]

- **CLoud Controller (CLC)** – tai servisas, atsakingas už informacijos surinkimą iš mazgų menedžerių ir užduočių paskirstymą klasterio kontrolieriams.
- **Cluster Controller (CC)** – tai servisas, kuris dažniausiai vykdomas klasterio centriniame mazge arba atskiroje mašinoje, kuri turi sujungimus su klasterio darbinių mazgų tinklu ir tinklu, kuriame dirba CLC.
CC surenka informaciją apie VM darbą ir planuoja VM paleidimą reikiamuose mazgų kontrolieriuose. CC taip pat administruoja VM tinklą ir užtikrina SLA vykdymą pagal CLC nurodymus.
- Darbiniai mazgai, kuriuos valdo vienas CC, turi būti viename potinklyje.

[Kontroleriai]

- **Node Controller (NC)** mazgų kontroleriai - tai servisai, kurie suinstaliuoti kiekviename fiziniame mazge, kuriame veikia VM. NC kontroliuoja VM paleidimą, vykdymą bei uždarymą, kopijuoja ir trina VM atvaizdus ir kontroliuoja mazgų hypervisorius. NC taip pat valdo virtualų tinklą.
- **Storage Controller (SC) – saugyklos kontroleris** užtikrina priėjimą prie blokinio tipo tinklinių saugyklų (pvz. Amazon Elastic Block Storage - EBS) ir gali veikti, kaip sąsaja su įvairiomis failų sistemomis (NFS, iSCSI, etc.). Walrus (put/get storage) yra Eucalyptus dalis ir leidžia vartotojui išsaugoti duomenis kaip objektus. Tai leidžia vartotojams kurti, trinti, peržiūrėti objektus ir joms pritaikyti prieigos kontrolės politiką.