[P271]

Информациони системи

10

Саша Малков

Универзитет у Београду Математички факултет

2021/2022

[P271]

Информациони системи

Саша Малков

Тема 14

Виртуализација

Виртуално

- Виртуално (енгл. *virtual*)
  - изворно:
    Скоро исто као нешто, али не у потпуности или не у складу са строгом дефиницијом
    - у српском језику попут “практично исто”
  - уобичајено у рачунарству:
    нешто што не постоји физички, али се софтверски ствара утисак постојања

Виртуализација

- Виртуализација је поступак стварања виртуалне верзије нечега
  - у контексту рачунарства, средство остваривања виртуализације је софтвер
  - предмет виртуализације може бити
    - реалан физички свет (виртуална стварност)
    - елементи рачунарског система (виртуални рачунар, систем, уређај)

Контрола рачунарског система (1)

- Првобитна решења
  - Апликативни софтвер
    - непосредно користи хардвер

Контрола рачунарског система (2)

- Једноставни монопрограмски системи
  - БИОС (енгл. *Basic Input Output System*)
    - програми за непосредну контролу хардвера
  - Апликативни софтвер
    - користи хардвер посредством БИОС-а
    - самостално управља ресурсима рачунара

Контрола рачунарског система (3)

- Оперативни системи
  - БИОС (енгл. *Basic Input Output System*)
    - програми за непосредну контролу хардвера
  - Оперативни систем
    - програми за управљање ресурсима рачунарског система
  - Апликативни софтвер
    - користи све рачунарске ресурсе (и хардвер) посредством оперативног система

Апстракција елемената хардвера

- Различити концепти / подсистеми ОС апстрахују различите елементе хардвера
  - Систем датотека
    - апстракција дискова
  - Процеси
    - апстракција адресног простора и изоловане меморије
  - Нити
    - апстракција процесора

Раздвојеност ОС и хардвера

- Савремени ОС су веома сложени
- Обављају велики број различитих фунцкија
- Ниво апстракције ОС је далеко изнад хардвера
- Штавише, исти ОС често раде на потпуно различитом хардверу

Слој апстракције хардвера

- Савремени ОС имају слој за апстракцију хардвера, који се непосредно ослања на (потенцијално специфичан) хардвер и остатку ОС-а пружа уједначену апстраховану слику
- Апликативни програми, као и већина компоненти ОС-а, раде користећи услуге слоја апстракције хардвера, практично потпуно независно од конкретних уређаја

Виртуалне машине

- Концепт виртуалне машине представља наредни ниво апстракције:
  - слој апстракције хардвера се издваја из ОС-а и представља независну целину – Надзорник виртуалних машина (НВМ, енгл. *Virtual Machine Monitor – VMM*, или *hypervisor*)

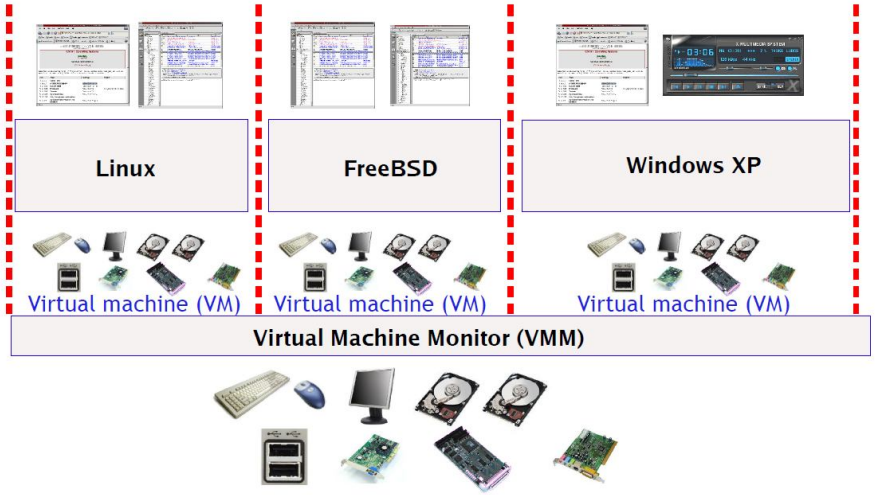
Виртуалне машине (2)

- НВМ се непосредно ослања на хардвер
- Један НВМ може истовремено да опслужује више оперативних система на истом рачунару
- Из угла сваког ОС-а изгледа као да је рачунар под његовом *потпуном* контролом
- Из угла апликативног софтвера *није видљиво* да ли је ОС непосредно над хардвером или се између налази НВМ

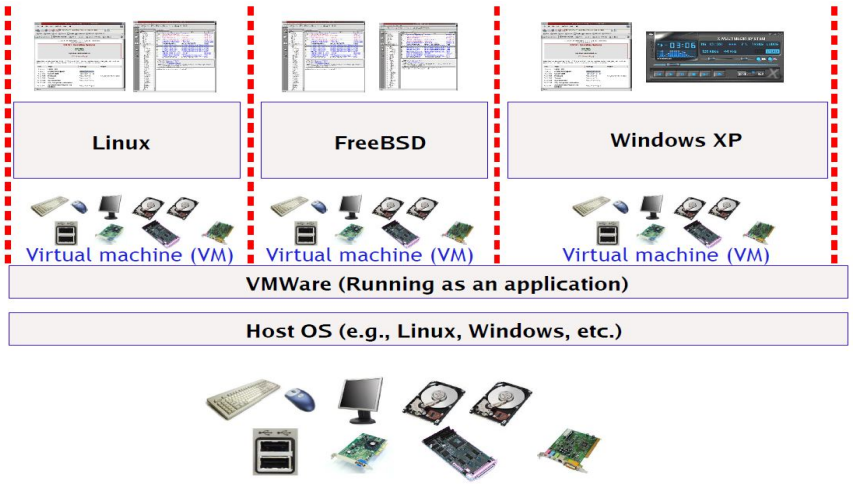
Термини

- Надзорник виртуалних машина
  - слој софтвера који се непосредно ослања на хардвер и подржава рад ОС-а
- Виртуална машина
  - апстрахован рачунарски систем који ради под НВМ-ом, а не на физичком хардверу
- Виртуални уређај
  - виртуална машина са инсталираним и конфигурисаним софтвером, потпуно спремна за рад
  - довољно ју је ископирати на други рачунар и укључити
  - (енгл. *virtual appliance*)
- Машина домаћин (енгл. *host machine*)
  - физички рачунар и софтвер (ОС и/или НВМ) који ради на њему
- Машина гост (енгл. *guest machine*)
  - виртуални рачунар и софтвер који ради на њему, ВМ

Пример архитектуре ВМ – Самосталан НВМ, без ОС-а



Пример архитектуре ВМ – НВМ који ради под ОС-ом машине домаћина



Мотивација

- Разликују се мотиви за виртуализацију
  - радних станица и
  - сервера

Мотивација – радне станице

- Повећана продуктивност
  - неки програми не постоје за све врсте ОС
  - различити ОС нису једнако погодни за све врсте послова
  - једноставније је имати више ВМ на једном рачунару него одржавати више физичких рачунара на једном радном месту
- Изоловање осетљивих система
  - заштита од вируса и других напасти
  - обука администратора, испробавање осетљивих поступака
  - обучавање у развоју системског софтвера
- Развојне радне станице
  - реално понашање мрежног окружења на једној радној станици
  - изградња на различитим развојним окружењима
  - тестирање
- Виртуални уређаји
  - поједностављена дистрибуција припремљених сложених окружења

Мотивација – сервери

- Консолидација сервера
  - више мањих сервера се виртуализује на једном физичком рачунару
  - раздвајање одговорности сервера, а тиме и олакшано одржавање
  - већа искоришћеност хардвера
  - уштеда на хардверу
- Напредна серверска окружења
  - олакшана репликација
  - једноставнија имплементација високе расположивости
  - пребацивање активних машина са једног на други рачунар

Циљеви

- Стварање илузије *комплетних* физичких машина
  - процесори, меморија, нивои заштите, систем прекида, улазно излазни уређаји,...
- Потпуна компатибилност са постојећим физичким хардвером
  - ОС и апликације у ВМ морају радити у неизмењеном облику
- Потпуна међусобна изолованост виртуалних машина
  - софтвер једне ВМ не сме бити у стању да ступи у контакт са виртуалним хардвером друге ВМ
- Омогућавање истовременог рада више ОС-а
  - потребан је висок ниво скалабилности
- Високе перформансе
  - посебно процесор и меморија
  - динамичко прилагођавање оптерећењу
- Флексибилност
  - поједностављено управљање расположивим ресурсима током рада ВМ
  - поједностављен трансфер активне ВМ на други физички рачунар

Кратка историја (1)

- 1965, *IBM Mainframe System M44*
  - Постојала је потреба да се велики систем партиционише на више мањих система према потребама корисника
  - Развијен је концепт виртуализације као решење
- 1967, Дијкстра
  - Предлаже различите нивое апсракције виртуалних машина

Кратка историја (2)

- 1970-..., *IBM S/370, S/390*
  - У својим системима IBM користи виртуалне машине као средство за управљање ресурсима
  - *IBM* модел:
    - физичка машина се дели на виртуалне реплике које су међусобно идентичне у свему осим у количини расположиве радне меморије
    - меморија је потпуно раздвојена, чиме је остварена потпуна безбедност
    - хардвер система је прилагођен виртуализацији
    - већина операција ради непосредно на хардверу, чиме су остварене високе перформансе

Кратка историја (3)

- 1990, програмски језик *Oak*
  - Обликована прва верзија програмског језика *Oak*, која је почивала на примени апликативних виртуалних машина
  - Овај језик је 1995. добио ново име – *Java*
  - *Java* модел:
    - виртуалне машине су симулиране
      - праве се за сваки програм посебно
    - у оквиру ВМ се не извршава ОС него само један програм
      - зато што ради само један програм
    - основна намена је преносивост програма

Кратка историја (4)

- 1999, *VMWare* и друга *PC* решења
  - Развијено прво комерцијално решење пуне виртуализације за платформу *x86*
  - За разлику од *IBM*-ових решења, овде хардвер није прилагођен
  - Потребно је симулирати већи број операција
    - сложенија имплементација
    - ниже перформансе

Врсте виртуалних машина

- Системске виртуалне машине
  - (називају се и *хардверске* виртуалне машине)
  - пружају апстракцију читавог рачунара
  - примери: *KVM, VMWare, VirtualBox, XEN,...*
  - само оне представљају данашњу тему
- Процесне (апликативне) виртуалне машине
  - пружају делимичну апстракцију рачунара, довољну за извршавање једног процеса
    - могу да подрже више програма (апликативни сервери)
    - у оквиру ВМ се не извршава ОС
  - примери: *JVM, CLR,...*
- Виртуализација на нивоу ОС-а
  - комбинација – у оквиру једног ОС-а пружају парцијалне инстанце истог ОС-а
  - примери: *FreeBSD Jail, LXC, OpenVZ,...*

Системске виртуалне машине

- Пуна виртуализација
- Хардверски подржана виртуализација
- Парцијална виртуализација
- Паравиртуализација

Системске виртуалне машине

- **Пуна виртуализација**
  - ВМ симулира све елементе хардвера потребне за рад неизмењеног оперативног система ВМ
  - први представник: *IBM CP-40*
  - примери: *VMware* (*Workstation*, *Server*), *Oracle VirtualBox*,...
- Хардверски подржана виртуализација
- Парцијална виртуализација
- Паравиртуализација

Системске виртуалне машине

- Пуна виртуализација
- **Хардверски подржана виртуализација**
  - хардвер пружа механизме за ефикасан рад надзорника, симулирање хардвера и изоловање ВМ
  - први представник: *IBM VM/370* (1972.)
  - примери: *Intel/AMD x86* (2005.), *IBM Power Architecture*, *VMware* (*Workstation*, *Fusion*), *Oracle VirtualBox*, *Xen*,...
- Парцијална виртуализација
- Паравиртуализација

Системске виртуалне машине

- Пуна виртуализација
- Хардверски подржана виртуализација
- **Парцијална виртуализација**
  - ВМ симулира већину (али не све) елемената хардвера
  - у оквиру ВМ не може да ради потпун ОС
    - може једна или више апликација
  - нешто између системске и процесне виртуализације
- Паравиртуализација

Системске виртуалне машине

- Пуна виртуализација
- Хардверски подржана виртуализација
- Парцијална виртуализација

- **Паравиртуализација**
  - ВМ не симулира хардвер већ пружа алтернативни *API* који замењује одређене компоненте гостујућег ОС-а
    - замењују се оне компоненте ОС-а које непосредно приступају хардверу
    - осетљиве инструкције се кодирају у складу са потребама ВМ
  - већа ефикасност али мања флексибилност
    - све ВМ морају да извршавају исти ОС
    - или НВМ мора да пружи интерфејс *API-ја* једног ОС за други
  - примери: *KVM, Xen,...*
    - Неки системи пуне виртуализације (*Vmware,...*) користе елементе паравиртуализације за подизање перформанси (*VMwareTools*)

Проблеми у имплементацији

- Гостујући ОС покушава да позива привилеговане инструкције
  - а то не би смео да чини, зато што то сме само надзорник (или домаћински ОС)
- Гостујући ОС покушава да управља страницама вирт. меморије
  - то производи потенцијалне проблеме зато што је тесно повезано са управљањем физичком меморијом
- Гостујући ОС мора да *верује* да ради на физичкој машини
  - ВМ мора да подржава све инструкције процесора, а неке нарушавају изолованост
  - ВМ мора да подржава све компоненте рада са виртуалном меморијом (страничење, сегментација,...)
  - ВМ мора да подржи улазно-излазне уређаје

Режим рада

- ОС по правилу има компоненте које раде у повлашћеном режиму, што омогућава пуну контролу хардвера
- ВМ по правилу не би смела да ради у повлашћеном режиму зато што не сме непосредно да приступа физичком хардверу

- Последица: ОС у ВМ мора да ради у корисничком, а не у повлашћеном режиму
  - неки процесори (и *x86*) имају и трећи “међу”-режим

Режим рада – интерпретација

- Једно решење је интерпретација
  - ВМ не извршава инструкције непосредно већ се рад процесора симулира програмом који интерпретира инструкције
  - може да се оствари пуна безбедност и изолованост

- Проблеми
  - сложеност – потребно је имплементирати читаву архитектуру процесора
  - спорост – интерпретирање инструкција процесора је за ред величине спорије од њиховог непосредног извршавања

Режим рада – извршавање

- Друго решење је непосредно извршавање
  - ВМ непосредно извршава инструкције процесора, али у корисничком режиму
  - овакав начин рада је високо ефикасан
  - покушаји извршавања заштићених инструкција изазивају *замке* и предају контролу надзорнику
    - надзорник проверава инструкцију и одлучује шта даље
      - може да безбедно емулира операцију и настави рад ВМ
      - може да забрани операцију и искључи ВМ
- Проблеми
  - умерена сложеност – потребно је имплементирати све заштићене инструкције процесора
  - умерено успорење – интерпретирају се само заштићене инструкције процесора
  - неке инструкције раде исправно само у заштићеном режиму, али не производе грешке иначе!!!

Режим рада – извршавање (2)

Изоловање ОС

- Уобичајено је да ОС и апликације не раде на истом нивоу привилегија
- Ако раде на истом, може доћи до проблема услед безбедности или исправности рада
- Могу да се користе додатни нивои заштите процесора, који иначе нису искоришћени:
  - прстен 0: НВМ
  - прстен 1: ВМ ОС
  - прстен 3: ВМ апликације

Режим рада – превођење

- Треће решење је превођење кода при учитавању
  - непосредно пре извршавања програма (или чак током извршавања) надзорник протрчи кроз код и преведе све проблематичне инструкције
    - нпр. *x86* инструкција *POPF* би требало да постави ново стање заставица, али у корисничком режиму не може да постави заставице прекида
  - праве се копије страница кода у меморији и одговарајуће таблице пресликавања
- Проблеми:
  - смањена ефикасност
- Паравиртуализација је вид оваквог рада, с тим да су сви делови ОС-а који користе привилеговане инструкције унапред преведени и прилагођени раду у ВМ
  - релативно једноставно
  - углавном ефикасно

Рад са меморијом

- Не сме свака ВМ да имплементира сопствену виртуалну меморију, зато што постоји само једна физичка меморија
- Уводи се додатни ниво индирекције
  - ВМ смеју само да читају таблице страница
  - одржава их надзорник

Виртуализација и ИС

- Који су основни инфраструктурни проблеми ИС?
- Које од њих може да олакша употреба виртуализације?

Инфраструктурни проблеми ИС

- Миграција
- Удвајање сервиса
- Скалирање
- Ниска искоришћеност сервера
- Хетерогеност

- ... и други ...

Инфраструктурни проблеми ИС (2)

- **Миграција**
  - пребацивање система или дела система са једног на други рачунар најчешће није једноставно
  - предузима се
    - када дође до квара рачунара
    - када се унапређује хардверска или софтверска платформа
  - често веома захтеван посао
    - може да захтева период неактивности система
- Удвајање (реплицирање) сервиса
- Скалирање
- Ниска искоришћеност сервера
- Хетерогеност

Инфраструктурни проблеми ИС (3)

- Миграција
- **Удвајање (реплицирање) сервиса**
  - прављење копије постојећег система
  - предузима се ради
    - обезбеђивања редундантности (превенција кварова)
      - у случају квара једног сервера неки други преузима његов посао
      - сваки се мора посебно инсталирати
      - реплике често стоје не радећи ништа или радећи врло мало
    - прављења тест верзије система (или дела система)
      - посебне развојне, пробне и продукционе верзије
  - удвајање није једноставно
    - потребан је додатни хардвер
    - сваки пут је потребно инсталирати ОС и сав потребан софтвер
    - идеалан случај је да системи имају исти хардвер, иначе је још теже
- Скалирање
- Ниска искоришћеност сервера
- Хетерогеност

Инфраструктурни проблеми ИС (4)

- Миграција
- Удвајање (реплицирање) сервиса
- **Скалирање**
  - прилагођавање система условима повећаног оптерећења
  - додавање меморије, процесора, дискова
    - ...постоје границе
  - може да захтева миграцију или унапређење софтвера
  - често се избегава иницијалним предимензионирањем хардвера
- Ниска искоришћеност сервера
- Хетерогеност

Инфраструктурни проблеми ИС (5)

- Миграција
- Удвајање (реплицирање) сервиса
- Скалирање
- **Ниска искоришћеност сервера**
  - често се тежи да један сервер обавља само једну функцију
    - лакше конфигурисање
    - лакше одржавање појединачних сервиса
    - лакше скалирање
  - ниједан од њих није ефикасно искоришћен
    - уобичајено 5-15%
  - велики трошкови
    - набавке хардвера
    - одржавања хардвера
    - администрирања
- Хетерогеност

Инфраструктурни проблеми ИС (6)

- Миграција
- Удвајање (реплицирање) сервиса
- Скалирање
- Ниска искоришћеност сервера
- **Хетерогеност**
  - разноврсност хардвера у оквиру информационе инфраструктуре
  - отежава многе послове, а пре свега
    - администрацију
    - удвајање сервиса
    - миграцију

Доприноси виртуализације

- Основни критеријуми су
  - спуштање цене (хардвера, одржавања)
  - подизање флексибилности
  - скраћивање периода неактивности система
- Посебно разматрамо
  - серверску виртуализацију
  - виртуално рачунарство

Доприноси виртуализације сервера

- Консолидација
- Удвајање виртуалних машина
- Динамична тест окружења
- Миграција виртуалних машина
- Скалирање

Консолидација

- Постављањем више малих ВМ на један физички сервер
  - штеди се простор
  - смањује се потрошња струје
  - смањује се учесталост хардверских кварова
    - додуше, кварови имају потенцијално веће последице

Удвајање виртуалних машина

- Удвајање ВМ је много једноставније
  - уместо понављања инсталације, ВМ се само ископира
  - прављење копија ВМ на различитим серверима је једнако сигурно као држање физички различитих сервера
  - ако резервна ВМ не ради ништа на неком серверу, значи да има простора за још других ВМ које могу нешто да раде
  - у случају кварова, када резервне реплике почну да раде, може да дође до пада перформанси, ако није добро испланирано

Удвајање виртуалних машина (2)

- Удвајање рачунара над дељеним дисковима:
  - често решење
  - виртаулни дискови су на безбедним (редундантним) уређајима
  - више копија ВМ користи потпуно исте виртуалне дискове
  - једна је активна, ако нешто откаже одмах постоји спремна друга ВМ на другом хардверу
    - или чак у другом центру података

Динамична тест окружења

- Поједностављено удвајање ВМ има за последицу лакше одлучивање за прављење вишеструких тест окружења
  - лакше прављење и одржавање
  - нижа цена
  - повећана безбедност
  - успешније и благовремено уочавање и решавање проблема

Миграција виртуалних машина

- Пребацивање ВМ са једног на други сервер је сасвим једноставно
  - на нову машину се инсталира само НВМ или ОС и НВМ
  - затим се ископирају потребне ВМ
    - савремена комерцијална решења допуштају да се ВМ пребацују са једне на другу физичку машину без прекида рада
    - посебно ако се ВМ чувају на дељеним системима дискова
- Савремен метод управљања оптерећењем, кроз распоређивање ВМ по физичким серверима

Скалирање

- Скалирање система је лакше у виртуализованом окружењу
  - када се дода нови физички сервер, на њега се пребаце изабране ВМ и тиме се растерете загушени сервери
  - све то много брже и једноставније уз скраћивање периода неактивности система

Ограничења виртуализације сервера

- Виртуализација сервера није ефикасна ако је сервер подложан претерано високом оптерећењу неког хардверског ресурса (или више њих): процесор, меморија, дискови, мрежа,...
  - дељењем снаге рачунара на више ВМ смањује се снага сваке од ВМ
  - ако на серверу постоји само једна ВМ, чак и она ради мање ефикасно него што би радила да није ВМ
  - (чак и тада је лакше мигрирати ВМ на нови рачунар него у случају физичких машина)
- У већини случајева миграција ВМ је ограничена на платформе са истим типом процесора

Виртуално рачунарство

- Виртуално рачунарство (*Virtual Computing*) је техника која обезбеђује да се један рачунар понаша као да је неки други
- То у пракси значи да је се један рачунар понаша као терминал, а други му пружа одговарајућу услугу и потребан хардвер

Доприноси виртуалног рачунарства

- Пуна контрола над удаљеним физичким рачунаром
  - корисник физички ради на слабом рачунару, а заправо се програми извршавају на удаљеном снажном рачунару
  - корисник може издалека да управља радом сервера

Доприноси виртуалног рачунарства (2)

- Пуна контрола над удаљеним виртуалним рачунаром
  - реплицирана инфраструктура предузећа
  - корисници са својих личних стоних или преносних рачунара имају терминалски приступ виртуалним рачунарима на серверима предузећа
  - унификована инфраструктура
  - лако одржавање виртуалних радних станица
    - све ВМ су међусобно идентичне реплике
    - софтвер се једанпут инсталира, а затим се копирају ВМ
  - лако се управља правима и безбедношћу
    - ако се корисников лични рачунар зарази вирусима и сл. његова пословна ВМ је изолована и безбедна
    - на локалним рачунарима се углавном не чувају подаци од пословног значаја, па је поједностављено прављење рез. копија

Контејнери

- Контејнери представљају новију технологију
  - представља алтернативу виртуализацији али
  - представља и вид виртуализације
  - комбинација виртуализације и тзв. *sandbox* система
- Вид паравиртуализације код кога процеси у контејнеру
  - виде *цео* домаћински рачунарски систем
  - у свим битним аспектима се ослањају на домаћински ОС
  - сви ресурси се користе изоловано и контролисано
    - читања могу да пролазе до фајл-система домаћина
    - писања остају у контејнеру

Контејнери (2)

- Нижа режијска цена од ВМ
  - не покреће се више инстанци ОС
    - уштеда меморије, простора на дисковима и процесорског времена
  - дели се и инсталиран софтвер
    - уштеда простора на диску и поједностављено конфигурисање
- Нешто мања флексибилност
  - сви контејнери деле исти инсталиран ОС
    - може много тога да се *замени* али се дели језгро ОС
- Олакшано одржавање
  - један ОС
    - лакше старање о безбедности
    - лакше ажурирање

Контејнери (3)

- Нису добри за развојна тест-окружења која захтевају више различитих оперативних система
- Одлични су за компонентне архитектуре софтвера
  - за сваки сервис (компоненту) може да се обезбеди посебан контејнер
  - свака компонента може да се инсталира и конфигурише за себе
  - свака компонента може да се мултиплицира
  - свака компонента може да користи одговарајуће (потенцијално различите) верзије библиотека и програма

Рачунарство у облаку

- Наредни корак у виртуализацији је рачунарство у облаку
  - читава рачунарска мрежа се апстрахује једним великим виртуалним рачунарским системом
  - привидно много програма ради на једном великом систему, а уствари се извршавају појединачно, или чак по деловима, на различитим рачунарима те мреже

Литература

- *James E. Smith, Ravi Nair,* ***The Architecture of Virtual Machines****, . Computer (IEEE) 38 (5): 32–38. 2005.*
- *WWW...*