**Лекція 4 Технології віртуалізації**

Однією з найбільш істотних технологічних новацій, що лежать в основі хмарних обчислень, є технології віртуалізації.

**Віртуалізація** - надання набору обчислювальних ресурсів або їх логічного об'єднання, абстраговані від апаратної реалізації, і забезпечує при цьому логічний ізоляцію обчислювальних процесів, які виконуються на одному фізичному ресурсі.

 **Віртуалізація** - це перехід від технології, що лежить в основі консолідації серверів і центрів обробки даних, до основних компонентів для створення гнучкої (надається на вимогу) інфраструктури

**Основні поняття технології віртуалізації**

***Віртуальна машина*** - ізольований програмний контейнер, який працює з власної ОС і додатками, подібно фізичному комп'ютера. Віртуальна машина діє так само, як фізичний комп'ютер, і містить власні віртуальні ОЗУ, жорсткий диск і мережевий адаптер.

 ***Віртуальна машина*** являє собою програмний контейнер, що зв'язує, або "інкапсулює" повний комплект віртуальних апаратних ресурсів, а також ОС і все її застосування в програмному пакеті.

***Виртуализация*** – это переход от технологии, лежащей в основе консолидации серверов и центров обработки данных, к основным компонентам для создания *гибкой предоставляемой по требованию инфраструктуры*

**Основні поняття технології віртуалізації**

Основними особливостями віртуальних машин є:

* сумісність (віртуальні машини сумісні з усіма стандартними комп'ютерами, віртуальна машина працює під управлінням власної гостьовий операційної системи і виконує власні додатки);
* ізольованість (віртуальні машини повністю ізольовані один від одного, як якщо б вони були фізичними комп'ютерами);
* інкапсуляція (віртуальні машини повністю інкапсулюють обчислювальну середу).
* віртуальні машини повністю незалежні від базового фізичного обладнання, на якому вони працюють.

***Хостової операційна система*** - це операційна система, встановлена на реальне обладнання. В рамках цієї операційної системи встановлюється програмне забезпечення віртуалізації як звичайна програма.

***Емулятор віртуальної машини*** - це програмне забезпечення, яке встановлюється на хостовую операційну систему і складається з монітора віртуальних машин і графічної оболонки.

***Монітор віртуальних машин*** є програмою, що забезпечує всі взаємодії між віртуальним і реальним обладнанням, що підтримує роботу однієї або декількох створених віртуальних машин і встановлених гостьових операційних систем.

 Графічна оболонка забезпечує взаємодію користувача з додатком віртуальної машини, дозволяючи налаштовувати створювані віртуальні машини під свої потреби і управляти її роботою.

***Гостьова операційна система*** - це операційна система, яка встановлюється на створену віртуальну машину. В якості гостьових операційних систем можна використовувати Window, Linux і ін.

При використанні технології віртуалізації отримують ***ієрархічну структуру взаємодії віртуальних ЕОМ і реальної апаратури.***

На нижньому шарі цієї ієрархії знаходиться реальне обладнання, управління яким розподіляється між хостовой операційною системою і емулятором віртуальних машин.

* ***Хостової операційна система і емулятор*** розподіляють між собою ресурси реальної ЕОМ і складають другий рівень ієрархії.
* ***Хостової операційна система*** займається управлінням працюють на ній додатків і розподілом між ними ресурсів реальної ЕОМ.
* ***Емулятор віртуальних машин*** управляє віртуальними машинами до встановлених на них гостьовими операційними системами, розподіляючи між ними ресурси реальної ЕОМ так, щоб у користувачів створювалося враження роботи на реальному обладнанні

Частково, розподіл ресурсів між віртуальними машинами можна налаштувати на етапі конфігурації віртуальних машин, вказавши обсяг оперативної пам'яті, розмір жорсткого диска, кількість віртуальних процесорів, віртуалізіруемие канали зв'язку і інші параметри.

***Гостьові операційні системи*** управляють роботою своїх додатків в рамках виділених емулятором ресурсів.

 Розглядаючи технологію віртуалізації, необхідно вивчити ***емулятор віртуальних машин, а саме монітор віртуальних машин***, що є базовою частиною технології віртуалізації.

Всі існуючі монітори віртуальних машин можна розділити на чотири види, що використовують:

* апаратну,
* апаратно-програмну,
* програмну
* доменну віртуалізації.

Це поділ - умовно, оскільки більшість моніторів віртуальних машин використовують, як програмну, так і апаратну віртуалізацію, так як програмна віртуалізація - вимоглива до ресурсів, а апаратна віртуалізація обмежується вузьким колом обладнання, що підтримує будь-якої вид моніторів віртуальних машин.

Доменна віртуалізація ґрунтується на логічному розподілі ресурсів на окремі частини (домени). В основному вона використовується в мейнфреймах. Цей тип віртуалізації з'явився першим і використовувався для розподілу ресурсів великих ЕОМ між окремими користувачами.

Монітори віртуальних машин, що використовують технологію апаратно-програмної віртуалізації, частину інструкцій виконують, безпосередньо на самому процесорі, а частину - емулюють.

Існують три типи **програмної емуляції інструкцій хостовой ЕОМ:**

* ***повна емуляція інструкцій,***
* ***вибіркова емуляція інструкцій,***
* ***емуляція API.***

При використанні ***повної емуляції*** інструкції інтерпретуються і перетворюються в інструкції, що сприймаються реальним процесором.

У цьому випадку з'являється можливість створювати віртуальні машини, що імітують роботу апаратури, не сумісної з архітектури з реальної ЕОМ.

 Наприклад, можна запускати віртуальну машину, що імітує роботу процесора з RISC-архітектурою, на реальній ЕОМ з процесором CISC-архітектури. Це можливо за рахунок того, що емуляція ведеться на рівні базових арифметико-логічних інструкцій, присутніх, практично, в будь-якому процесорі.

Інтерпретація кожної інструкції призводить до значної витрати ресурсів реальної ЕОМ і знижує швидкодію програм, які потребують гостьовою операційною системою. Сучасні сервери і персональні ЕОМ мають всі більшою продуктивністю. Тому віртуалізація, з використанням інтерпретації інструкцій, набуває популярності. Представниками даного класу віртуальних машин є: **Microsoft Virtual PC, Bochs, Simics** і ін.

Такі віртуальні машини є незамінними при налагодженні і розробці програмного забезпечення, написаного на мовах низького рівня, і при емуляції ЕОМ зі специфічною архітектурою на стандартизовані персональні комп'ютери і сервери.

Не всі інструкції необхідно інтерпретувати. Частина інструкцій віртуальної машини можна виконувати без змін на реальному процесорі. Монітор віртуальних машин, проаналізувавши код, може інструкції віртуальної машини, що збіглися з інструкціями реального процесора, без змін відправити для виконання на реальному процесорі, а решта інструкції інтерпретувати - ***вибіркова емуляція інструкцій.***

 З'являються додаткові витрати на аналіз інструкцій. Оскільки в програмах часто зустрічаються цикли, інтерпретація яких може проводитися одноразово, і найбільш прості інструкції, здатні без зміни виконуватися на процесорі складають більшу частину програм, то продуктивність віртуальної машини збільшується в кілька разів, в порівнянні з повною емуляцією інструкцій.

До віртуальним машинам цього типу відносяться, наприклад: **VMware Workstation, VMware Server, Serenity Virtual Station і ін**.

У третьому випадку, ***емулюються API гостьової операційної системи***.

***API (Application Programming Interface)*** - це інтерфейс прикладного програмування

Усі працюючі програми взаємодіють з обладнанням за допомогою інтерфейсу API. Тому можна перехопити звернення програм, що працюють під управлінням гостьової операційної системи, до API, перетворити його до виду, прийнятому в хостовой операційній системі, і ретранслювати отриманий результат до API хостовой операційної системи.

 Результат виконання запиту хостовой операційною системою перетвориться до виду, що приймається гостьовою операційною системою, і передається програмі, що видала запит.

 Якщо гостьова і хостової операційні системи сумісні за своїми API, то перетворювати звернення не потрібно, достатньо тільки перенаправляти їх.

Однак у такої системи віртуалізації є недоліки:

Не всі програмне забезпечення можна запускати на віртуальній машині з цим принципом віртуалізації, оскільки часто використовуються *недокументовані API і звернення безпосередньо до апаратури.*

Операційні системи активно розвиваються, вносяться коректування в API і додаються нові можливості. Тому емулятори API швидко застарівають і для їх модернізації необхідні великі витрати трудомісткості.

Емулятори API прив'язуються до конкретних операційних систем. Це звужує коло їх використання та споживчі властивості.

Однак використання емуляції API дозволяє уникнути значних втрат продуктивності.

Як приклад віртуальних машин, що використовують емуляцію API, можна привести такі продукти, як:

**Wine (Wine Is Not an Emulator),** який використовується для запуску Dos і Windows - додатків під управлінням операційної системи Linux.

**UML (User Mode Linux),** вбудований в ядро Linux і дозволяє запускати кілька копій операційної системи на одному комп'ютері.

**Безпека в віртуальних хмарах**

**Віртуалізація - це перехід** від технології, що лежить в основі консолідації серверів і центрів обробки даних, до основних компонентів для створення гнучкої надається на вимогу інфраструктури.

При реалізації віртуалізації в будь-якому середовищі виникає багато завдань, які треба вирішити.

Розглянемо питання, пов'язані з безпекою, які необхідно вирішити, коли мова йде про використання віртуалізації для хмарних обчислень.

Один з ризиків - ***ризик компрометації гипервизора віртуальних машин***.

   ***Гипервизор (англ. Hypervisor) або Монітор віртуальних машин*** (в комп'ютерах) - програма або апаратна схема, що забезпечує або дозволяє одночасне, паралельне виконання декількох операційних систем на одному і тому ж хост-комп'ютері.

***Гипервизор*** також забезпечує ізоляцію операційних систем один від одного, захист і безпеку, поділ ресурсів між різними запущеними ОС і управління ресурсами.

Якщо ***гипервизор*** ненадійний, то він стане першою стратегічною метою зловмисників. Якщо не усунути цю небезпеку, то в хмарі атака може привести до масштабних руйнувань. Це вимагає додаткового рівня ізоляції мережі і посиленою системи моніторингу безпеки.

Для аналізу цієї небезпеки спробуємо для початку зрозуміти природу гипервизора.

Консультант з безпеки і одного із засновників компанії Nemertes Research Group Inc. Андреаса Антонопулос (Andreas Antonopoulos) вважає,

що ***"Гіпервізор - вузькоспеціалізовані пристрої***.

   ***гипервизор*** менше і більш спеціалізований, ніж операційна система загального призначення, і менше відкритий для атак, так як у нього менше або взагалі немає відкритих зовні мережевих портів.

 ***гипервизор*** нечасто змінюється і не виконує програми сторонніх розробників.

 У гостьовій ОС, яка може стати жертвою атак, ***немає прямого доступу до Гіпервізору.***

 ***Гипервизор*** прозорий для мережевого трафіку, якщо не брати до уваги вхідний і вихідний трафік виділеного інтерфейсу управління гіпервізором.

На поточний момент не задокументовано жодної атаки на ***Гипервизор*** також говоритися про низьку ймовірність таких атак.

Тому хоча масштаб руйнувань у разі компрометації гипервизора може бути величезним (компрометація всіх гостьових систем), ймовірність такого події низька, тому що уразливість гипервизора і ймовірність атаки дуже низькі .

**Наступна проблема** полягає в масштабуванні функціональності віртуальних ЛВС за межі існуючих кордонів для підтримки великих за розміром хмар.

**Різновиди віртуалізації:**

***1 / віртуалізація серверів (повна віртуалізація і паравіртуалізація);***

***2 / віртуалізація на рівні операційних систем;***

***3 / віртуалізація мережі;***

***4 / віртуалізація додатків;***

***5 / віртуалізація подань;***

***6 / віртуалізація робочих місць САПР;***

***7 / віртуалізація сховищ.***

**Технологія віртуалізації сервері**в дозволяє запускати на одному сервері декілька логічних одиниць - ***віртуальних машин***, які повністю відтворюють роботу незалежних фізичних серверів.

Це дає можливість розміщувати на одній одиниці обладнання кілька десятків незалежних операційних систем і корпоративних додатків, ефективніше використовуючи IT-інфраструктуру.

         ***Віртуалізацію*** можна описати як ***дію гипервизора,*** що дозволяє створювати безліч логічних розділів, в яких будуть працювати різні операційні системи (одночасно на одному фізичному сервері).

Кожен розділ (званий також ***віртуальною машиною***) - це програмне середовище, яке надає ресурси (за допомогою емуляції обладнання або пристроїв).

            Поверх неї можна інсталювати операційну систему, а також одне або кілька додатків.

В основі рішення віртуалізації на рівні машини лежить монітор віртуальних машин (***Virtual Machine Monitor, VMM). VMM*** відповідає за створення і ізоляцію віртуальної машини і збереження її стану, а також за організацію доступу до системних ресурсів.

Схема ***VMM*** залежить від архітектури конкретного процесора; незважаючи на те, що VMM дозволяє працювати всередині віртуальної машини немодифікованим операційним системам.

**При реалізації VMM** для створення інтерфейсу між віртуальними машинами і віртуалізованими системними ресурсами використовуються три можливих методи:

* ***повна віртуалізація,***
* ***власна віртуалізація***
* ***і паравіртуалізація***.

***Повна віртуалізація***. При використанні цього методу монітором VMM (для абстрагування віртуальної машини від реального обладнання) створюється і підтримується повна віртуальна система.

 Цей підхід дозволяє виконувати у віртуальній машині операційну систему без всяких її модифікацій.

Перевагою повної віртуалізації і підходу з повним розв'язанням фізичного обладнання та віртуальної машини є здатність легко переносити віртуальні машини між серверами з різними фізичними конфігураціями.

***Власна віртуалізація.*** Така віртуалізація залежить від архітектури віртуалізіруемого процесора (наприклад, такий, як в серіях процесорів AMD-V і Intel VT). Ці процесори мають в своїй апаратній частині нові режими виконання, інструкції та структури даних, які призначені для зменшення складності VMM.

При власній віртуалізації монітора VMM не потрібно підтримувати в програмному забезпеченні характеристики ресурсів віртуальної машини і її стан.

Точно так же, як і в разі повної віртуалізації, усередині віртуальних машин операційні системи можуть виконуватися без їх модифікації. Hyper-V використовує цей метод для роботи застарілих операційних систем.

Такий тип реалізації має багато переваг - від спрощення архітектури VMM і до істотного підвищення продуктивності (в результаті зниження накладних витрат програмного забезпечення).

***Паравіртуалізація.*** Паравіртуалізація була розроблена як альтернатива використанню двійковій трансляції при обробці невіртуалізіруемих інструкцій процесора х86. При цьому підході потрібно модифікація гостьових операційних систем (для того, щоб уможливити "гіпервизови" від віртуальної машини до Гіпервізор).

**Рішення по серверної віртуалізації:**

**VMware vSphere** - платформа для серверної віртуалізації, що надає максимальні рівні доступності та швидкості реагування для всіх додатків і служб.

**VMware vCenter** - єдина консоль управління внутрішньої віртуальної інфраструктурою дата-центрів

**VMware vCloud Director** - інструмент управління внутрішніми і зовнішніми "хмарами" організації.

**Citrix XenServer** - рішення Enterprise-рівня для віртуалізації серверів.

**Microsoft Server Hyper-V** - система віртуалізації в серверній середовищі Microsoft, що надає організаціям широкі можливості по управлінню і масштабування IT-ресурсів.

Microsoft System Center Virtual Machine Manager - рішення, призначене для управління фізичними і віртуальними машинами.

**Віртуалізація на рівні операційної системи** заснована на ідеї підтримки операційною системою хоста декількох ізольованих розділів (або віртуальних середовищ, virtual environment (VE)).

Віртуалізація досягається за допомогою мультиплексування доступу до ядра (з забезпеченням безпеки системи від віртуальних середовищ).

**Віртуалізація на рівні ядра ОС** має на увазі використання одного ядра хостовой ОС для створення незалежних паралельно працюють операційних середовищ.

Для гостьового ПО створюється тільки власне мережеве та апаратне оточення. Такий варіант використовується в **Virtuozzo (для Linux і Windows), OpenVZ (безкоштовний варіант Virtuozzo) і Solaris Containers.**

**Віртуалізація мережі** - це повне відтворення фізичної мережі програмним методом.

Віртуальні мережі аналогічні фізичним мереж з точки зору надійності і можливостей.

Однак вони мають безліч додаткових експлуатаційних переваг, таких як незалежність від обладнання, швидка ініціалізація, можливість розгортання без переривання роботи систем, автоматизоване обслуговування та підтримка як сучасних, так і застарілих додатків.

**Віртуалізовані застосування** (такі як бази даних, системи ERP і CRM, електронну пошту, додатки для спільної роботи, проміжне ПО Java, засоби бізнес-аналітики та ін.) переносяться в віртуальне середовище,     де працюють швидше і краще, характеризуються високою доступністю і адаптивністю, а також підтримують можливість аварійного відновлення і використання в хмарної інфраструктурі.

Рішення **VMware** по віртуалізації додатків, засноване на **VMware vCloud Suite**, допомагає підвищити якість ІТ-послуг, знизити складність інфраструктури, досягти максимальної ефективності, а також знизити витрати за рахунок виділення правильного обсягу ресурсів.

**Віртуалізація додатків** - це технологія, яка спрямована на розділення і ізоляцію додатків на стороні клієнта (що працюють під місцевою операційною системою).

 Додатки ізолюються в віртуальному середовищі, що знаходиться між операційною системою і стеком додатків.

Віртуальне середовище завантажується до додатка, ізолює його від інших додатків і операційної системи, а також запобігає модифікацію додатком локальних ресурсів (таких, як файли і настройки реєстру).

Дана технологія дозволяє використовувати на одному комп'ютері, а точніше в одній і тій же операційній системі кілька несумісних між собою додатків одночасно. Віртуалізація додатків дозволяє користувачам запускати одне і теж заздалегідь сконфигурированное додаток або групу додатків з сервера.

При цьому додатки будуть працювати незалежно один від одного, не вносячи жодних змін в операційну систему.

  Такий варіант віртуалізації використовується в:

 **Sun Java Virtual Machine, Microsoft Application Virtualization (раніше Softgrid), Thinstall (на початку 2008 р увійшла до складу VMware), Symantec / Altiris.**

**Решенія для віртуалізації додатків і термінального доступу** на основі продуктів:

* **Citrix XenApp** - фактичний стандарт доставки будь-яких Windows-додатків з мінімальними витратами в будь-яку точку світу. Citrix XenApp забезпечує захищений термінальний доступ до корпоративних ресурсів і централізоване управління ними.
* **Citrix NetScaler** - рішення для оптимізації процесу доставки web-додатків.
* **Citrix Branch Repeater** - рішення щодо прискорення та оптимізації доставки додатків, робочих столів.
* **VMware ThinApp** - рішення, яке створює пакет, що включає в себе додаток і пов'язану з ним частину операційної системи, що дозволяє здійснювати термінальний доступ до додатка.
* **VMware Zimbra** - система автоматизації спільної діяльності робочих груп (пошта, спільні документи).
* **Microsoft App-V** - рішення для віртуалізації і доставки додатків, швидкого оновлення, запуску несумісних додатків, управління правами.

**Віртуалізація уявлень (робочих місць)** - це інфраструктура віртуальних робочих столів VDI.

 На відміну від «звичайного» термінального доступу, спрощуючи, мова йде про декілька віртуальних машинах на фізичному сервері. Кожен користувач отримує свій власний віртуальний ПК, куди може підключатися хоч з телефону.

**Віртуалізація робочих столів** реалізується за допомогою інфраструктури Virtual Desktop Infrastructure (VDI). Цей термін позначає комбінацію апаратного забезпечення, програмного забезпечення для віртуалізації, а також інструментів управління.

Віртуалізація робочих столів може бути реалізована або як статичні віртуальні робочі столи, або як динамічні віртуальні робочі столи.

При першому варіанті фізичний настільний комп'ютер замінюється віртуальним. У другому варіанті кінцеві користувачі динамічно підключаються до одного з віртуальних робочих столів з пулу (на вимогу).

Віртуальні робочі столи розміщуються на надійних відмовостійких серверах в дата-центрах. Користувач завжди має повний контроль над усіма своїми ресурсами. Підключення проводиться за допомогою служби термінального доступу Microsoft Windows по захищених каналах (RDP), що забезпечує конфіденційність інформації, що передається.

Для комфортної роботи з віддаленим робочим столом використовуються технології **Microsoft, VMware, Citrix**. Після підключення користувачів до віддаленого робочого столу можна скористатися всіма мережевими і локальними пристроями (флеш-накопичувачі, приводи, принтери і т.д.).

Різні рішення для організації віддаленого робочого столу:

* **VDI від Amazon AWSБ**
* **Amazon WorkSpace** - це віддалені робочі столи в хмарі Amazon AWS з попередньо встановленими пакетами офісних додатків з можливістю інтеграції сервісу з локальної службою каталогів.
* **Сервіс DaaS** - це швидкий доступ до робочого столу користувачів з будь-якої точки, з будь-якого пристрою. Користувачі отримують можливість працювати ефективніше, оперативно одержуючи доступ до своїх даних в будь-який час.
* **VDI на базі Citrix або Vmware**

**Віртуалізація робочих місць САПР**

Технологія віртуалізації робочих місць САПР, побудована на базі рішень **Citrix і технології NVIDIA GRID.**

**Технологія NVIDIA GRID** - це рішення для віртуалізації GPU, віддаленого доступу та управління сеансом, яке дозволяє декільком користувачам одночасно працювати з графічно насиченими додатками, використовуючи загальні ресурси GPU.

Технологія покликана вирішити проблему віртуалізації і віддаленого доступу до робочих місць в таких областях, як автоматизація проектування (CAD), управління інформацією в будівництві (BIM), управління життєвим циклом вироби cv (PLM), автоматизація діяльності кредитно-фінансових установ, робота з системами архівації і передача зображень в області охорони здоров'я, фото- і відеоредагування.

Завдяки цьому, а також використання технологій Citrix XenServer GPU pass-through і Citrix XenDesktop HDX 3D стало можливим запускати важкі 3D-додатки на стороні сервера і надавати до них доступ в термінальному режимі з повною підтримкою професійної графіки NVIDIA GRID.

переваги:

* Зниження до мінімуму ризику втрати корпоративних даних огляду на їх відсутність на локальному робочому місці і можливості прямого доступу до них.
* Економія на ТСО і на всіх випливають витратах на обслуговування робочих місць, складнощами з пошуком в конкретній точці кваліфікованих ІТ-фахівців і т.д.
* Можливість дистанційної роботи співробітників.

**Віртуалізація сховищ**

Мета ***віртуалізації сховищ*** як одного з компонентів програмного сховища - підвищення продуктивності без придбання додаткового обладнання для зберігання даних.

***Віртуалізовані сховища*** повинні підтримувати швидку ініціалізацію, щоб забезпечити розгортання високопродуктивних ефективних сховищ з тією ж швидкістю, що і ВМ (вирт машин)

Модель управління сховищами повинна орієнтуватися на потреби ВМ і забезпечувати зручність роботи адміністраторам віртуальних середовищ, в завдання яких входить управління ресурсами зберігання. Для зручної роботи з віртуалізованими сховищами від них вимагається високий ступінь інтеграції з платформою гипервизора.

***Віртуалізація сховищ VMware*** - це поєднання можливостей, яке формує рівень абстракції для ресурсів фізичного сховища і підтримує їх адресацію, оптимізацію і адміністрування в віртуальному середовищі.

***Технології віртуалізації сховищ*** забезпечують ефективний спосіб управління ресурсами зберігання в віртуальної інфраструктури і реалізують такі переваги:

* значне підвищення ефективності і гнучкості використання сховищ;
* спрощення установки виправлень ОС і зниження вимог до драйверів, усунення залежності від топології сховища;
* збільшення часу безвідмовної роботи додатків і спрощення стандартних процесів;
* використання і доповнення існуючої інфраструктури зберігання.