

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Осухівська Г.М.

(підпис)

(прізвище та ініціали)

« ____ » _____ 2022 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього
ступеня

Магістр

(назва освітнього ступеня)

за спеціальністю 123 «Комп'ютерна інженерія»

(шифр і назва спеціальності)

студенту Ромашевській Наталії Анатоліївни

(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби віртуалізації для організації навчального процесу в ДВНЗ Нововолинський електромеханічний коледж

Керівник роботи Жаровський Р.О., к.т.н.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «14» грудня 2022 року № 4/7-1011

2. Термін подання студентом завершеної роботи 22.12.2022 р.

3. Вихідні дані до роботи 12 ПК з встановленими мовами програмування, Mathcad, Mathcad, AutoCAD та іншим ПЗ. Сервер з встановленою серверною ОС, VMware з 12, SQL Server, 12 ПК з встановленим VMware та OS Linux з SQL Server.

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ

1. Експериментальне впровадження технології віртуалізації у процес навчання

2. Серверна віртуалізація. Загальні поняття

3. Локальна віртуалізація настільних систем навчального закладу

4. Охорона праці та безпека в надзвичайних ситуаціях

Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Актуальність і мета дослідження.

2. Задачі дослідження, об'єкт і предмет, наукова новизна і практична цінність дослідження.

3. Огляд технології віртуалізації

4. Експериментальне впровадження технології віртуалізації у процес навчання

5. Локальна віртуалізація настільних систем навчального закладу

6. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
<i>Безпека в надзвичайних ситуаціях</i>			
<i>Охорона праці</i>			

7. Дата видачі завдання 15.12.2022

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	<i>Актуальність і мета дослідження технології віртуалізації навчальних закладах.</i>		<i>виконано</i>
2	<i>Визначення задач дослідження, об'єкту і предмет, наукової новизни і практичної цінності дослідження.</i>		<i>виконано</i>
3	<i>Вивчення технології віртуалізації</i>		<i>виконано</i>
4	<i>Експериментальне впровадження технології віртуалізації у процес навчання</i>		<i>виконано</i>
5	<i>Серверна віртуалізація. Локальна віртуалізація настільних систем навчального закладу</i>		<i>виконано</i>
6	<i>Охорона праці та безпека в надзвичайних ситуаціях</i>		<i>виконано</i>
7	<i>Оформлення пояснювальної записки і графічного матеріалу</i>		<i>виконано</i>
8	<i>Захист кваліфікаційної роботи магістра</i>		

Студент

(підпис)

Ромашевська Н.А.

(прізвище та ініціали)

Керівник роботи

(підпис)

Жаровський Р.О.

(прізвище та ініціали)

АННОТАЦІЯ

Методи та засоби віртуалізації для організації навчального процесу в ДВНЗ Нововолинський електромеханічний коледж // Кваліфікаційна робота // Ромашевська Наталія Анатоліївна // ТНТУ, комп'ютерна інженерія, група СІд-2 // Тернопіль, 2022 // с. – 78, рис. – 46, табл. – 3, додат. – 1, бібліогр. – 21.

Ключові слова: віртуалізація, сервер, операційна система, SQLServer, VMware, Active Directory, гіпервізор, права доступу, віртуальна машина.

Тема даної кваліфікаційної роботи магістра є актуальною, оскільки, в наш час, питання про якісне навчання студентів постає дуже часто перед викладачами, особливо надання практичних знань.

Ця робота присвячена обґрунтуванню ефективності застосування технології віртуалізації як з погляду викладацької діяльності, так і ефективності самої технології.

Вибір підходу до опису ефективності застосування технології здійснюється на підставі результатів експериментального впровадження технології віртуалізації в навчальний заклад, який займається підготовкою спеціалістів ІТ.

ABSTRACT

Methods and means of virtualization to provide educational process at the Novovolyn Electromechanical College // Master's thesis // Nataliya Anatoliivna Romashevska // TNTU, computer engineering, SID-II group // Ternopil, 2022 // p. – 78, fig. - 46, tab. – 3, add. – 1, bibliography. - 21.

Keywords: virtualization, server, SQLServer, operating system VMware, Active Directory, hypervisor, access rights, virtual machine.

The topic of this master's qualification work is relevant, because, nowadays, the question of high-quality education of students arises very often before teachers, especially the provision of practical knowledge.

This work is devoted to substantiating the effectiveness of the application of virtualization technology from both the point of view of teaching activity and the effectiveness of the technology itself.

The choice of the approach to the description of the effectiveness of the technology application is made based on the results of the experimental implementation of the virtualization technology in the educational institution engaged in the training of IT specialists.

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ .	8
ВСТУП	9
РОЗДІЛІ ЕКСПЕРИМЕНТАЛЬНЕ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ У ПРОЦЕС НАВЧАННЯ.....	12
1.1 Огляд технології віртуалізації.....	13
1.2 Визначення завдань експерименту.....	20
1.3 Налаштування всього необхідного для проведення експерименту	21
1.4 Встановлення та налаштування сервера	23
1.5 Обробка результатів експерименту	24
1.6 Аналіз опрацьованих результатів.	26
1.7 Висновок	27
РОЗДІЛ 2 СЕРВЕРНА ВІРТУАЛІЗАЦІЯ. ЗАГАЛЬНІ ПОНЯТТЯ.....	28
2.1 Технологія віртуалізації за допомогою "Гіпервізор"	28
2.1.1 Опис віртуалізації Гіпервізор.....	28
2.1.2 Віртуалізація серверів баз даних	31
2.1.3 Ефективне використання ресурсів	31
2.1.4 Спрощене адміністрування	32
2.1.5 Динамічність ІТ-інфраструктури.....	32
2.1.6 Реалізація.....	32
2.2 Процес створення віртуального сервера.....	34
РОЗДІЛ 3 ЛОКАЛЬНА ВІРТУАЛІЗАЦІЯ НАСТІЛЬНИХ СИСТЕМ НАВЧАЛЬНОГО ЗАКЛАДУ	40
3.1 Переваги та використання.....	40
3.2 Робота з App-V	42

3.3 Контроль доступу, розподіл прав під час роботи через vCenter	53
3.4 Налаштування сертифікатів SSL	62
3.5 Висновки	64
РОЗДІЛ4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ	65
4.1 Охорона праці	65
4.2 Застосування віртуалізації у навчанні з безпеки в надзвичайних ситуаціях	68
ВИСНОВОК.....	72
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	73
Додаток А. Тези конференцій	75

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І
СКОРОЧЕНЬ

App-V – asociative parallel processor-virtualized

CA – certificate authority

DA – Direct Access

GB – Giga Bite

HDD – Hard Disk Device

MB – Mega Bite

MDOP – Microsoft Desktop Optimization Pack

RAM -Random Access Memory

SC – Shared Cache

SCSI – Small computer system interface

SSL – Secure Socket Layer

TLS – Transport Layer Security

AT або AD – Актив Директори або Active Directory

БД - База Даних

ВМ – Віртуальна машина

ІТ чи IT – Інформаційна технологія або Information Technologies

ОС чи OS – Операційна Система чи Operation System

ПК чи PC – Персональний Комп'ютер чи Personal Computer

СУБД - Система Управління Базами Даних

ВСТУП

Актуальність теми. В умовах сучасних технологій та швидкості їх розвитку далеко не завжди вдається наздогнати технічний прогрес, особливо це стосується ІТ технологій. На жаль дуже часто виходить саме так що після того, як нам вдається освоїти одну технологію, витративши на її вивчення величезну кількість часу і сил, їй на зміну приходить інша – більш сучасна, далеко не завжди, швидко-освоювана, але необхідна до вивчення. І, на жаль, в умовах навчального закладу далеко не всі технічні дисципліни можна освоїти, без можливості спробувати той чи інший принцип у дії.

Саме таку можливість надає використання віртуалізації під час вивчення профільних предметів і навчальної практики, що дає можливість випускати технічних фахівців з адміністрування серверів або серверних систем. Саме застосування цих технологій надає можливість, при виникненні тієї чи іншої проблеми, значно скоротити час на її вирішення.

Оскільки фізично неможливо на заняттях надати кожному студенту свій власний сервер для навчання і після однієї навчальної пари занять надати в такому ж робочому стані ці самі сервери для наступної групи, виникає необхідність використовувати технологію віртуалізації для організації навчального процесу.

Мета кваліфікаційної роботи. Метою даної роботи є дослідження методів і засобів віртуалізації з метою використанні даної технології у процесі навчання.

Задачі кваліфікаційної роботи:

- Огляд технологій віртуалізації;
- Проаналізувати результати експерименту;
- Розробити алгоритм роботи на базі віртуальних серверів;
- Здійснити практичну реалізацію віртуальних систем в навчальному закладі;
- Експериментально дослідити застосування технології віртуалізації в навчальному закладі на базі 2 кабінетів;

– Дослідити та проаналізувати результати впровадження технології віртуальних серверів в навчальному закладі.

Об’єкт дослідження: система віртуалізації для забезпечення навчального процесу.

Предмет дослідження: технологія віртуалізації гіпервізор, критерії ефективного використання віртуальних сервісів, система розподілу доступу.

Методи дослідження: методи експериментального аналізу та дослідження операцій; методи тестування інформаційних систем.

Наукова новизна дослідження полягає в запровадженні технології віртуалізації програм, що дозволило спростити розгортання, адміністрування, оновлення та видалення програмного забезпечення, що використовуються під час навчального процесу.

Практичне значення результатів кваліфікаційної роботи. Дані, отримані в результаті проведених досліджень використані в навчальному процесі для підготовки фахівців у галузі розробки та створення бази даних у SQL, WEB програмування та адміністрування операційних систем.

Публікації. Результати дослідження апробовано на

1. Наталія Ромашевська, Олена Прокопюк, Руслан Жаровський. Використання технологій віртуалізації у процесі навчання студентів. Матеріали X науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (7-8 грудня 2022 року), ст.141

2. Олена Прокопюк, Наталія Ромашевська, Яна Войтович, Руслан Жаровський. Автоматизація та оптимізація навчального процесу в вищих навчальних закладах. Матеріали X науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (7-8 грудня 2022 року), ст.141

3. **Структура роботи.** До складу кваліфікаційної роботи магістра входить розрахунково-пояснювальна записка. Розрахунково-пояснювальна записка містить

вступ, 4 розділи, загальні висновки, список використаної літератури і додатки.

Обсяг роботи: розрахунково-пояснювальна записка – 78 арк. формату А4.

РОЗДІЛІ

ЕКСПЕРИМЕНТАЛЬНЕ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ У ПРОЦЕС НАВЧАННЯ

Віртуалізацією називають процес виокремлення комп'ютерних ресурсів один від одного, що дозволяє зменшити залежність між ними. Це спрощує управління змінами у системі з допомогою їх локалізації у тому чи іншому шарі ізольованих з допомогою віртуалізації ресурсів.

В фізичному середовищі апаратне забезпечення, операційна система та програми тісно пов'язані і сильно залежать один від одного. У віртуальному середовищі, навпаки, віртуальні елементи логічно ізольовані та залежать один від одного значно менше.

Щоб краще зрозуміти, як це відбувається, розглянемо принцип «машинної віртуалізації». На хост-комп'ютері встановлюється програмний комплекс - гіпервізор віртуальних машин, що здійснює поділ ресурсів системи: оперативної пам'яті, процесора та пристроїв введення-виведення між віртуальними машинами. Кожна віртуальна машина (ВМ) емулює звичайний фізичний комп'ютер, і відповідно на ній може бути розгорнута операційна система та програми. При цьому машинна віртуалізація забезпечує такий ступінь ізольованості та надійності, якби кожна віртуальна машина працювала незалежно на своєму власному обладнанні.

Віртуальну машину можна легко зупиняти, робити резервні копії та запускати заново, оперуючи набором файлів, що описують поточний стан її оперативної пам'яті та жорсткого диска. Оскільки у віртуальній машині емулюється віртуальне обладнання, універсальне всім хост-систем, віртуальні машини можна переносити інші комп'ютери, навіть якщо апаратна конфігурація цих систем не збігається.

1.1 Огляд технології віртуалізації

Види віртуалізації.

Віртуалізація платформ - це створення програмних систем на основі існуючих апаратно-програмних комплексів, які залежать або не залежать від них

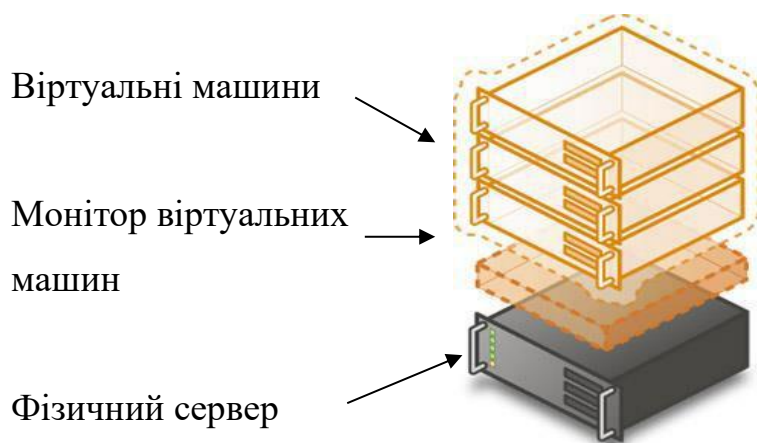


Рис. 1.1. Віртуалізація платформ

Часткова емуляція (нативна віртуалізація)

В цьому випадку віртуальна машина використовує для віртуалізації лише необхідну кількість апаратного забезпечення (оперативної пам'яті, пам'яті на жорсткому диску та інше) для того, щоб вона могла бути запущена саме ізольовано (рис.1.2).



Рис.1.2. Нативна віртуалізація

Недоліком даного виду віртуалізації є залежність віртуальних машин від архітектури апаратної платформи.

Приклади продуктів для віртуалізації: Virtual PC, VMware Workstation, VMware ESX Server, Virtual Iron, VirtualBox, VMware Server, Parallels Desktop та інші.

Повна емуляція

Віртуальна машина повністю віртуалізує все своє апаратне забезпечення при збереженні гостьової операційної системи в незмінному вигляді (рис.1.3).

Приклади емуляторів: Bochs, PearPC, QEMU, Hercules Emulator.



Рис.1.3. Повна емуляція

Часткова віртуалізація, а також "віртуалізація адресного простору"

Віртуальна машина частково симулює відразу кілька екземплярів апаратного оточення, зокрема навіть адресний простір (рис.1.4).

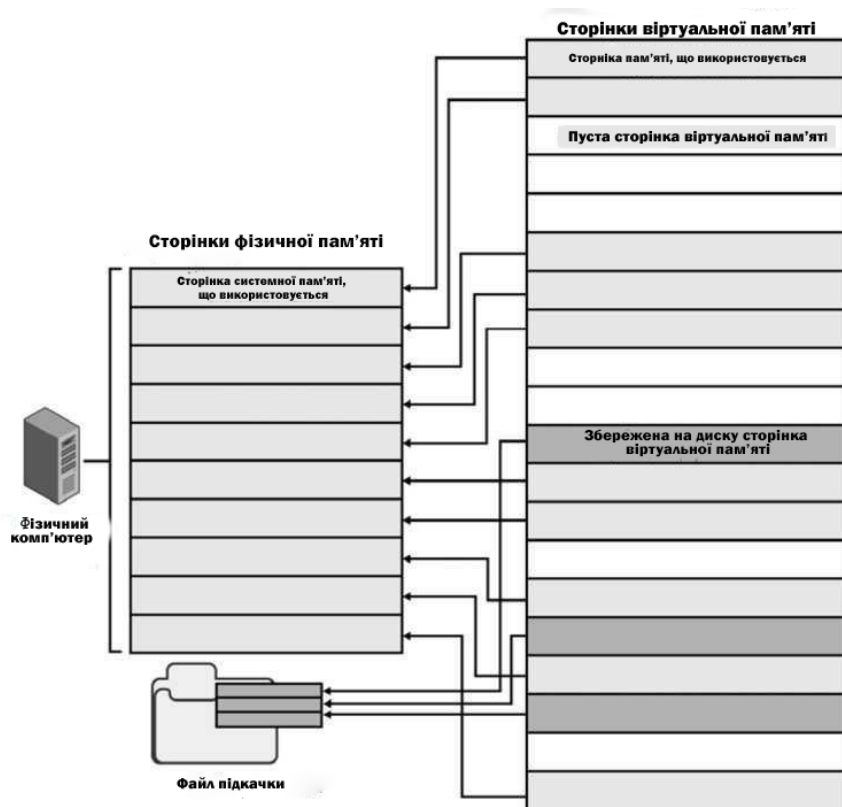


Рис.

1.4. Часткова

віртуалізація

Віртуалізація рівня операційної системи

Віртуалізація фізичного сервера є лише на рівні операційної системи з метою створення кількох захищених віртуалізованих серверів одним фізичним.

Приклади віртуалізації рівня ОС: FreeBSD Jails, Virtuozzo, Linux-VServer, OpenVZ, Solaris Containers.

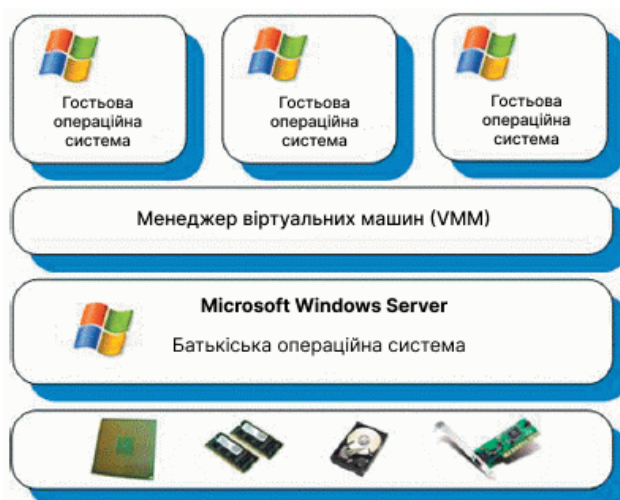


Рис.1.5. Віртуалізація рівня операційної системи

Паравіртуалізація

Симуляція апаратного забезпечення здійснюється за допомогою спеціального програмного інтерфейсу застосувань – API, для взаємодії з гостьовою операційною системою (рис.1.6).

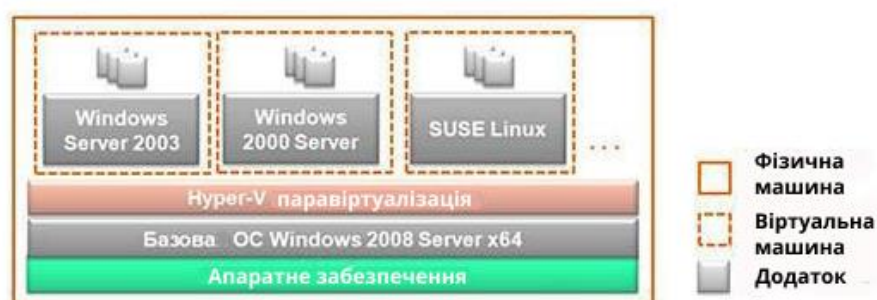


Рис 1.6. Паравіртуалізація

Віртуалізація рівня додатків

В цьому випадку сама програма розміщується в контейнер з необхідними елементами для своєї роботи: файлами реєстру, файлами конфігурації, користувальницькими системними об'єктами. В результаті виходить додаток, який не вимагає установки на аналогічній платформі. Прикладом такого підходу є Thinstall, Altiris, Trigenex, Softricity.



Рис.1.7. Віртуалізація програм.

Віртуалізація ресурсів

Віртуалізація ресурсів концентрує, абстрагує та спрощує управління групами ресурсів, таких як сховища даних, мережі та простору імен (рис.1.8).

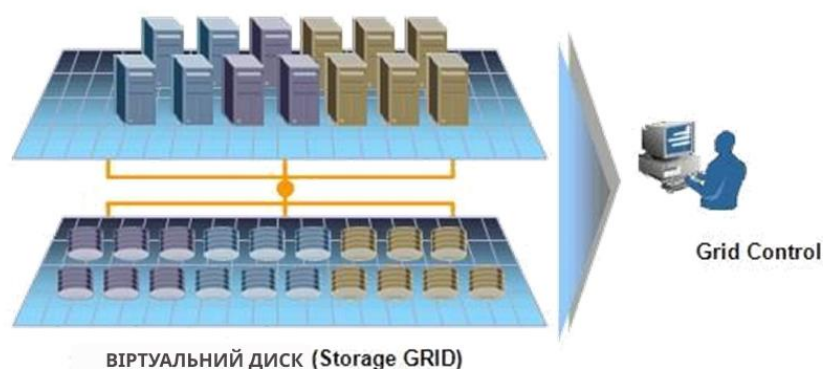


Рис.1.8. Віртуалізація ресурсів

Кластеризація комп'ютерів, розподілені обчислення

Застосовується при об'єднанні окремих комп'ютерів у глобальні системи, що вирішують спільно загальне завдання (рис.1.9).

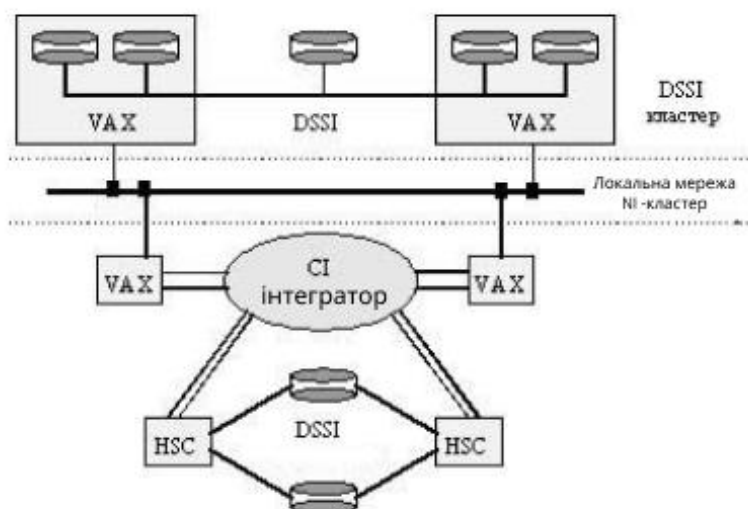


Рис.1.9. Кластеризація комп'ютерів

Об'єднання, агрегація та концентрація компонентів

Організація кількох фізичних чи логічних об'єктів у пули ресурсів, тобто групи, які представляють зручні інтерфейси користувача. Приклади:

- віртуальні приватні мережі;
- багатопроцесорні системи;
- RAID-масиви;

- віртуалізація систем зберігання SAN (Storage Area Network);
- трансляція мережевих адрес.



Рис.1.10. Віртуалізація систем зберігання

Інкапсуляція

Це процес створення системи, що надає користувачеві зручний для роботи інтерфейс та приховує подробиці складності своєї реалізації (рис.1.11).

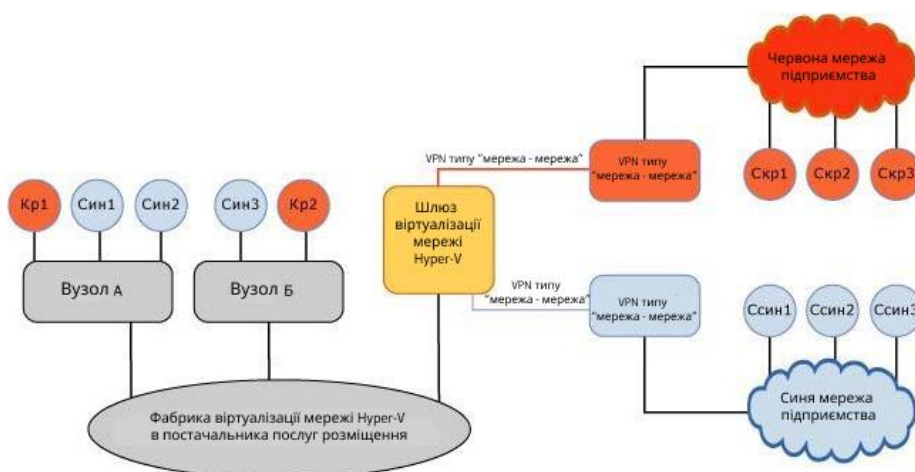


Рис.1.11. Шлюз віртуалізації мереж Hyper-V

Поділ ресурсів

В процесі віртуалізації при цьому підході, зазвичай, відбувається поділ якогось одного дуже великого ресурсу кілька об'єктів, що зручні у використанні. У мережах зберігання даних прийнято називати зонуванням ресурсів.

Переваги віртуалізації

Економія на апаратному забезпеченні відбувається за розміщення кількох віртуальних серверів однією фізичному сервері (рис.1.12).



Рис.1.12. Заміна 3-х серверів одним за допомогою VMware

Віртуалізація кількох машин одному хості

На одному хості може бути запущено кілька віртуальних машин, які об'єднані у віртуальну мережу

Можливості щодо навчання роботи з операційними системами

Для різних студентів можна створити репозиторій, готових до використання віртуальних машин з різними гостьовими операційними системами та запускати їх у міру необхідності з метою навчання. Їх можна запускати, налаштовувати, експериментувати, а отім спокійно відновлювати за потреби.

Підвищена керованість віртуальних машин

Копії файлів з віртуальною машиною можна розмістити, перенести на інший ПК і там відразу запускати. Не потрібно створювати жодних образів для міграції, бо віртуальна машина не прив'язана до конкретної апаратури.

Організація встановлення додатків

віртуальне оточення може бути створено конкретного використання, встановивши у ній все необхідне програмне забезпечення.

Підвищена керованість віртуальних машин

При використанні віртуальних машин можна створювати резервні копії (бекапів), створення знімків станів віртуальних машин («снапшотів») та відновлення після збоїв.

Недоліки віртуалізації

- Неможливість емуляції всіх пристроїв.
- Деякі платформи віртуалізації вимогливі до апаратного забезпечення (VMware, ESX Server).
- Хороші платформи віртуалізації коштують грошей (але є багато безкоштовних альтернатив).

1.2 Визначення завдань експерименту

В нашому навчальному закладі був проведений експеримент у ході, якого вдалося з'ясувати та наочно порівняти працездатність та стабільність роботи сервера з технологією віртуалізації порівняно із звичайним використанням ПК.

Метою експерименту було визначити працездатність, стабільність роботи та часу витраченого на відновлення працездатності сервера з технологією віртуалізації порівняно із звичайним використанням ПК у процесі навчання.

Для цього експеримент проводився у двох аудиторіях для підготовки фахівців у галузі розробки та створення бази даних у SQL з усім необхідним програмним забезпеченням. В обох аудиторіях встановлюється стандартне програмне забезпечення для навчання фахівців: Мови програмування, Mathcad, AutoCAD, MS Office та інше. Єдиною відмінністю є саме те, що в одній аудиторії встановлюється сервер, налаштовується Active Directory та домен. Далі - розгортається VMware з 12 віртуальними машинами, на одній встановлюється SQL Server - для навчання розробників, після закінчення установки та налаштування - знімається образ для перекидання на решту 11 віртуальних машин та резервного відновлення на випадок непередбачених проблем.

В іншій аудиторії на навчання розробників – кожному комп'ютері встановлюється VMware, і однієї віртуальної машині встановлюється OS Linux, у

якому ставиться SQL Server, налаштовується, після цього зберігається образ однієї віртуальної машини і ставиться у інші 11 комп'ютерів.

Весь експеримент складається із трьох частин.

Мета першої частини експерименту – підготовка навчальних аудиторій, тобто. встановлення та налаштування програмного забезпечення.

Мета другої частини експерименту – експериментальна перевірка працездатності та стабільної роботи двох аудиторій, а також фіксування всіх випадків технічних проблем та фіксування часу на їх усунення.

Мета третьої частини – підрахунок та обробка всіх отриманих у ході експерименту даних та висновки.

1.3 Налаштування всього необхідного для проведення експерименту

Кількість випробуваних ПК - 24 .

Кількість аудиторій – 2 по 12 ПК у кожній. (рис.1.13, рис.1.14) Параметри ПК – OS Windows 7x32, HDD 500Gb RAM 4Gb (3,41 доступних через 32-х бітну операційну систему).

Мережа в обох аудиторіях 100Mb (обмежена параметрами свіча TP-LINK SF1024D).

Необхідне програмне забезпечення для повноцінного використання ПК розробниками – OS Windows 7, MS office 2010, мови програмування – Visual Studio, C++, C#, VMware з встановленим на ньому ОС Linux та SQL Server. Для оптимальної роботи доменної мережі вибирається сервер із наступними параметрами – CPU Core i7 3.0, RAM 12Gb HDD 500GB 7200RPM, поділений на 2 диски. Для операційної системи та встановленого програмного забезпечення - 320GB та 100GB для резервних образів з VMware, драйвера та дистрибутиви програм необхідних для адміністрування.

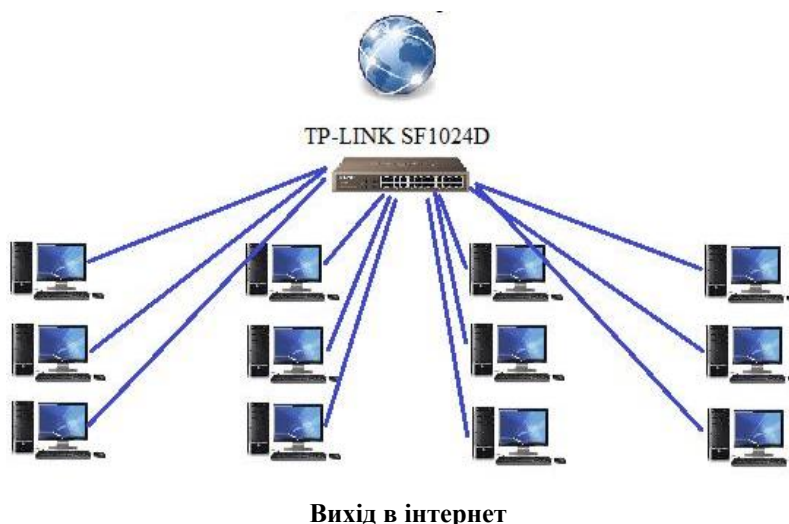


Рис.1.13. Схема аудиторії "А" звичайна мережа, VMware і SQL Server встановлений на кожному стаціонарному ПК

В якості операційної системи на сервері в аудиторії «Б» (рис.1.14) вибирається Windows Server 2008, він зручніший в адмініструванні, ніж Windows Server 2012 і більш функціональний у плані адміністрування доменних мереж, ніж попередні версії серверних операційних систем сімейства Windows.

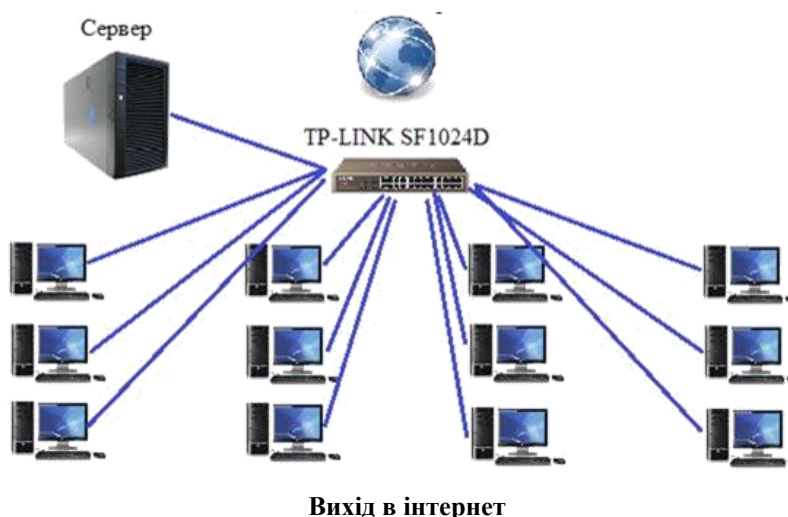


Рис.1.14. Схема аудиторії «Б» доменна мережа, VMware встановлений лише на сервері

Для аудиторії «Б» відмінностями після встановлення всього програмного забезпечення є те, що нам не потрібно встановлювати VMware з ОС Linux та SQL Server на жодний ПК крім сервера і замість робочої групи вводиться ПК в єдиний домен із сервером. Було прийняте рішення доменну мережу використовувати

через, можливості зручного адміністрування та створення єдиних правил для доменної групи "студенти". Завдяки доменній архітектурі - є можливість обмежити для учня доступ на сервер, та дозволити тільки до виділеному йому віртуальному простору, тобто повністю заборонити йому доступ до файлів із резервними образами та до операційної системи сервера.

Також, завдяки налаштованому Active Directory, здійснюється моніторинг та логування змін кожного учня для подальшого виявлення вразливостей та їх усунення.

1.4 Встановлення та налаштування сервера

Після того як встановлюється операційна система Windows Server 2008 R2. У ролях сервера підключається та налаштовується Active Directory, додаються користувачі облікові записи для домену такі як - "Студент 1", "Студент 2", ... , "Студент 12", для того, щоб у кожного учня був свій доступ до сервера, під своїм обліковим записом. Далі встановлюється VMware з ОС Linux, SQL Server і налаштовується кожного учня віртуальний SQL Server. Як резерв - під обліковим записом адміністратора, на сервері піднімається ще одну (13 VMware), але доступ на неї для всіх крім викладача і адміністратора закривається з міркувань політики безпеки (рис.1.15).

Таким чином, в мережі аудиторії «Б» є всього 13 комп'ютерів, включаючи сервер, але після підключення кожного ПК до сервера для роботи з SQL, що навчається працює виключно на своєму SQL сервері.

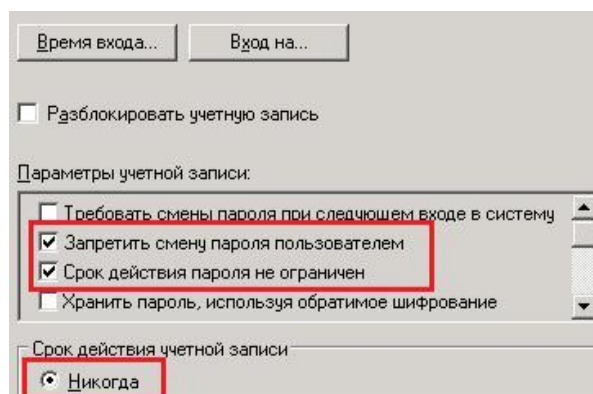


Рис.1.15. Налаштування пароля для студента Active Directory

Недолік такого методу полягає в необхідності використовувати досить потужний сервер, який у свою чергу коштує дорожче, ніж звичайний ПК. Проте плюсами цієї технології є – розвантаження мережі, т.к. завдяки Active Directory налаштовується доступ на сервер і є можливість заборонити будь-яке виявлення даних віртуальних ПК з ОС Linux та SQL Server у спільній мережі. Найголовнішим плюсом є керованість, моніторинг активності користувачів та налаштування споживаних ресурсів для VMware для всіх користувачів так наприклад для кожного співробітника, що навчається, ми на сервері виділяємо по 512 MB ОП та 5GB місця на сервері. Для самого сервера залишається при максимальному навантаженні 6GB ОП та 260GB дискового простору, чого більш ніж достатньо для адміністрування по CPU при одночасному сеансі - 12 користувачів, йде навантаження 30-40%, що теж цілком допустимо.

1.5 Обробка результатів експерименту

Після закінчення 4-х місяців виявлено 36 зафіксованих проблем (рис.1.16) в аудиторії «А» та 12 технічних проблем в аудиторії «Б» (рис.1.17).

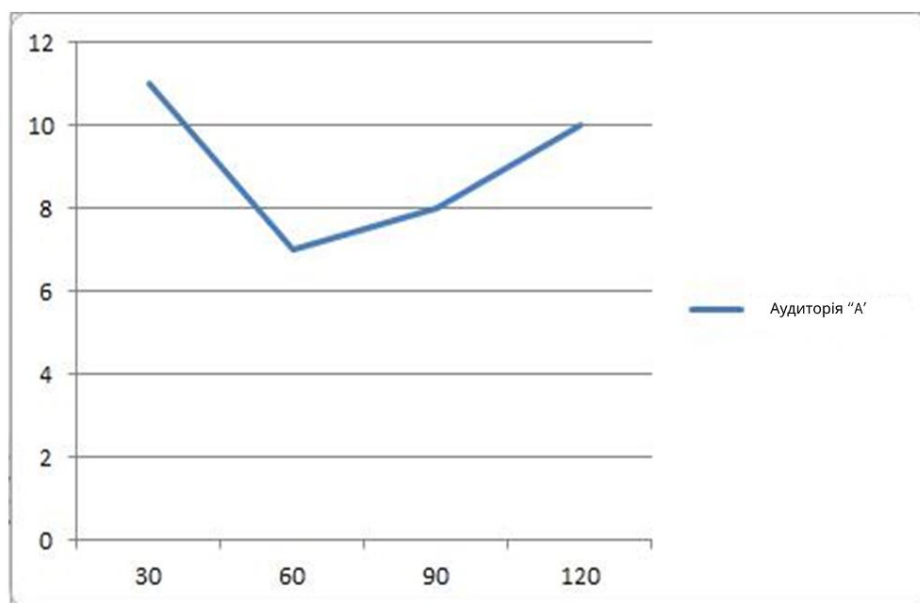


Рис.1.16. Графік технічних проблем аудиторії «А»

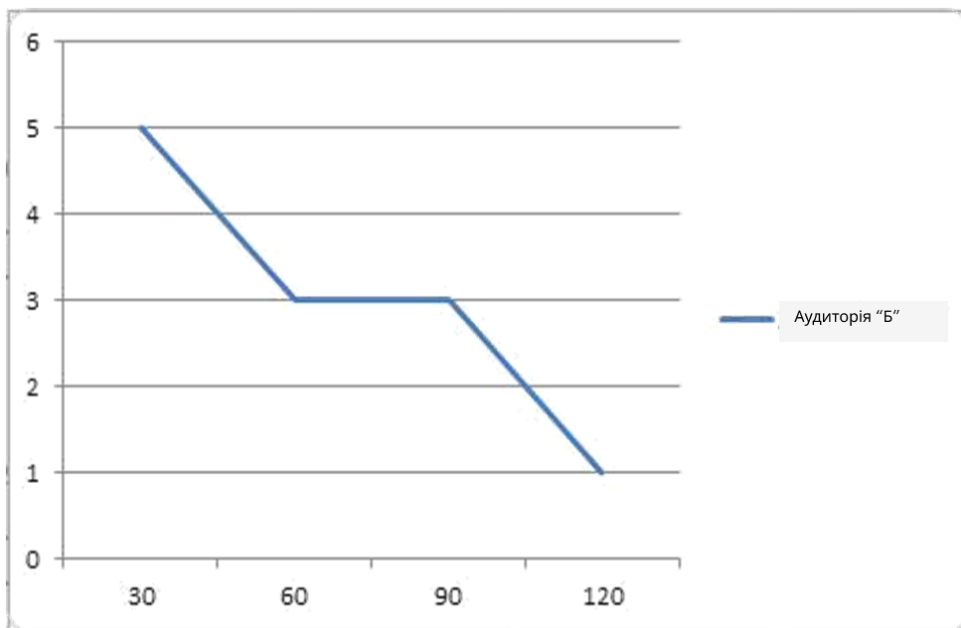


Рис.1.17. Графік технічних проблем аудиторії «Б»

Найчастішими проблемами в аудиторії «А» були слабка мережа, а також через велику кількість віртуальних ПК свіч не встигав обробляти запити і з мережі часто відключалися різні ПК. Також мало місце випадкове видалення ПЗ VMware з резервним файлом. Як правило, файл образ, з налаштованим на ньому Linux і SQL Server, має вагу як мінімум 4,4GB. Отже, перекидання цього файлу по мережі або через USB накопичувач на ПК, де він зник, займає близько 40 хвилин, а встановлення та налаштування VMware з Linux та SQL Server не менше 2х годин.

Найчастішими проблемами в аудиторії «Б» виявилися складність налаштування політики безпеки та деяка специфіка в адмініструванні ролей, прав доступу. Дуже багато часу спочатку йшло на освоєння принципів адміністрування. Однак, після того як вдалося засвоїти адміністрування VMware, кількість технічних збоїв скоротилося до 1 на місяць і витрачений час на усунення технічних проблем також вдалося скоротити (табл. 1.1).

В таблиці 1.1 по аудиторіям «А» та «Б» показано всі технічні проблеми та витрачений час на їх усунення за 4 місяці експерименту.

Таблиця 1.1

Результат технічних проблем за 4 місяці

Аудиторія	1й місяць		2й місяць		3й місяць		4й місяць	
	Техн. проблем (кількість)	Затрачено часу (хв)	Техн. проблем (кількість)	Затрачено часу (хв)	Техн. проблем (кількість)	Затрачено часу (хв)	Техн. проблем (кількість)	Затрачено часу (хв)
А	11	275	7	260	8	350	10	320
Б	5	120	3	60	3	50	1	10

1.6 Аналіз опрацьованих результатів.

Основні результати проведеного експерименту:

Допрацьована та повністю налаштована доменна система разом з технологією віртуалізації на базі VMware дозволяє в 3 рази скоротити випадки технічних збоїв, а час усунення цих збоїв у 5 разів.

Система проста у користуванні та зрозуміла. Проте політики безпеки та винятків потребують ретельного та уважного налаштування.

Система Windows Server 2008 R2 з технологією віртуалізації дозволяє дати доступ до свого власного віртуального сервера і дати повноцінну можливість спробувати, налаштувати, зіпсувати та відновити її самостійно, без шкоди для інших студентів, при невдачі при відновленні стажером, що навчається - викладач або системний адміністратор здатний відновити працездатність SQL Server протягом 5-10 хвилин (на відміну від звичайного методу 40 хвилин або більше). Технологія VMware забезпечена необхідним набором функціонального забезпечення.

В експериментальній частині проекту брали участь студенти коледжу, викладачі та адміністратор мережі.

Експеримент доводить, що робота з Active Directory та віртуалізацією дозволяє кожному студенту індивідуально навчатися технологіям без будь-якого ризику для оточуючих (тобто без варіантів зриву для інших учнів). Також

дозволяє в середньому в 3 рази скоротити ризик виникнення технічної проблеми, і що найголовніше зменшити час на вирішення проблем, що виникли.

1.7 Висновок

У ході цього експерименту:

1. Розглянуто алгоритми та методи впровадження технології віртуалізації в навчальний процес;
2. Проведено аналіз існуючого апаратного забезпечення для апробації технології;
3. Підібрано та проаналізовано найкращі програмні рішення для реалізації на існуючому апаратному забезпеченні;
4. Проведено встановлення та налаштування ПЗ на локальних машинах та сервері;
5. Протестовано застосування технології віртуалізації в двох варіантах реалізації.

Результати:

- Допрацьована та повністю налаштована доменна система разом з технологією віртуалізації на базі VMware дозволяє в 3 рази скоротити випадки технічних збоїв, а час усунення цих збоїв у 5 разів.
- Система проста у користуванні та зрозуміла.
- Проте політики безпеки та винятків потребують ретельного та уважного налаштування.

РОЗДІЛ 2

СЕРВЕРНА ВІРТУАЛІЗАЦІЯ. ЗАГАЛЬНІ ПОНЯТТЯ

2.1 Технологія віртуалізації за допомогою "Гіпервізор"

2.1.1 Опис віртуалізації Гіпервізор

Гіпервізор – це програма або апаратна схема, що забезпечує або дозволяє одночасне, паралельне виконання декількох або навіть багатьох операційних систем на тому самому хост-комп'ютері. Гіпервізор також забезпечує ізоляцію операційних систем один від одного, захист та безпеку, поділ ресурсів між різними запущеними ОС та управління ресурсами.

Гіпервізор може надавати працюючим під його керуванням, на одному хост-комп'ютері, ОС засоби зв'язку та взаємодії між собою так, ніби ці ОС виконувались на різних фізичних комп'ютерах.

Гіпервізор сам по собі певною мірою є мінімальною операційною системою. Він надає запущеним під його керуванням операційним системам сервіс віртуальної машини, віртуалізуючи або емулюючи реальне (фізичне) апаратне забезпечення конкретної машини. І керує цими віртуальними машинами, виділенням та звільненням ресурсів їм. Гіпервізор дозволяє незалежне "ввімкнення", перезавантаження, "вимикання" будь-якої з віртуальних машин з тієї чи іншої ОС. При цьому операційна система, що працює в віртуальній машині під керуванням гіпервізора, може, але не зобов'язана знати, що вона виконується у віртуальній машині, а не на реальному апаратному забезпеченні.

Гіпервізори першого типу працюють безпосередньо на апаратних ресурсах фізичного комп'ютера. Вони функціонують як програма управління. Гостьові операційні системи, що працюють у віртуальних машинах, розташовуються рівнем вище за гіпервізор.

Так як гіпервізори першого типу працюють безпосередньо на апаратних ресурсах комп'ютера вони, як правило, забезпечують кращу швидкодію та безпеку, ніж будь-які інші типи гіпервізорів.

В як приклади гіпервізорів першого типу можна навести:

- Microsoft Hyper-V;
- Citrix XenServer;
- VMware ESX Server.

Гіпервізори другого типу працюють у середовищі операційної системи, запущена на фізичному комп'ютері. Гостьові операційні системи, у свою чергу, працюють у віртуальних машинах, що розташовані над рівнем гіпервізора.

Як видно з порівняння двох типів гіпервізорів, операційні системи у віртуальних машинах, які працюють під керуванням гіпервізора другого типу, знаходяться на один рівень далі від апаратних ресурсів фізичного комп'ютера. Цей додатковий рівень є причиною зниження продуктивності віртуальних машин гіпервізорів другого типу. Крім того, кількість віртуальних машин, які можна запустити на прийнятному рівні продуктивності з тієї ж причини значно обмежена.

Прикладами гіпервізорів другого типу є:

- Microsoft Virtual Server;
- VMware Server.

Гіпервізори з монолітною архітектурою мають на увазі використання драйверів, спеціально написаних з урахуванням роботи з гіпервізором. Вони керуються гіпервізором і, по суті, виконуються серед гіпервізора.

Монолітна архітектура має певні переваги, але в той же час має досить серйозні недоліки. Однією з основних переваг можна назвати відсутність необхідності в батьківській операційній системі, тому що всі гостьові операційні системи працюють з апаратними засобами фізичного комп'ютера за допомогою драйверів в гіпервізорі.

З іншого боку той факт, що драйвери мають бути спеціально написані для гіпервізора, створює певні труднощі. Враховуючи різноманітність та кількість пристроїв, ймовірність того, що для конкретного пристрою не знайдеться спеціальний драйвер, досить висока. Це веде до необхідності тісної співпраці між виробниками гіпервізорів та апаратних пристроїв, з метою забезпечити спеціалізовані драйвери. Це своє чергу означає, що виробники гіпервізорів даної

архітектури залежать від виробників апаратних пристроїв, оскільки без спеціалізованих драйверів їхній продукт немає цінності. Все це веде до того, що кількість пристроїв, на яких можуть працювати гіпервізори даної архітектури, зазвичай менше, ніж кількість пристроїв, на яких здатні працювати гіпервізори іншої архітектури.

Ця архітектура також становить потенційну загрозу безпеці. Так як драйвери виробників пристроїв з перспективи гіпервізора вважаються стороннім кодом, виконання їх у гіпервізорі на привілейованому рівні може становити небезпеку.

Приклад гіпервізора з монолітною архітектурою є VMware ESX Server.

Гіпервізори мікроядерної архітектури не потребують спеціалізованих драйверів, оскільки вони мають операційну систему, що знаходиться в батьківському розділі. Цей батьківський розділ забезпечує середовище, де запускаються драйвери для апаратних пристроїв фізичного комп'ютера. Розділ можна розуміти як одну із віртуальних машин, запущених на гіпервізорі.

В мікроядерній архітектурі необхідно встановити драйвери пристроїв лише для операційної системи, що у батьківському розділі. Немає потреби встановлювати драйвери для всіх віртуальних машин, оскільки коли у віртуальній машині виникає необхідність отримати доступ до фізичного пристрою комп'ютера, вона робить це шляхом звернення до батьківського розділу. Тобто в мікроядерній архітектурі у гостьових операційних систем немає можливості безпосередньо використовувати фізичні ресурси комп'ютера, вони роблять це тільки через запити батьківської операційної системи.

Мікроядерна архітектура має певні переваги в порівнянні з монолітною. По-перше, оскільки потреби у спеціалізованих драйверах немає, можливе використання всього спектра існуючого обладнання. По-друге, відсутність вбудованих драйверів знімає з гіпервізора додаткове навантаження, що робить його меншим і менш складним, відповідно більш надійним. По-третє, відсутність стороннього коду всередині гіпервізора (яким є драйвери) знімає ризик потенційних проблем з безпекою.

Однак мікроядерна архітектура має помітний недолік — необхідність батьківського розділу. Це додає додаткове навантаження на систему (здебільшого прийнятну), у зв'язку з необхідністю підтримки батьківського розділу та здійсненням та контролем запитів дочірніх розділів на фізичні ресурси комп'ютера.

Прикладом гіпервізора з мікроядерною архітектурою є Microsoft Hyper-V.

2.1.2 Віртуалізація серверів баз даних

Віртуалізація серверів баз даних є одними з основних напрямів цієї технології. Враховуючи необхідність у централізованому зберіганні інформації, яке забезпечують сервери з СУБД, та їх наявність у організаціях практично будь-якого рівня, роблять сервери баз даних найбільш очевидним претендентом на віртуалізацію.

Стосовно навчального закладу можна виділити відразу дві СУБД як потенційних кандидатів на віртуалізацію:

- MS SQL Server;
- Oracle.

Віртуалізація даних СУБД забезпечить низку переваг порівняно з традиційною моделлю розгортання СУБД. Розглянемо їх докладніше.

2.1.3 Ефективне використання ресурсів

Завдяки розміщенню СУБД на віртуальній машині основного сервера не потрібно купувати окремої фізичної машини до виконання цієї ролі. Крім того, з урахуванням невеликих розмірів спеціальності, можна з великою ймовірністю говорити про те, що ресурси виділеного для цієї мети сервера не будуть використовуватися повністю. Оскільки стосовно кафедри таких серверів потрібно два, по одному на кожен СУБД, необґрунтовані витрати зростуть вдвічі. Витрата електричних ресурсів також знижується.

2.1.4 Спрощене адміністрування

З використанням віртуалізації завдання з адміністрування серверів із СУБД значно спрощуються. Використовуючи знімки віртуальних машин, кластеризацію та можливість перенесення віртуальних машин усередині кластера дозволяють створити середовище, в якому час простою буде зведений до мінімуму. Крім того, при відмові віртуального сервера з СУБД час на відновлення роботи можна мінімізувати та практично усунути проблему втрати важливої інформації.

2.1.5 Динамічність ІТ-інфраструктури

Використання віртуалізації дозволяє здійснювати динамічний перерозподіл ресурсів між серверами, що дозволяє всій інфраструктурі підлаштовуватися під навантаження в кожен окремий час, забезпечуючи таким чином комфортну роботу всім користувачам.

2.1.6 Реалізація

Розглянемо традиційну модель розгортання СУБД. Без застосування віртуалізації, кожен окрему СУБД необхідно розгорнути на окремій фізичній машині. Це необхідно, щоб уникнути можливих конфліктів між різними СУБД. В результаті маємо мінімум два сервери із встановленими на них різними СУБД, як показано на рис. 2.1.

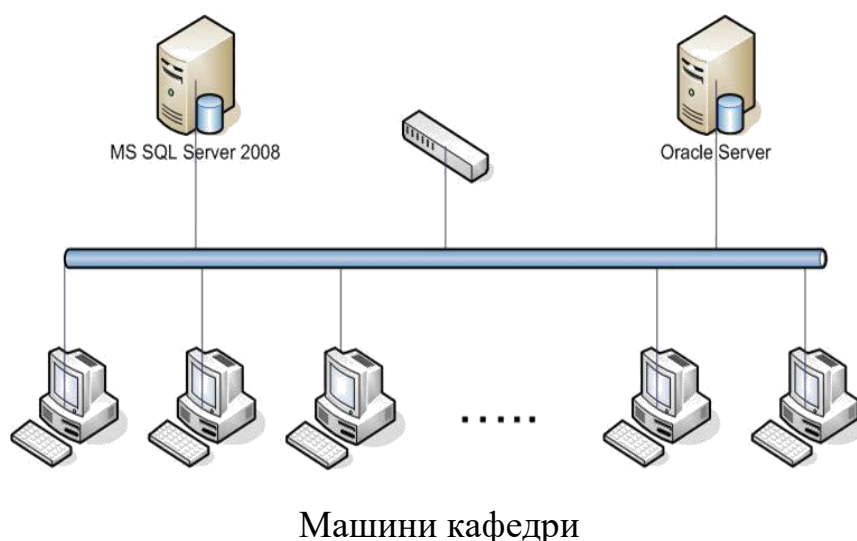


Рис. 2.1. Традиційна модель

Як видно з рисунка, у традиційній моделі є два окремі фізичні сервери. Клієнтські машини підключаються до мережі та працюють з тим сервером, який зараз необхідний. Розглянемо переваги та недоліки цієї моделі.

Перевага:

Простота реалізації — при такому способі розгортання серверів із СУБД не потрібні жодні додаткові дії, крім безпосередньо встановлення та налаштування СУБД на сервери.

Недоліки:

Низька стійкість до відмов - при виході з ладу фізичного обладнання сервера час простою буде вимірюватися годинами, якщо не добою.

Складність резервного копіювання — для резервного копіювання операційних систем у разі їх відмови доведеться використовувати стороннє програмне забезпечення, яке, зазвичай, вимагає додаткових вкладень.

Зазначені недоліки могли б бути вирішені, використовуючи реплікацію або подібні технології від виробників СУБД, але вони вимагатимуть ще одного сервера на кожну СУБД, що значно збільшить вартість системи.

Тепер подивимося, як дана система буде виглядати використовуючи технологію віртуалізації. В даному варіанті обидві СУБД розміщуються на одному фізичному сервері. Кожна СУБД встановлена на окремій віртуальній машині, щоб унеможливити конфлікти, як показано рис.2.2

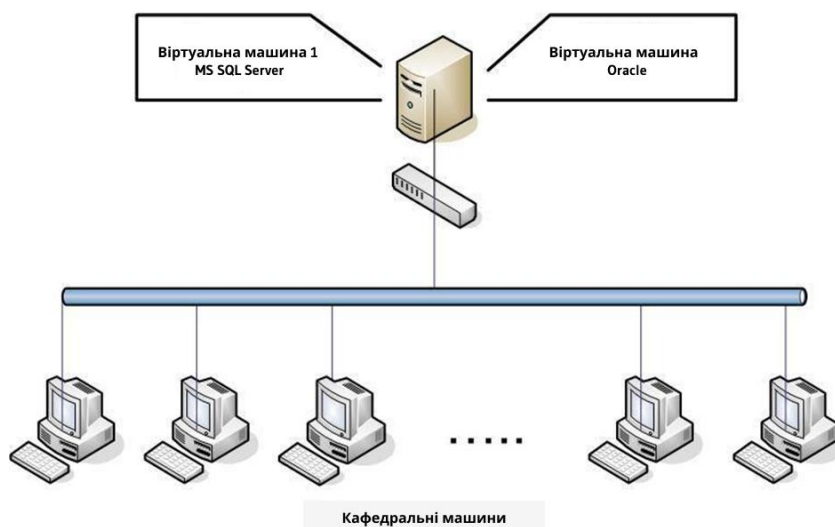


Рис.2.2. Використання віртуалізації

Як видно з малюнка, обидва сервери знаходяться на одному фізичному комп'ютері, але в різних віртуальних середовищах. Це одночасно надає кожній СУБД свою «чисту» операційну систему і скорочує кількість фізичного обладнання. Розглянемо переваги та недоліки даної системи.

Переваги:

Використання ресурсів — під час розміщення обох СУБД однією сервері ресурси сервера використовуються ефективніше, у результаті підвищується ефективність вкладення коштів.

Резервне копіювання та адміністрування — в силу вбудованих інструментів управління віртуальними машинами, резервне копіювання стає простим завданням. Знімки віртуальних машин можна зберігати окремо на відмовостійкому зовнішньому сховищі. Відновлення віртуального сервера після відмови операційної системи не займе півгодини. При цьому зробити це можна віддалено.

На перший погляд може здатися, що дана система менш надійна, тому що якщо сервер вийде з ладу, то вийдуть з ладу і обидва віртуальні сервери. Однак це проблема вирішується створенням кластера і більш докладно розглянута в останньому розділі.

2.2 Процес створення віртуального сервера

Віртуальний сервер є віртуальною машиною з встановленим на неї серверним програмним забезпеченням. Відповідно створення віртуального сервера практично нічим не відрізняється від створення віртуальної машини.

Створення віртуальних машин здійснюється за допомогою керуючої консолі Nureg-V, як показано на рис.2.3.

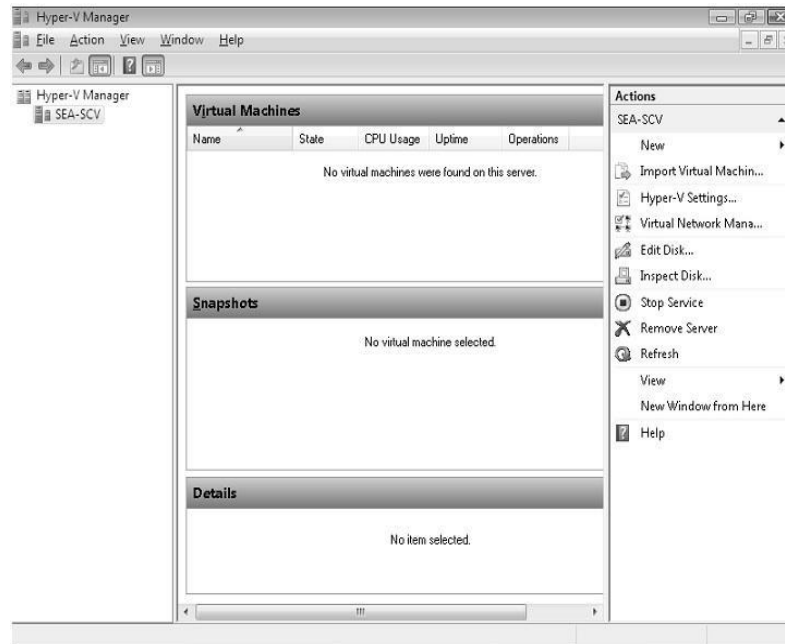


Рис.2.3. Керуюча консоль Hyper-V

Для створення нової віртуальної машини потрібно вибрати New | Virtual Machine. Процес створення віртуальної машини проходить згідно з наступними етапами:

- Назва віртуальної машини.
- Визначення розташування конфігураційних файлів віртуальної машини.
- Виділення пам'яті.
- Налаштування мережі.
- Налаштування системи зберігання даних.
- Встановлення операційної системи.

У ході створення віртуальною машини потрібно вказати місце для двох типів файлів: конфігураційні файли віртуальної машини і файл віртуального жорсткого диска.

Це можна зробити або при створенні віртуальної машини, або задати за замовчуванням для всіх створюваних віртуальних машин, як показано на рис.2.4.

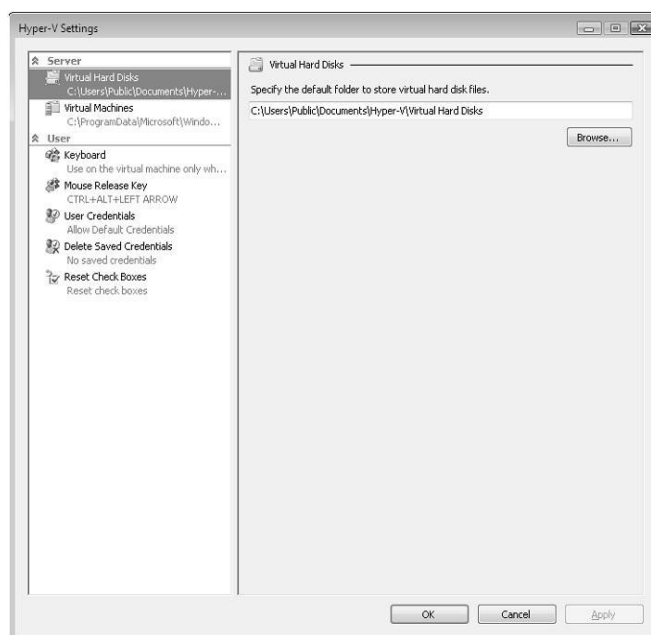


Рис. 2.4. Налаштування розташування конфігураційних файлів VM

Для доступу до віртуальних машин необхідно налаштувати на них доступ із мережі. У Hyper-V існує три види мережі:

- Зовнішня віртуальна мережа (External Virtual Networks).
- Внутрішня віртуальна мережа (Internal virtual networks).
- Приватна віртуальна мережа (Private Virtual Networks).

Зовнішня віртуальна мережа – віртуальна мережа, що має вихід «у зовнішній світ». При створенні мережі типу External необхідно вказати інтерфейс мережі, через який буде здійснюватися вихід назовні. При цьому фізичний інтерфейс втрачає всі налаштування мережі, і створюється віртуальний адаптер в хостовій ОС, до якого прив'язуються всі необхідні протоколи та налаштування. Фізичний інтерфейс залишається лише з одним протоколом: Virtual Network Switching Protocol [2].

Крім цього, у Windows Server 2008 R2 з'явилася можливість створювати мережі типу External, але при цьому однаково ізолювати їх від хостової ОС. Робиться це зняттям галочки.

Внутрішня віртуальна мережа – мережа, до якої можуть підключатися лише віртуальні інтерфейси – віртуальних машин та хостової ОС. До фізичного

інтерфейсу мережа типу Internal не прив'язується, і, відповідно, виходу «зовні» немає.

Приватна віртуальна мережа - те саме, що й Internal, за винятком того, що до такої мережі можуть підключатися тільки віртуальні машини. Мережа типу Private не має доступу ні до зовнішнього світу, ні до хостової ОС. У табл.2.1 наведено порівняльну характеристику всіх видів віртуальних мереж.

Таблиця 2.1

Типи віртуальних мереж

Тип віртуальної мережі	Між VM на хост машині	Між VM та батьківським розділом	Між VM та зовнішньою мережею
External	✓	✓	✓
Internal	✓	✓	
Private	✓		

Постановка задач дослідження та реалізації експерименту

В нашому навчальному закладі було вирішено провести практичну реалізацію локальної віртуалізації настільних систем. Основною метою було вивчення можливостей, полегшення адміністрування ПЗ в класах під час навчального процесу, і в подальшому надати можливість студентам самостійно налаштовувати сервери для спільного використання.

Для проведення даного дослідження виділено комп'ютерні класи, розроблено алгоритм досліджень та поставлено ряд задач.

Налаштувати сервер таким чином, щоб була можливість локальної віртуалізації програм, а це дозволить:

- Керувати установкою, оновленням та видаленням ПЗ на клієнських комп'ютерах;
- Розподіляти права доступу до різних ПЗ.

Для реалізації експерименту обрано технологію App-V

Для роботи звичайного користувача на сучасному комп'ютері можуть знадобитися десятки, якщо не сотні різних додатків. Встановити їх на комп'ютері -

це не проблема, але потрібно також їх тимчасово оновити, забезпечити роботу кількох версій (наприклад, MS Office 2003/2007/2010) і сумісність з іншими додатками, нарешті, видалити програми, коли вони перестають бути потрібними (не завжди видаляється додаток повністю, часто воно залишає лишні папки/файли, ключі реєстру).

Вирішити ці проблеми дозволяє віртуалізація програми. Ідея у технології наступна. Замість установки на цільовому комп'ютері програми встановлюються на спеціально підготовлений "чистий" комп'ютер (наприклад, на віртуальну машину з клієнтською ОС). На етапі встановлення та початкових налаштувань додатків спеціальна утиліта (в App-V вона називається Sequencer) відстежує всі залежності від даних додатків: файли, папки, ключі та вікна реєстру, системні бібліотеки та упаковує їх. Потім пакетований додаток переноситься на кінцевий комп'ютер, де запускається і працює в окремому контейнері (його також часто називають пісочниця). Вам не потрібно встановлювати і налаштовувати додаток, все, що вам потрібно – просто запустити його. При цьому у вас залишається можливість змінювати різні параметри віртуальних додатків, налаштовувати асоціації між розширеннями файлів і віртуальними додатками.

У централізованій інфраструктурі App-V ви можете вільно налаштовувати права на додатки, дозволяючи їх завантаження та запускати лише визначеним користувачам і групам. Один раз завантаживши додаток, користувач може відключитися від корпоративної мережі та перейти до команди, додаток буде запущено з локального кеша, без необхідності підключатися до сервера App-V (а може і не запускатиметься, якщо цього вимагають стандарти безпеки у вашій організації). Пакети віртуальних програм App-V можна поширювати, використовуючи існуючі засоби доставки програм на робочі станції (наприклад, SCCM 2007). App-V прекрасно працює з рішеннями термінального доступу та віртуалізації представлення (на базі MS RDS або Citrix XenApp), а також з VDI (VMware View, MS RDS, Citrix XenDesktop). В останньому випадку можна істотно заощадити на дисковому просторі віртуальних робочих станцій, створених на клієнтах лише для читання кешу для віртуальних програм і розмістивши його в

загальній папці, доступній для всіх клієнтів у мережі. Враховуючи, що встановлені на робочих станціях додатки можуть зайняти і 10 і 20 Гб вільного простору, економія отримується дуже великою. Після цього за допомогою App-V можна контролювати ліцензійну чистоту, обмежуючи кількість одночасно запущених екземплярів програм.

Інфраструктура App-V включає в себе такі компоненти:

Application Virtualization Client – компонент, що встановлюється на клієнтську робочу станцію або термінальний сервер, і дозволяє отримувати, оновлювати та запускати віртуальні додатки.

Microsoft Application Virtualization Sequencer - компонент, що встановлюється на цей комп'ютер, на якому виконується установка, настройка і упаковка додатків.

Application Virtualization Management Server – централізований сервер, який дозволяє публікувати віртуальні додатки, налаштовувати до них доступ, керувати ліцензіями та багато іншого.

Application Virtualization Management Console - оснастка, яка дозволяє підключатися й керувати одним або кількома App-V Management Server'ами. IIS Server – дозволяється підключатися до керуючого сервера App-V Management Server з консолі App-V

Management Console. SQL-сервер – використовується для розміщення бази даних керуючих серверів. Потоковий сервер, що дозволяє поширювати пакети додатків на клієнтські комп'ютери.

РОЗДІЛ 3

ЛОКАЛЬНА ВІРТУАЛІЗАЦІЯ НАСТІЛЬНИХ СИСТЕМ НАВЧАЛЬНОГО ЗАКЛАДУ

3.1 Переваги та використання

Стосовно кафедри, локальна віртуалізація настільних систем принесе найбільший зиск використовуючи технологію App-V. Віртуалізація програм дозволить спростити розгортання, адміністрування, оновлення та видалення програм, що використовуються на кафедрі під час роботи та навчання.

Локальна віртуалізація програм дозволяє:

- Централізовано управляти установкою програмних продуктів по всій кафедрі.
- Підтримувати усі програмні продукти в актуальному стані, усунути проблеми, що виникають при різних встановлених версіях однієї програми.
- Централізовано керувати видаленням програмних продуктів.
- Централізовано розподіляти права доступу тих чи інших користувачів до тих чи інших програмних продуктів.
- Підтримувати клієнтські комп'ютери у чистому стані, оскільки необхідність встановлення програмних продуктів безпосередньо відпадає.

Розглянемо додатки, що найбільш підходять на роль віртуалізованих додатків.

Таблиця 3.1

Список додатків

	Назва програми
1	MS Visual Studio 2010
2	MS Office 2010
3	Foxit Reader
4	MS SQL Management Studio

Розглянемо сценарії використання вищеописаних віртуалізованих програм.

Віртуалізація програм може надати якісно новий спосіб використання програмних продуктів. Щоб переконатися в цьому, спочатку подивимося на традиційну модель.

В традиційній моделі на кожен клієнтський комп'ютер необхідно встановити окрему копію програми. Відповідно, кожен програмний продукт займає на комп'ютері певну кількість місця, вимагає персонального адміністрування, оновлення і так далі. Все це займає час і при виникненні несправностей вимагає тривалого часу їх усунення, як показано на рис. 3. 1.



Рис. 3.1. Традиційна модель

Як видно з малюнка, при традиційній моделі розгортання додатків час, необхідний процедуру, зростає пропорційно кількості машин у створенні. Будь-які операції з обслуговування займатимуть величезну кількість часу та сил.

Віртуалізація програм дозволяє централізувати цей процес і значно скоротити час, потрібний на розгортання та обслуговування.

Розгортання програм за допомогою App-V.

На відміну від традиційної моделі розгортання, віртуалізація пропонує зовсім інший підхід. Усі програми, що потрібні користувачам, централізовано встановлюються на сервер додатків один раз. У цьому випадку кафедральний адміністратор заздалегідь готує та встановлює програми на сервер, після чого публікує їх на клієнтські машини. При необхідності в додатку, наприклад, почалася пара з програмування, клієнтські комп'ютери запитують цю програму з сервера, сервер в потоковому режимі передає необхідні для запуску дані і комп'ютер клієнта виконує програму використовуючи свої обчислювальні потужності, рис.3.2.

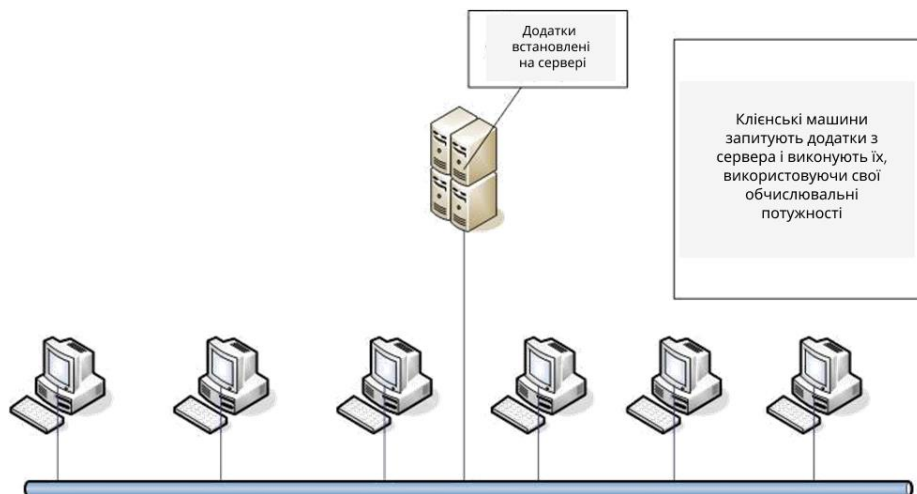


Рис. 3.2. Локальна віртуалізація програм

Оскільки програми виконуються, використовуючи ресурси клієнтських машин, навантаження на сервер знижується. Зважаючи на те, що деякі вищезазначені програми можуть мати значні вимоги до ресурсів, такий підхід дозволяє розвантажити центральний сервер для виконання інших завдань. З урахуванням того, що північ додатків є віртуальним сервером, поряд із серверами баз даних, це значно знижує навантаження з фізичних серверів.

3.2 Робота з App-V

Для роботи з віртуальними програмами використовується спеціальна консоль управління. Вона дозволяє виконувати основні функції для розгортання програм:

- Імпорт програми - процес перетворення програми, щоб воно могло бути доступним для потокової передачі з сервера. Необхідні файли .osd або .sprj. Під час імпорту нової програми створюються автоматично.
- Ручне додавання програми – процес ручного імпорту програм. Необхідно вказати всю необхідну інформацію для імпорту.
- Надання та заборона доступу до програми – обмеження доступу до програми конкретним користувачам або групам, що показано на рис. 3.3.

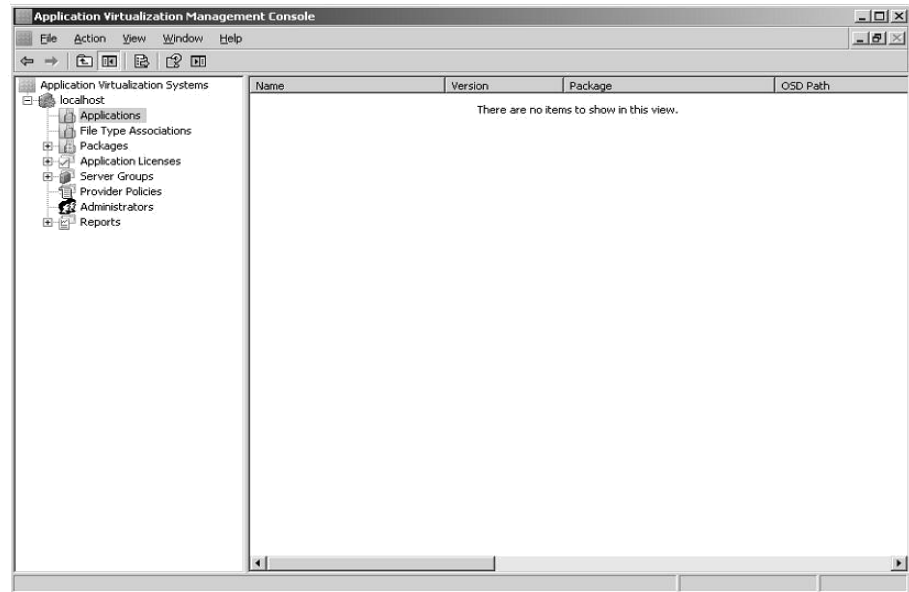


Рис. 3.3. Консоль управління віртуалізацією програм

Для успішного імпорту програми необхідно вказати його .osd або .sprj файл. Використовую .osd файл адміністратор змушений буде додавати кожен пакет окремо, використовую .sprj файл можна встановити весь пакет повністю, як показано на рис. 3.4.



Рис. 3.4. Вибір потрібного файлу

Під час імпорту програми необхідно вказати додаткову інформацію, а також бажано дати опис додатку, як показано на рис. 3.5.

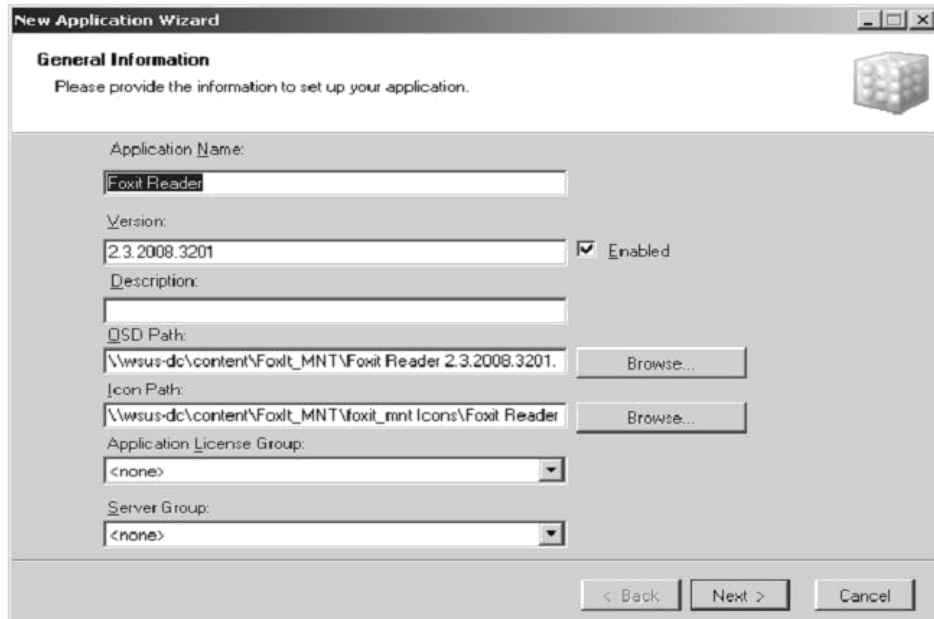


Рис. 3.5. Опис програми та інші параметри

У процесі імпорту адміністратор має можливість вказати розташування ярликів програми та інших файлів на клієнтських машинах, як показано на рис. 3.6.

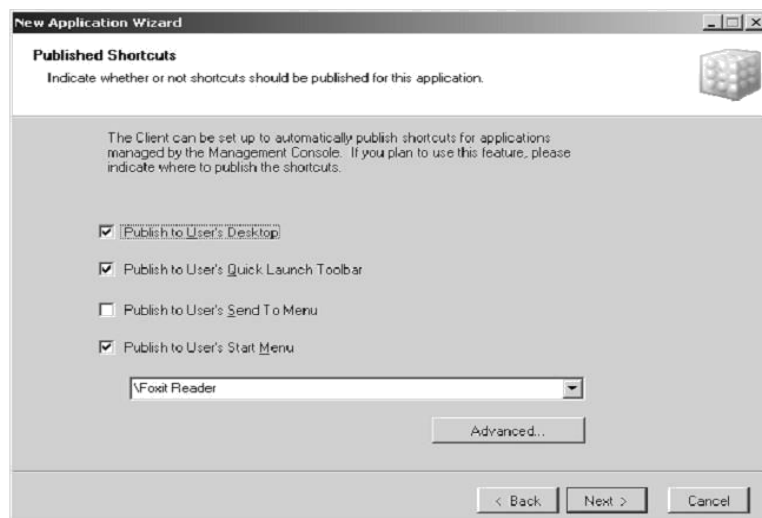


Рис. 3.6. Налаштування програми на клієнтських комп'ютерах

Для усунення конфліктів щодо дозволів файлів настійно рекомендується вказати під час імпорту налаштування асоціації. Це усуне можливі конфлікти у майбутньому та дозволяє підтримувати робоче середовище цілісного на всіх машинах. Подібні заходи значно спрощують адміністрування, роблячи його прозорішим. Майстер із встановлення віртуальної програми дозволяє зробити це відразу під час встановлення. Найкращою практикою вважається зробити це саме на цьому етапі. На рис. 3.7 показано вікно налаштувань асоціацій файлів.

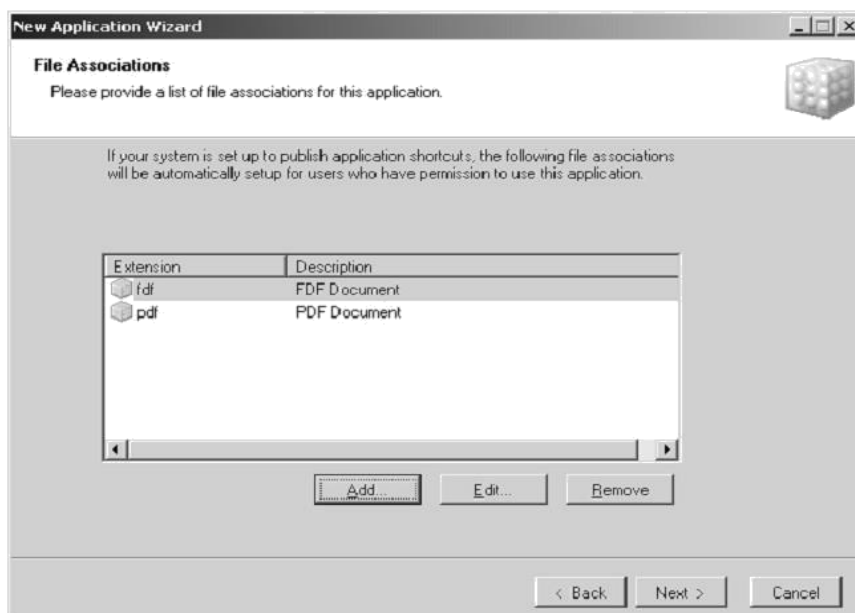


Рис. 3.7. Налаштування асоціацій файлів

Для обмеження доступу до програм використовуються групи та користувачі з установок контролера домену мережі. Інтеграція з Active Directory дозволяє гнучко налаштовувати доступ до програм. Наприклад, можна заборонити доступ студентів молодших курсів до додатків по роботі з базами даних, тоді як офісні програми будуть доступні всім користувачам. Приклад налаштувань показаний рис. 3.8.

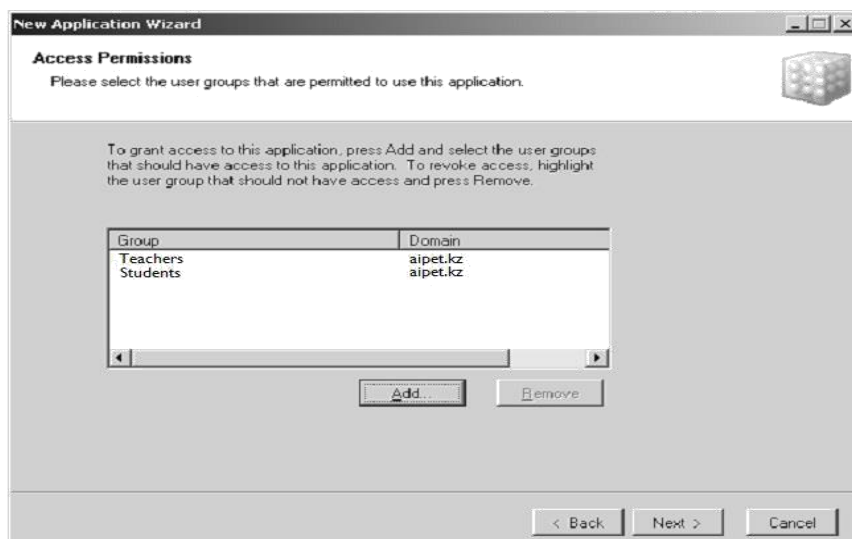


Рис. 3.8. Налаштування доступу до програми

Після надання всіх необхідних відомостей рекомендується знову перевірити всі налаштування. У разі виникнення конфліктів система видасть відповідне попередження, як показано на рис.3.9.

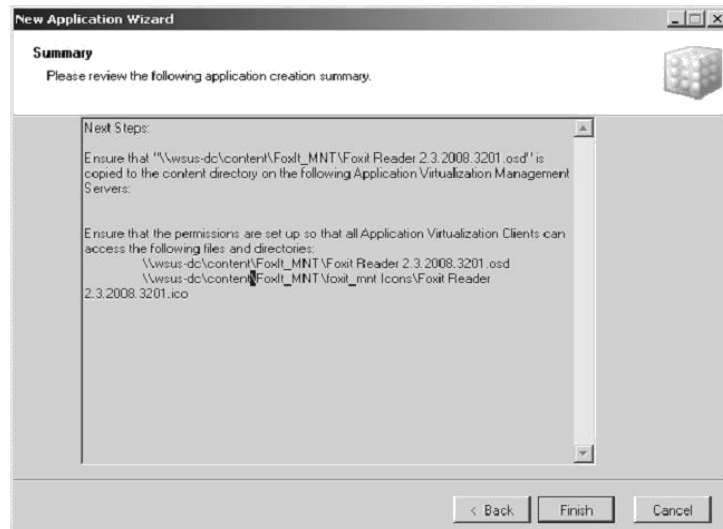


Рис. 3.9. Зведена інформація про програму

Додаток готовий до передачі клієнтам, як видно з рис.3.10.

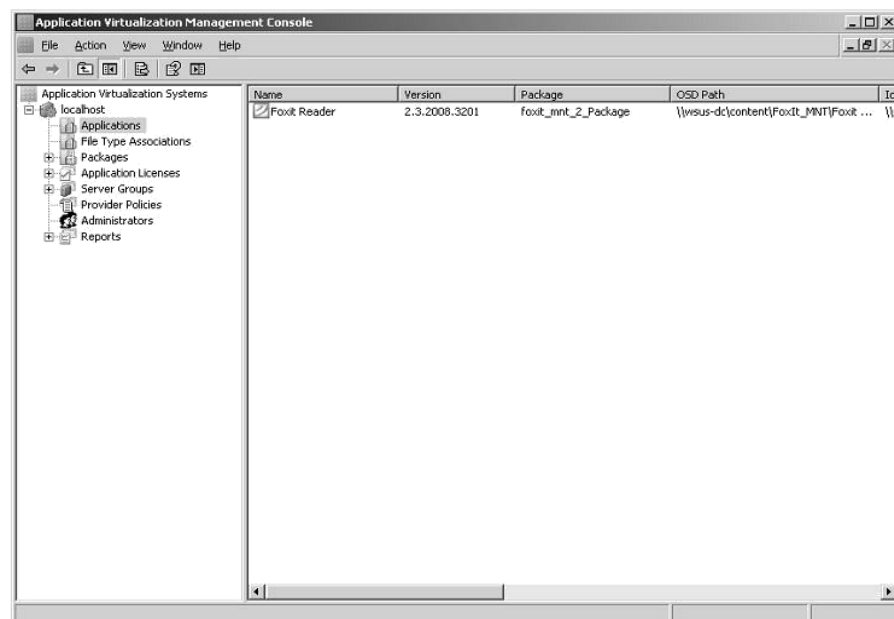


Рис.3.10 - Додаток готовий до передачі клієнтам

Щоб клієнти мали можливість запросити програму з сервера, необхідно встановити клієнтську програму. Вона входить до MDOP (Microsoft Desktop Optimization Pack). Цей пакет розповсюджується безкоштовно за умови, що клієнт має активну корпоративну ліцензію.

Варто зазначити, що в цьому варіанті реалізації для виконання додатків використовуються ресурси локальних комп'ютерів. Це рішення виправдане, якщо сервер не має додаткових обчислювальних потужностей. Сервер лише потоково розсилає програми клієнтам.

Можливий інший спосіб реалізації, при якому навантаження виконання додатків лягає на сам сервер. Даний вид реалізації вимагатиме ще одного сервера і, зрозуміло, значно потужніший сервер додатків.

У випадку кафедри перший варіант більш доцільний, оскільки дозволяє користуватися наявними локальними машинами, в той же час, економлячи на придбанні додаткових обчислювальних потужностей для центральних серверів.

Так як безпека є основною вимогою при роботі з серверами баз даних, а безперервність роботи та мінімізація часу простою є основною вимогою у навчальних закладах необхідно вжити певних заходів щодо забезпечення стійкості до відмови системи. Для вирішення цієї проблеми було вирішено використати кластеризацію.

Кластеризація, по суті, є способом об'єднання кількох окремих машин у єдину, відмовостійку систему. Кожна машина в кластері є вузол, при виході якого з ладу, навантаження і сервіси це вузла беруть на себе інші вузли кластера, забезпечуючи таким чином безперервну роботу системи.

Для створення кластера на основі серверів віртуалізації Hyper-V необхідно:

- Мінімум два сервери із встановленою операційною системою Microsoft Windows Server 2008 R2 Enterprise або Datacenter Edition з встановленою роллю Hyper-V та компонентом Failover Clustering. Слід використовувати однакову версію операційної системи на всіх вузлах - не можна на один вузол ставити Enterprise Edition, а інший Datacenter. Вузли повинні бути однакової архітектури — не можна використовувати як один вузол Itanium сервер, а як інший — x64. Крім того, однаковий спосіб встановлення повинен бути використаний на всіх вузлах - не можна на один вузол ставити Server Core, а на інший Full Installation. Апаратне забезпечення вузлів також має бути якомога ідентичнішим. Усі вузли кластера повинні входити до одного домен системи AD DS.

- Зовнішнє сховище даних, що складається як мінімум із двох логічних юнітів. Сховище повинно включати один логічний юніт, налаштований як диск-свідок. Цей диск містить копію дискаконфігурацією кластера. Крім цього має бути

ще один логічний юніт, який зберігає віртуальні машини та їх віртуальні жорсткі диски.

Мережева інфраструктура, що з'єднає всі компоненти кластера, повинна бути, включаючи зовнішнє сховище даних, може бути реалізована декількома способами. Проте вона повинна бути спроектована таким чином, щоб забезпечити стійкість до відмов, і бажано, надмірність ліній.

Для кафедри пропонується використовувати простий кластер, що складається із двох вузлів. Це забезпечить необхідний рівень стійкості до відмов при мінімально можливих витратах. Показано на рис.3.11.

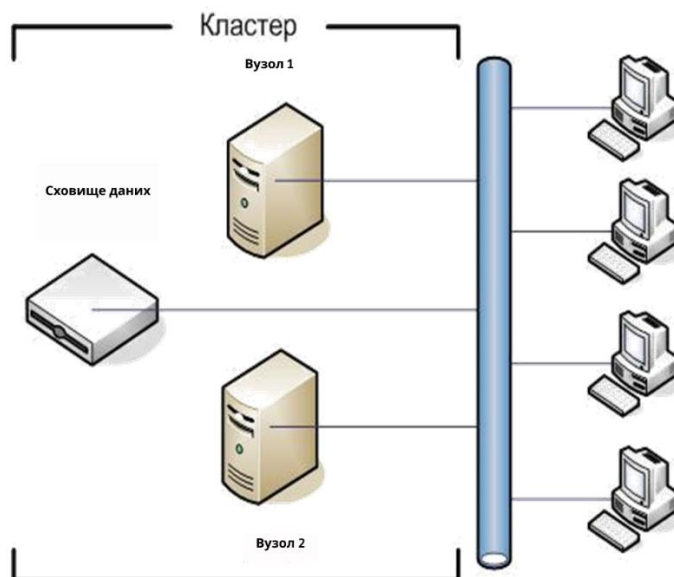


Рис.3.11. Схематичне зображення кластера

Використовуючи кластер можна переносити працюючі віртуальні машини між вузлами не перериваючи роботи користувача. Для цього необхідно налаштувати віртуальну машину із використанням Live Migration. Для зниження часу простою при адмініструванні серверів, кафедральні сервери баз даних рекомендується розташовувати у віртуальних машинах, налаштованих використовувати з Live Migration.

Для цього необхідно:

- Налаштувати кластер з урахуванням вимог, наведених вище.

- Встановити Windows Server 2008 R2 за участю Hyper-V на кожну машину.
- Встановити компонент Failover Clustering на кожну машину та налаштувати сервери як вузли в кластері. Рекомендується перевірити правильність налаштування, використовуючи вбудований майстер Validate A Configuration Wizard, як показано на рис. 3.3.
- Використовуючи контрольну панель, активуйте Cluster Shared Volumes. Це дозволить усім вузлам у кластері використовувати загальне зовнішнє сховище. Зробити це можна лише один раз на кожному кластері.
- Додати сховище зі списку можливих сховищ, що використовують відповідні елементи контрольної панелі.
- Створити віртуальні машини, які мають використовувати функції Live Migration. Для збереження конфігураційних файлів та віртуальних жорстких дисків необхідно вибрати загальне сховище, яке було налаштовано вище. Віртуальна машина має бути створена на вузлі, що має доступ до спільного сховища.
- Необхідно налаштувати віртуальну машину як високо доступну, використовуючи контрольну панель та вкладки Configure A Service Or Application. Це необхідно зробити з усіма віртуальними машинами, які планується використовувати із Live Migration.

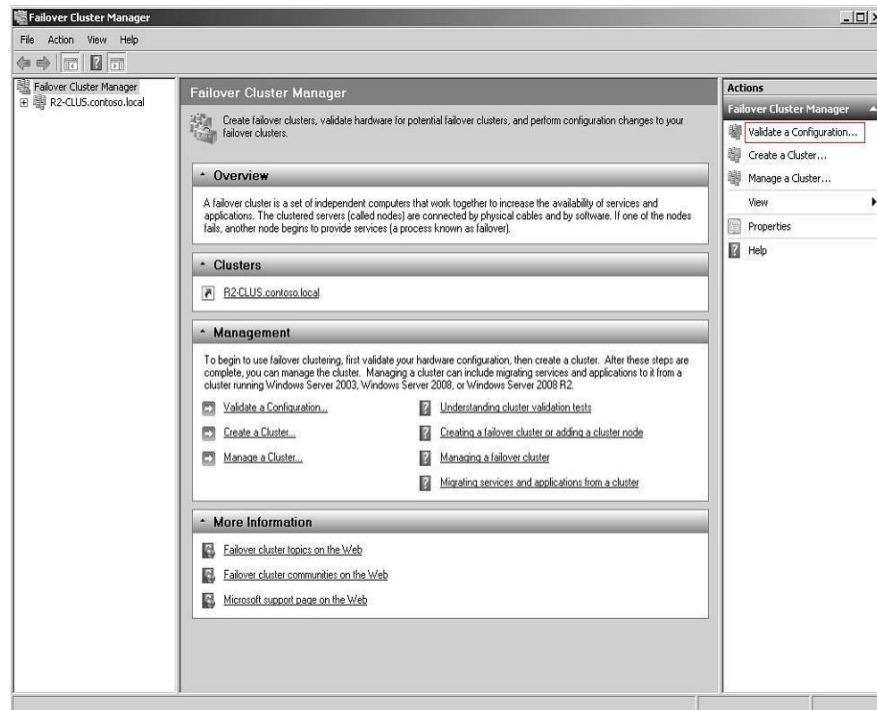


Рис.3.12. Використання майстра Validate A Configuration Wizard

– Необхідно вказати для якої віртуальної машини, яка кластерна мережа повинна використовуватися, як показано на рис.3.12.

На цьому етапі можна завершити налаштування кластера та віртуальних машин, що працюють з функцією Live Migration. У результаті всі віртуальні машини, налаштовані вищеописаним способом, мають підвищену стійкість до відмов і при правильному адмініструванні можуть працювати практично безперервно.

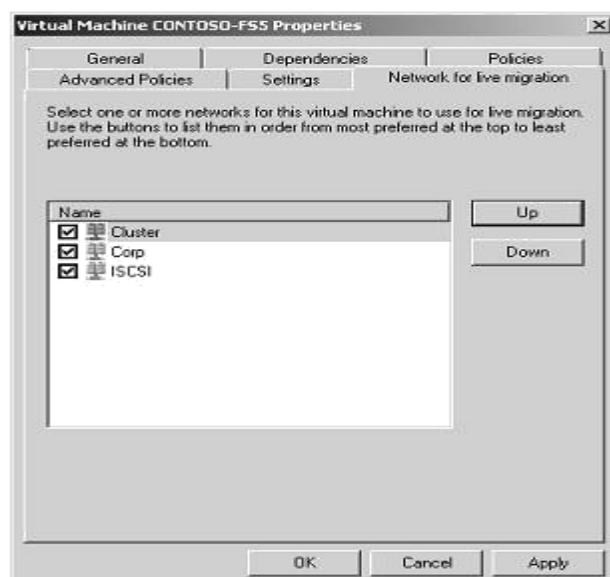


Рис.3.13. Вибір кластерної мережі

Щоб перенести віртуальні машини з одного вузла кластера на інший, не перериваючи роботи, необхідно зробити наступне:

- Відкрити панель керування кластером
- Вибрати потрібну віртуальну машину та виконати Live Migrate Virtual Machine To Another Node. Потім вказати вузол куди необхідно перенести машину, як показано рис.3.14.

- Процес переміщення віртуальної машини буде показаний у центральній частині панелі керування, як показано на рис.3.15.

Час, необхідний для переносу віртуальної машини, залежить від кількості оперативної пам'яті, налаштованої для віртуальної машини, навантаження обох вузлах, так і пропускної спроможності мережного каналу, що з'єднує вузли кластера.

- Після завершення перенесення власником віртуальної машини стає другий вузол, як показано на рис.3.16.

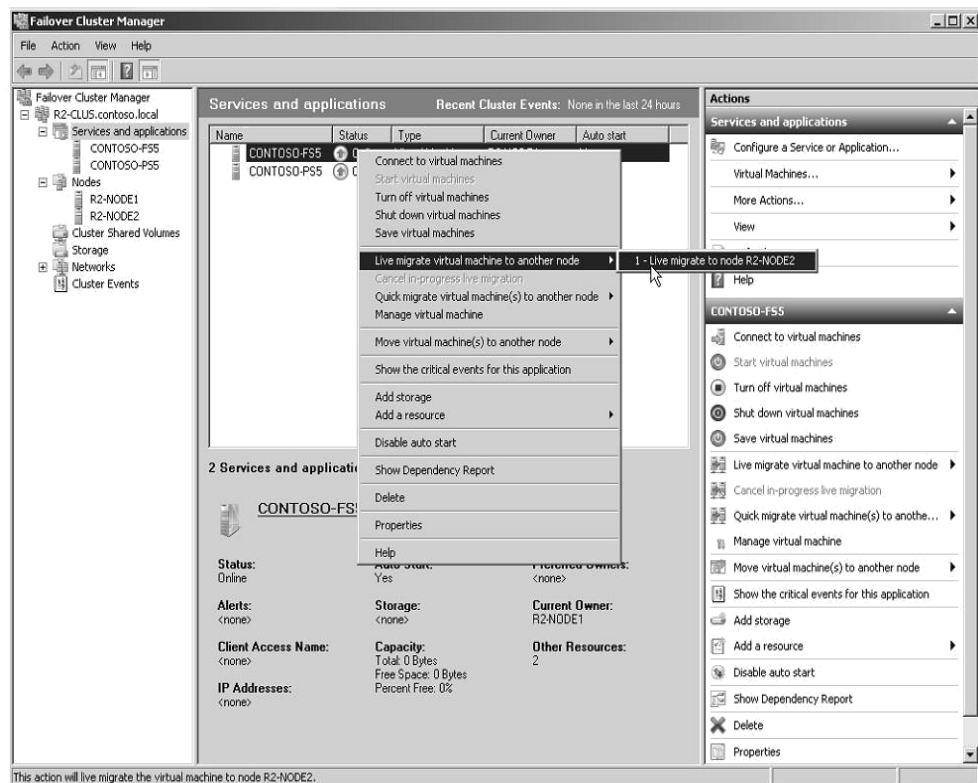


Рис.3.14. Live Migration у дії

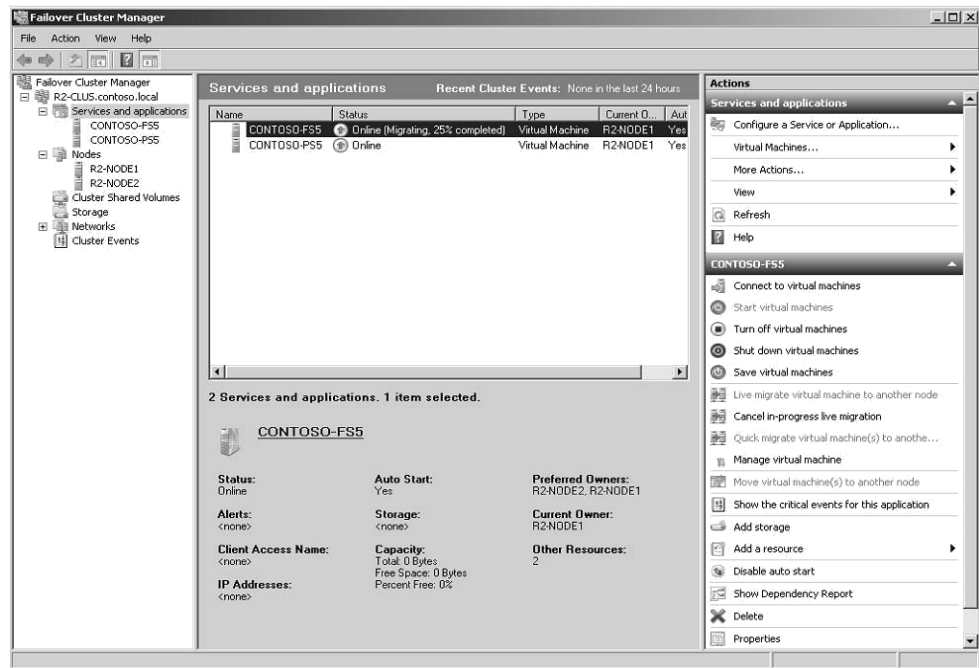


Рис.3.15. Процес перенесення віртуальної машини

В версії R2 з'явилася можливість переносити віртуальні машини з використанням Windows PowerShell. Це можна виконати наступною командою:

```
Get-Cluster "<Cluster Name>" | Move-ClusterVirtualMachineRole -Name  
"<VM group name>" -Node "<Destination node name>"
```

В вищезазначеній команді <Cluster Name> ім'я вузла, на якому знаходиться віртуальна машина. <VM group name> назва групи віртуальної машини та <Destination node name> ім'я вузла в кластері, куди необхідно перемістити віртуальну машину за допомогою Live Migration.

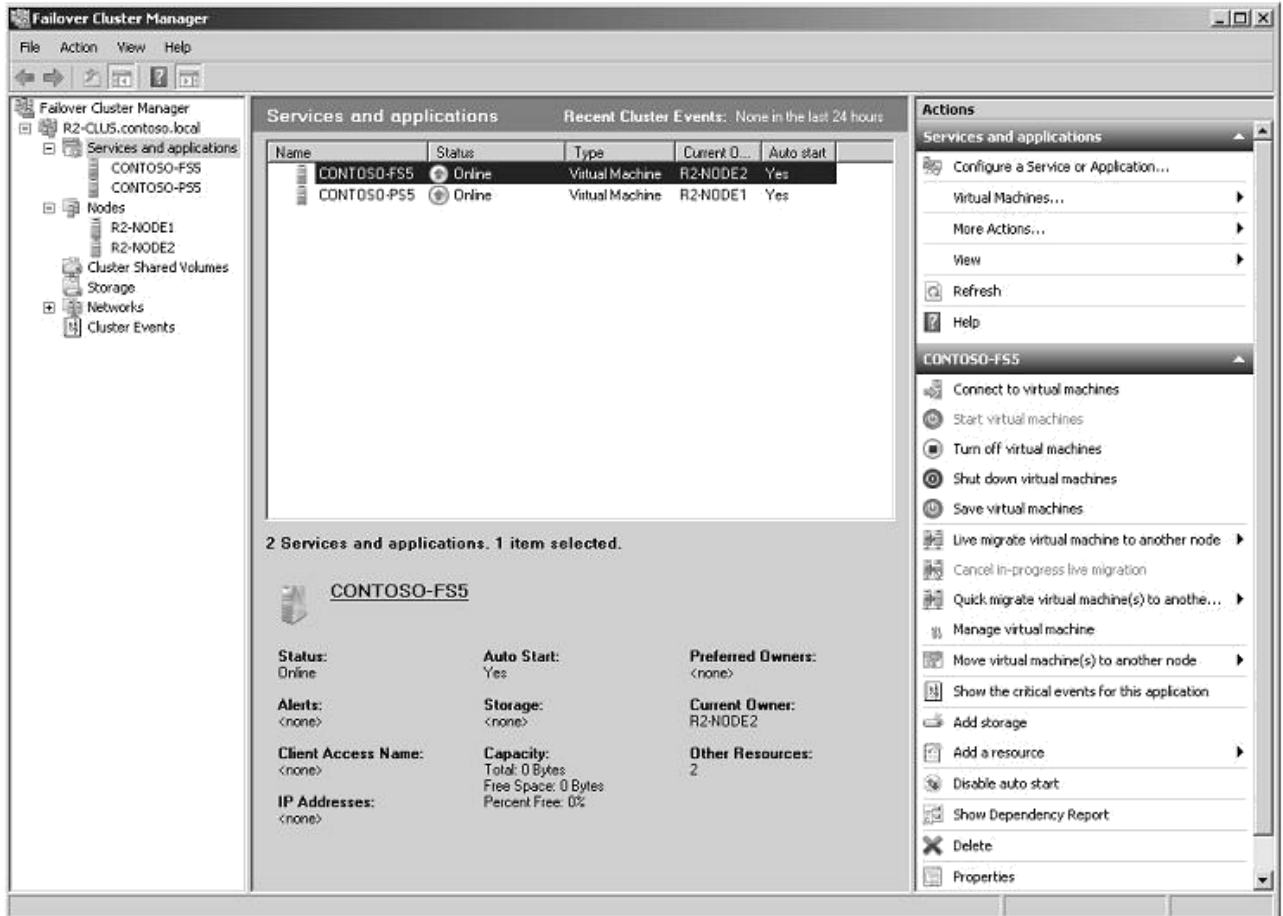


Рис.3.16. Результат перенесення віртуальної машини

3.3 Контроль доступу, розподіл прав під час роботи через vCenter

VCenter пропонує досить гнучку систему роздачі прав. Що вона являє собою, показано на рис.3.17. Тут видно список привілеїв (прав), включених у роль Administrator.

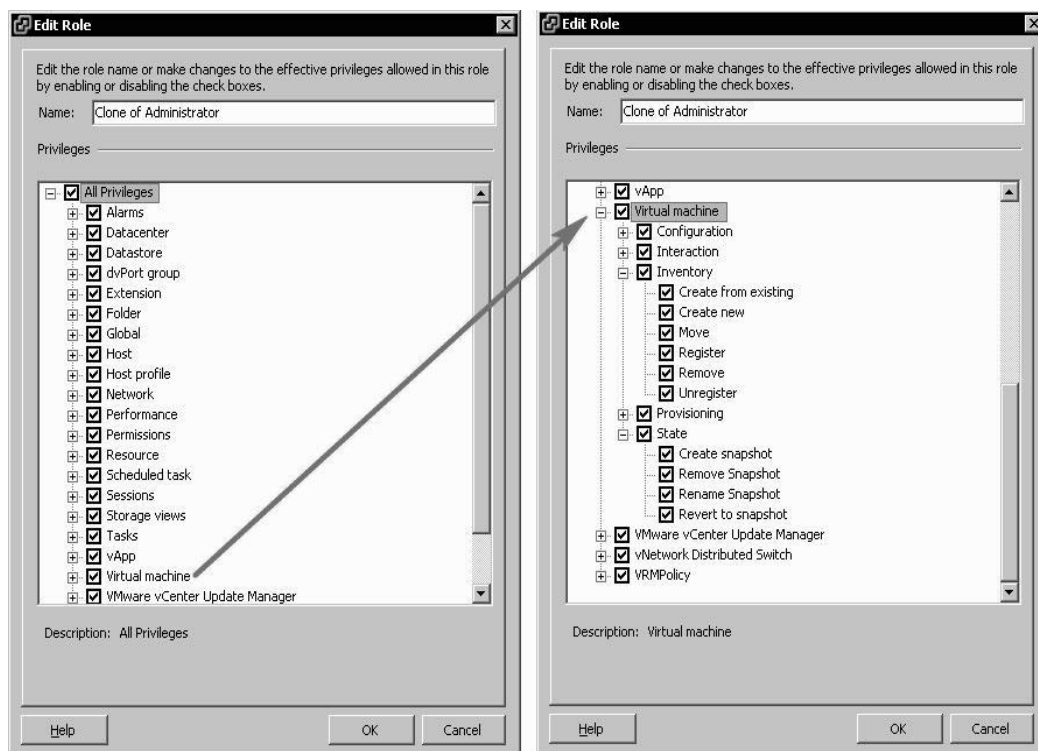


Рис.3.17. Налаштування привілеїв на vCenter

Привілей - це право на атомарну дію. На рисунку справа показані привілеї для віртуальних машин, такі як "Створити", "Видалити", "Створити знімок стану (snapshot)" та ін. Набір якихось привілеїв називається роллю.

Роль – це конкретний набір привілеїв, тобто дозволених дій. Роль можна дати користувачеві або групі на якийсь рівень ієрархії vCenter, як показано на рис.3.18.

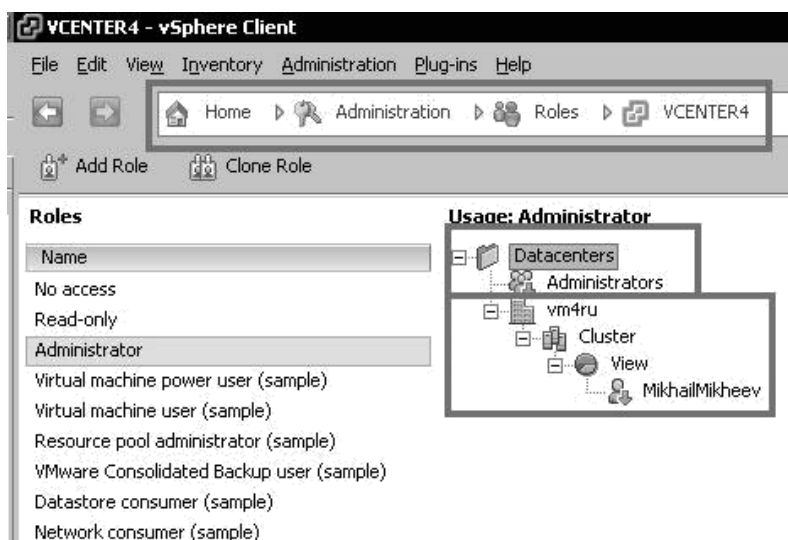


Рис. 3.18. Інформація про те, на який рівень ієрархії і якому користувачеві призначено обрану роль

Тут видно, що роль Administrator (ліворуч) дана групі Administrators на рівні об'єкта Datacenters (найвищому рівні ієрархії vCenter). Це налаштування за замовчуванням – група локальних адміністраторів на сервері vCenter має всі права на всю ієрархію. Крім того, тут цю роль видано користувачеві на пул ресурсів під назвою «View».

vCenter не має власної БД користувачів, він користується:

- локальними користувачами та групами Windows, створеними на сервері, на якому встановлено vCenter;
- доменними користувачами та групами того домену, до якого входить сервер vCenter (якщо він в домен входить).

Таким чином, порядок дій для видачі якихось прав користувачеві чи групі наступний:

1. Створюється користувач/група, якщо вони ще немає. Вони можуть бути локальними у Windows vCenter або доменними, якщо він входить у домен.
2. Створюється роль. Для цього шляхом Home Administration Roles. Потім:
 - у контекстному меню порожнього місця вибирається пункт Add для створення нової ролі з нуля;
 - у контекстному меню існуючої ролі вибирається Clone для створення копії існуючої ролі. Якщо необхідно змінити створену роль, викликається нею контекстне меню і вибирається Edit. Чекбоксом відзначаються всі необхідні привілеї.
3. Потім Home Inventory і вибирається:
 - Hosts and Clusters для роздачі прав на видимі у цій ієрархії об'єкти – кластери, сервери, каталоги із серверами, пули ресурсів та інше;
 - VMs and Templates – на ВМ, шаблони та каталоги з цими об'єктами;
 - Datastore – для роздачі прав на сховища;
 - Networking – для роздачі прав на Комутатори.

Приклад показаний на рис.3.19.

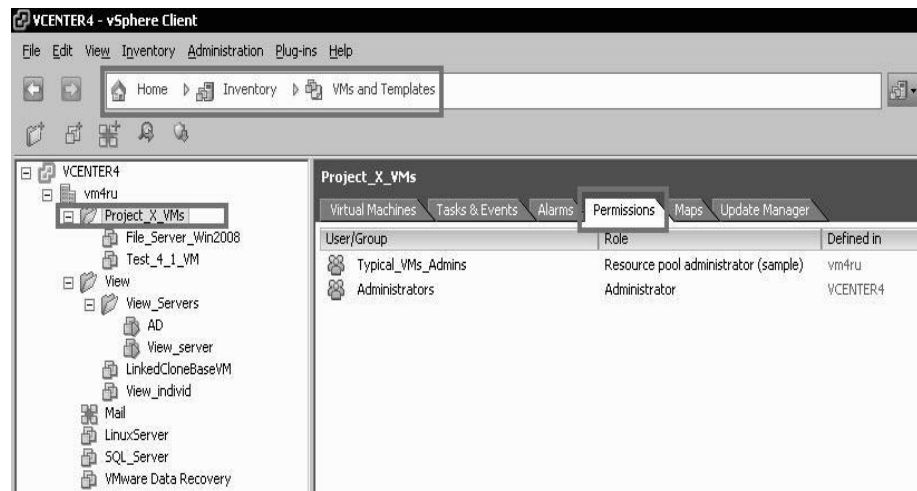


Рис. 3.19. Перегляд дозволів для вибраного об'єкта

Тут видно каталоги для VM (вони блакитного кольору і видно лише в режимі "VMs and Templates"). Якщо перейти на закладку Permissions, буде видно інформацію про те, хто і які права має зараз на обраний об'єкт.

В даному прикладі видно, що група Administrators має права ролі Administrator, до того ж ця роль призначена групі лише на рівні «vcenter4» (тобто в корені ієрархії vCenter, на прикладі vcenter4 – це ім'я машини із встановленим vCenter). Крім того, групі "Typical_VMs_Admins" призначено роль "Resource pool administrator (sample)" на рівні "vm4ru" (у даному прикладі це назва об'єкта Datacenter, що містить всі сервери та VM).

Тепер необхідно дати деякі права групі чи користувачеві на об'єкт ієрархії. Залишаючись на закладці Permissions цього об'єкта, викликається контекстне меню і необхідно вибирати Add Permissions (рис. 3.20).

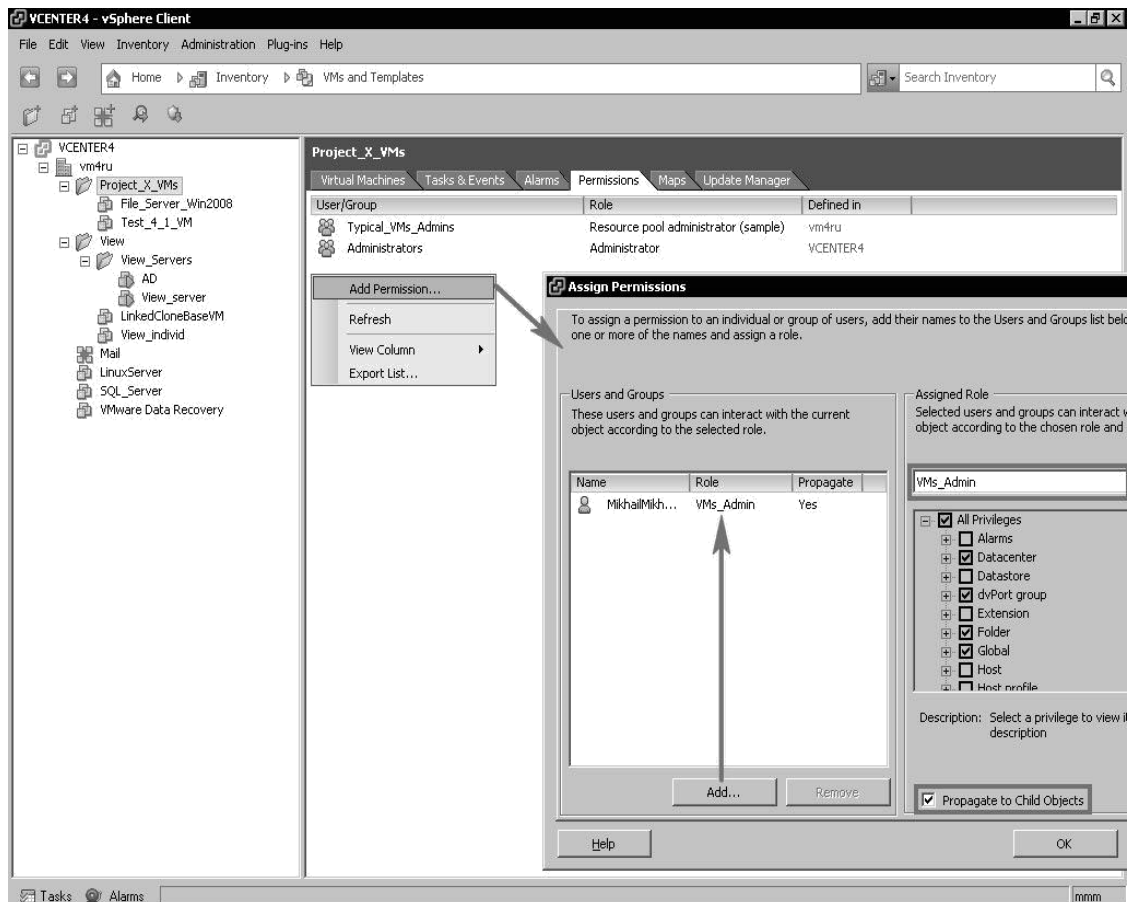


Рис.3.20. Призначення ролі каталог з VM

У вікні натисканням кнопки Add вибираються користувачі та групи, потім у правій частині випадаючого меню вибирається роль, яку необхідно їм задати. Бажана роль до цього моменту має бути створена, робиться це в меню Home Administration Roles.

Слід звернути увагу на прапорець Propagate to Child Objects (застосовувати до дочірніх об'єктів). Якщо він не стоїть, то права видаються лише на об'єкт (каталог Project_X_VMs), але не на галузь його подібних об'єктів.

У цьому прикладі було дано користувачеві (створеному у Windows, на якій встановлено vCenter) роль VMsAdmin (яка була створена в vCenter) на каталог ProjectXVMs. Якщо звернутися клієнтом vSphere від імені цього користувача, то буде видно наступну картину, рис. 3.21.

Користувач не бачить інших об'єктів, окрім тих, на які має права, тобто двох VM. Якщо він переглядає списки подій (Events), йому доступні події лише цих двох

об'єктів. Йому недоступне призначення ролей, недоступне керування ліцензіями і т.п.

Далі декілька правил застосування прав.

Найважливіше: якщо користувачеві видано різні права на різних рівнях ієрархії vCenter, то результуючими для якогось об'єкта є перші, що зустрічаються знизу вгору – рис. 3.21.

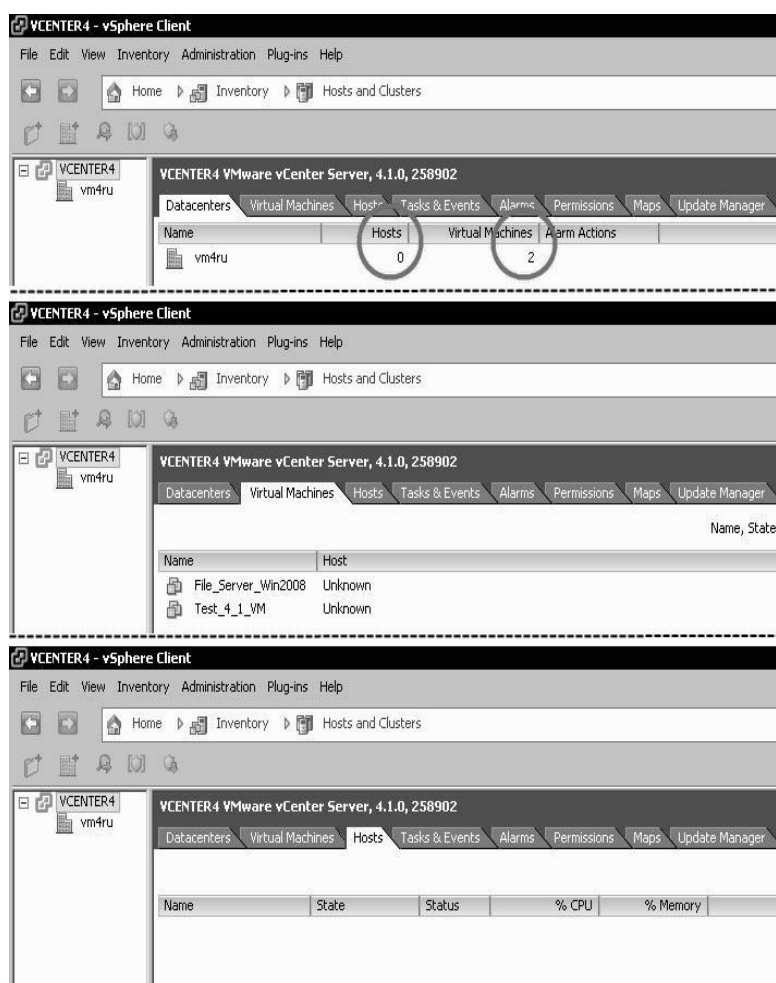


Рис. 3.21. Підключення від імені непривілейованого користувача

Це досить типова ситуація: користувач VasilyPurkin має роль адміністратора (тобто всі права) на всю ієрархію. На пул ресурсів nonCriticalProductionVMs видані обмежені права групі користувачів, до яких входить і VasilyPurkin. За правилами розповсюдження привілеїв vCenter, для цього пулу і для ВМ, що входять до нього, користувач не володіє правами адміністратора, тільки правами на читання (рис. 3.22).

Ситуація типова, тому що не виключено, що адміністратор даватиме якимось групам користувачів обмежені права на групи ВМ (або мереж, або сховищ. Втім, ВМ вірогідніші). І буває, Адміністратор сам входить, або починає входити через якийсь час, в цю саму групу. І внаслідок цього втрачає адміністративні привілеї на гілку ієрархії.

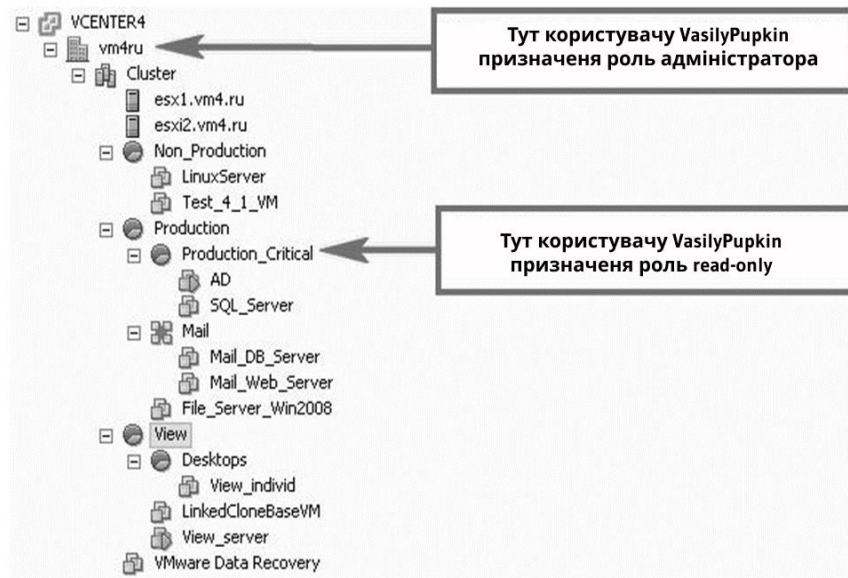


Рис. 3.22. Ілюстрація варіантів призначення різних прав різні рівні ієрархії.

Інший випадок – на рис. 3.23.

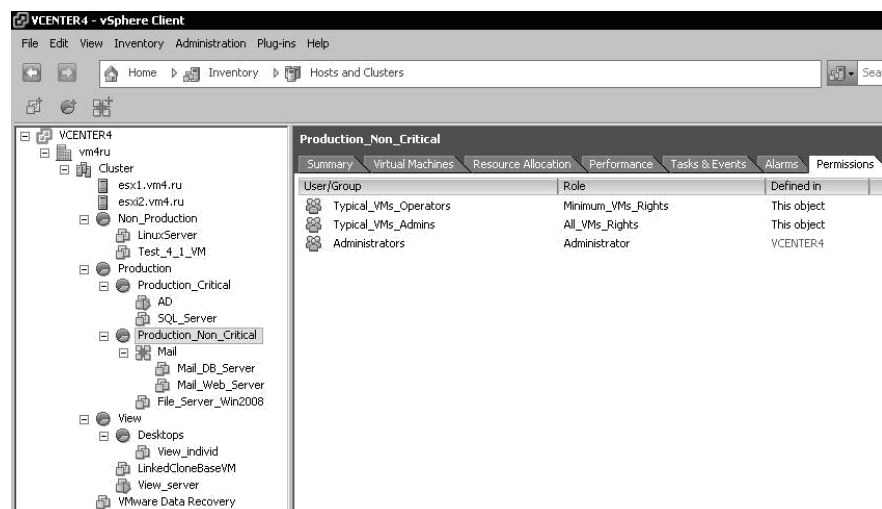


Рис. 3.23. Ілюстрація видачі різних прав двом групам однією об'єкт ієрархії

Тут видно, що на той самий об'єкт в ієрархії видано різні права двом групам. Які права діятимуть у випадку, якщо ми входимо до обох груп? У цьому разі відбувається об'єднання привілеїв:

– Ми матимемо тих, що входять хоча б в одну роль. Останній приклад на рис. 3.24.

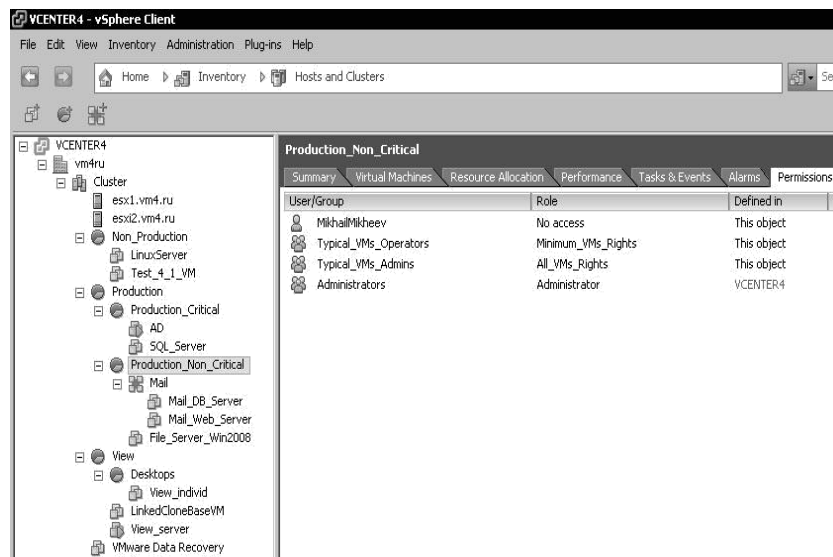


Рис. 3.24.Видача різних прав користувачеві та групі, до якої він входить, на один об'єкт

Тут на один об'єкт в ієрархії видано права і безпосередньо користувачеві, і групам, до яких він входить. У разі результуючими є ті права, видані безпосередньо користувачеві.

В даному прикладі це роль "No access". Ця існуюча по замовчуванню роль необхідна для явного позбавлення доступу. Загальні міркування щодо розмежування прав доступу.

Якщо в організації один адміністратор, то, швидше за все, система роздачі прав не стане в нагоді або знадобиться дуже обмежено – на рівні надання прав на деякі ВМ деяким групам користувачів.

А от якщо з різними областями віртуальної інфраструктури мають працювати різні групи адміністраторів, операторів та користувачів, то має сенс зробити приблизно так:

1. Складіть перелік повсякденних завдань, які доведеться вирішувати. Якщо щось забудете - нічого страшного, виконайте кілька ітерацій.

Безпека. Розширені налаштування, безпека, профілі налаштувань

2. Перерахуйте, які об'єкти ієрархії та елементи інтерфейсу використовуються для виконання кожного завдання зі списку, складеного вище. Про кожен і докладно.

3. Розпишіть, хто і де це виконуватиме.

Отриманий у результаті документ називається "матрицею доступу до інформації". Хто, куди, навіщо? Фактично це – основа внутрішньої документації з безпеки віртуальної інфраструктури, на її основі створюватимуться ролі та видаватимуться на ті чи інші рівні ієрархії, за її допомогою фіксуватимуться зміни. Наявність документації, куди вносяться зміни до конфігурації, є обов'язковою – інакше ви ризикуєте, що в якийсь момент заплутатися аж до втрати доступу до інфраструктури.

Не використовуємо стандартні ролі vCenter. За винятком ролі Administrator (тобто всі права), Read-only (перегляд інформації про об'єкт) та No Access (явна відсутність доступу). Інші існуючі ролі не рекомендується використовувати (за винятком ролі VMware Consolidated Backup user (sample)).

Зрозуміло, правильним буде створення ролей під конкретні потреби, а не використання однієї ролі, яка може все. Створюємо ролі під конкретні завдання із мінімально необхідним набором прав. Існуючі за умовчанням ролі не відповідають цій умові.

Однозначно ролі повинні призначатися персоніфіковано, тобто не повинно бути облікового запису, з-під якого можуть автентифікуватися декілька осіб. Це надзвичайно допомагає, зокрема, якщо необхідно відновити послідовність подій та винну особу.

Не використовуються локальні облікові записи, за особливих випадків. Лише доменні. Тим більше це зручніше – для аутентифікації у vSphere можна використовувати той обліковий запис, від імені якого було виконано вхід у Windows, і не набирати пароль заново.

Налаштування за замовчуванням: локальна група адміністраторів має всі права на корінь ієрархії vCenter. Звичайно ж, правильно буде:

1. Створити персоніфікований обліковий запис (навіть два).
2. Наділити їх правами адміністратора на все у vCenter.
3. Прибрати їх дані в сейф, користуватися ними лише у виняткових випадках.
4. Позбавити групу локальних адміністраторів прав у vCenter.

3.4 Налаштування сертифікатів SSL

VMware vSphere, зокрема продукти ESX(i) 4, vCenter 4, VMware Converter Enterprise і VMware Update Manager 4, підтримують SSL v3 і TLS v1 (зазвичай використовується просто «SSL»). Якщо SSL увімкнено, трафік між вузлами віртуальної інфраструктури зашифрований, підписаний і не може бути непомітно змінений. ESX(i), як і інші продукти VMware, використовує сертифікати X.509 для шифрування трафіку, що передається по SSL.

В vSphere 4 перевірка сертифікатів увімкнена за замовчуванням, і вони використовуються для шифрування трафіку. Однак ці сертифікати за промовчаням генеруються автоматично під час інсталяції ESX(i). Ця процедура не вимагає від адміністратора якихось дій. Але вони не видані центром сертифікації (certificate authority, CA. Також іноді згадується в російськомовній документації як «Центр, що засвідчує», УЦ). Такі самопідписані сертифікати потенційно вразливі для атак «людина у середині». Тому що для них, перш ніж починається шифрування трафіку, не проводиться перевірка справжності самих сертифікатів.

При спробі підключення до ESX(i) або vCenter (за допомогою клієнта vSphere або браузера) користувачеві видається відповідне попередження (рис. 3.4б), повідомляє йому про те, що віддалена система може не бути довіреною і встановити її справжність неможливо. Звичайно, це попередження можна відхилити, можна занести сертифікати всіх керованих систем до списку довірених, але це може послабити безпеку інфраструктури. До того ж, можливо, в вашій організації заборонено використання систем із недовіреними сертифікатами (адміністративно чи технічно).



Рис. 3.25. Попередження про недовірений сертифікат

Для вирішення цих проблем вам потрібно буде запитати довіреного центру сертифікації відповідний сертифікат і замінити ним згенеровані автоматично. Довірений центр сертифікації може бути комерційним (наприклад, VeriSign, Thawte або GeoTrust) або встановленим у мережі (наприклад, Microsoft Windows Server Active Directory Certificate Services, AD CS або OpenSSL).

Приблизний план цієї дії має такий вигляд.

1. Отримання сертифіката для ESX(i), заміна ними згенерованих за замовчуванням сертифікатів.
2. Отримання сертифікатів для vCenter 4 та Update Manager
3. Заміна сертифікатів, що згенеровані за промовчанням. Зверніть увагу на те, що заміна сертифіката для вже встановленого Update Manager можлива лише Налаштування сертифікатів SSL

Розширені налаштування, безпека, профілі налаштувань із його перевстановленням. Це пов'язано з тим, що він зберігає свої сертифікати у своєму власному форматі, конвертація в який відбувається при встановленні продукту.

Тут не наводяться конкретні інструкції, оскільки вони сильно залежать від вашої інфраструктури, та й далеко не всім адміністраторам vSphere доведеться займатися цим питанням.

3.5 Висновки

Впровадження віртуалізації дозволило практично переконатися у всіх перевагах, запропонованих даної технологією. Консолідація серверів значно знизила загальну вартість обладнання, витрати на електроенергію та обслуговування.

Віртуалізація програм дозволила прискорити процес розгортання клієнтських програм на робочі станції, спростити їх обслуговування, зробити процес більш гладким та швидким.

Підвищилася стійкість до відмови серверів, час простою при збоях скоротився до мінімуму. Завдяки можливості робити знімки, відновлення практично будь-якого сервера та віртуальної машини є справою кількох хвилин.

Крім того, отриманий досвід та вміння в розготанні технології, налаштуванні сервера, клієнтських комп'ютерів та їх обслуговуванні, можна застосувати під час проведення занять по спецпредметам та створити на цій базі практикум для підготовки фахівців у галузі розробки та створення бази даних у SQL, адмініструванні серверів та ОС.

РОЗДІЛ 4

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

При дослідженні переваг технології віртуалізації у процесі навчання студентів важливим є дотримання вимог охорони праці, техніки безпеки та протипожежної безпеки при роботі з комп'ютерною технікою. Основними регламентуючими нормативними документами охорони праці користувачів ПК є НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями», а також Примірні інструкція з охорони праці під час експлуатації електронно-обчислювальних машин, затверджена наказом Міністерства доходів і зборів України від 5 вересня 2013 р. № 443, ДБН В.2.5-56:2014 «Системи протипожежного захисту».

Організація робочого місця користувача відеотерміналу та ЕОМ повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги»

Заходи з охорони праці користувачів персонального комп'ютера розглядаються в трьох основних аспектах: соціальному, психологічному та медичному.

У соціальному плані розв'язання цих проблем пов'язане з оптимізацією умов життя, праці, відпочинку, харчування, побуту, розвитком культури, транспорту.

Значне місце у профілактиці розладів здоров'я належить психології праці. Тому заходи, пов'язані з формуванням раціональних виробничих колективів, у яких відсутня психологічна несумісність, сприяють зменшенню нервово-психічного перенапруження, підвищенню працездатності та ефективності праці.

Оскільки відразу цю проблему усунути неможливо на рівні підприємств, установ та організацій послідовно усували такі виробничі умови, які є сприятливими для розвитку стресу.

Важливу роль у профілактиці захворювань відводиться медицині. Комплекс даних заходів спрямований на відновлення функціонального стану зорового та опорно-рухового апарату, також направлений на зниження ймовірності розвитку перевтоми та перенапруження.

Для забезпечення безпеки на робочому місці проводиться розробка національних нормативних документів, спрямованих на охорону праці користувачів ПК. Найбільш повним нормативним документом щодо забезпечення охорони праці користувачів ПК є «Державні санітарні правила й норми роботи з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин» ДСанПіН 3.3.2.007–98.

До організації робочого місця користувача ПК висуваються ряд вимог серед яких: вимоги до виробничих приміщень, гігієнічні вимоги до організації та обладнання робочих місць, вимоги до режимів праці та відпочинку та вимоги до профілактичних медичних оглядів.

Вимоги до виробничих приміщень полягають у наступному:

- площа на одне робоче місце становить не менше 6 м^2 , а об'єм не менше ніж 20 м^3 ;
- приміщення для роботи повинно мати штучне та природне освітлення;
- необхідно щоденно робити вологе прибирання.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід, і забезпечувати коефіцієнт природної освітленості (КПО) не нижче, ніж 1,5%.

Гігієнічні вимоги до параметрів виробничого середовища включають вимоги до параметрів мікроклімату, освітлення, шуму й вібрації, рівнів електромагнітного та іонізуючого випромінювання. У виробничих приміщеннях на робочих місця із ПК мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря.

Норми мікроклімату для приміщень з ПК:

- у холодну пору року температура повітря при категорії робіт легка-1а має бути $22\text{-}24 \text{ }^\circ\text{C}$, вологість 40-60%;

- у холодну пору року температура повітря при категорії робіт легка-1б температура має бути 21-23 °С, вологість також 40-60 %;
- у теплу пору року при категорії робіт легка-1а температура в приміщеннях має бути 23-25 °С з вологістю 40-60%;
- у теплу пору року при категорії робіт легка-1б температура має бути 22-24 °С з вологістю 40-60%.

Штучне освітлення в приміщеннях із робочими місцями, обладнаними ПК має здійснюватись системою загального рівномірного освітлення.

Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300–500 лк, згідно з ДБН В.2.5–28 – 2006 «Природне та штучне освітлення». Якщо це неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення.

Конструкція робочого місця користувача ПК має забезпечити підтримання оптимальної робочої пози.

Робочі місця із ПК розташовуються відносно світлових прорізів, щоб природне світло падало збоку, переважно зліва.

При розміщенні робочих столів із персональним комп'ютером дотримуються таких відстаней: між бічними поверхнями БДТ – 1,2 м; від тильної поверхні одного ПК до екрана іншого – 2,5 м.

Екран ПК розташовують на оптимальній відстані від очей користувача, що становить від 60 до 70 см, але не ближче, ніж за 60 см з урахуванням розміру літерно-цифрових знаків і символів.

Клавіатуру розташовують на поверхні столу на відстані від 10 до 30 см від краю, звернутого до працівника.

Для забезпечення захисту і досягнення нормованих рівнів комп'ютерних випромінювань застосовують екранні фільтри, локальні світлофільтри (засоби індивідуального захисту очей) та інші засоби захисту, що пройшли випробування в акредитованих лабораторіях і мають щорічний гігієнічний сертифікат.

При організації праці, пов'язаної з використанням ПК, для збереження здоров'я працівників, запобігання професійним захворюванням і підтримки

працездатності передбачаються внутрішньо змінні регламентовані перерви для відпочинку.

Працівники з ПК підлягають обов'язковим медичним оглядам: попереднім – при влаштуванні на роботу і періодичним – протягом трудової діяльності, відповідно до наказу МОЗ України N45 від 31.03.94 р.

Періодичні методичні огляди мають проводитися раз на два роки комісією в складі терапевта, невропатолога та офтальмолога.

Охорона праці робочого місця користувача персонального комп'ютера є дуже важливою, оскільки не дотримання вимог може призвести до професійних хвороб.

4.2 Застосування віртуалізації у навчанні з безпеки в надзвичайних ситуаціях

Моніторинг небезпек, що можуть причинити надзвичайну ситуацію, проводиться на основі Наказу Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи «Про затвердження Положення про моніторинг потенційно небезпечних об'єктів» від 06.11.2003 р. № 425.

Щорічно в нашій країні виникають надзвичайні ситуації природного та техногенного характеру, що призводить до загибелі багатьох людей і значних матеріальних збитків.

Метою класифікації НС є створення ефективного механізму оцінювання події, що відбулася або може відбутися у прогнозований термін, та визначення ступеня реагування на відповідному рівні управління. Надзвичайні ситуації можна класифікувати за наступними ознаками.

Класифікація надзвичайних ситуацій [5]:

- За сутністю та причинами виникнення: природні, соціальні, техногенні.
- За масштабом та глибиною: локальні, об'єктові, місцеві, регіональні, національні, глобальні

– За характером походження: соціально-політичного характеру, воєнного характеру.

Види надзвичайних ситуацій

Природного характеру: метеорологічні (засуха, значне підвищення чи зниження температури, буря, ураган, смерч), тектонічні (землетрус, цунамі, виверження вулкану, зсув), селевий (потік, повінь, лавина, камнепад, снігові замети, пожежа); космічні (підвищене радіоактивне випромінювання, падіння великого космічного тіла); біологічні (аномальне підвищення кількості макробіологічних об'єктів, епідемія);

Антропогенного характеру: аварії та катастрофи (транспортні, пожежі, вибухи, руйнування споруд, руйнування обладнання, руйнування з порушенням енерго-, водо-, тепло- та інших систем життєзабезпечення населення та виробництва, руйнування з викидом радіоактивних речовин, руйнування з викидом отруйних речовин, руйнування з викидом небезпечних мікроорганізмів).

Що стосується причин виникнення надзвичайних ситуацій в Україні, то можна виділити такі основні:

- військовий стан;
- надзвичайне техногенне навантаження території;
- значний моральний та фізичний знос основних виробничих фондів більшості підприємств України;
- погіршення матеріально-технічного забезпечення, зниження виробничої і технологічної дисципліни;
- незадовільний стан збереження, утилізації та захоронення високотоксичних, радіоактивних та побутових відходів;
- ігнорування економічних факторів, вимог, стандартів;
- недостатня увага керівників відповідних органів державного управління до проведення комплексу заходів, спрямованих на запобігання надзвичайним ситуаціям природного і техногенного характеру та зниження їх наслідків;
- відсутність сучасних систем управління небезпечними процесами;

- низька професійна підготовка персоналу та населення до дій в екстремальних умовах;
- дефіцит кваліфікованих кадрів;
- низький рівень застосування прогресивних ресурсозберігаючих і екологобезпечних технологій [5].

Захист населення і територій від надзвичайних ситуацій техногенного та природного характеру здійснюється на принципах:

- пріоритетності завдань, спрямованих на рятування життя та збереження здоров'я людей і довкілля;
- безумовного надання переваги раціональній та превентивній безпеці;
- вільного доступу населення до інформації щодо захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру;
- особистої відповідальності і піклування громадян про власну безпеку, неухильного дотримання ними правил поведінки та дій у надзвичайних ситуаціях техногенного та природного характеру;
- відповідальності у межах своїх повноважень посадових осіб за дотримання вимог цього Закону;
- обов'язковості завчасної реалізації заходів, спрямованих на запобігання виникненню надзвичайних ситуацій техногенного та природного характеру та мінімізацію їх негативних психосоціальних наслідків;
- урахування економічних, природних та інших особливостей територій і ступеня реальної небезпеки виникнення надзвичайних ситуацій техногенного та природного характеру;
- максимально можливого, ефективного і комплексного використання наявних сил і засобів, які призначені для запобігання надзвичайним ситуаціям техногенного та природного характеру і реагування на них.

Щодо основних заходів у сфері захисту населення і території від надзвичайних ситуацій, то до них відносяться: інформування та оповіщення; спостереження; укриття в захисних спорудах; евакуаційні заходи; інженерний захист; медичний захист; біологічний захист; радіаційний та хімічний захист.

Навчальному закладу можуть загрозувати наступні надзвичайні ситуації:

- пожежа (старе приміщення зстарюю проводкою);
- руйнування споруд;
- руйнування з порушенням енерго-, водо-, тепло- та інших систем життєзабезпечення населення та виробництва тощо.
- небезпека, пов'язана з військовим станом в Україні;

В навчальному закладі здійснюються заходи щодо створення безпечних умов для студентів при виникненні надзвичайних ситуацій та заходи щодо ліквідації можливих аварій. Є достатнє число евакуаційних виходів, шляхи евакуації. На основі проведеного аналізу можемо прийти до висновку, що в навчальному закладі створені безпечні умови для студентів при виникненні надзвичайних ситуацій. Проте є певні недоліки, на які потрібно звернути увагу. Так, наприклад, не завершено облаштування бомбосховища (зараз використовується тимчасове).

ВИСНОВОК

Впровадження віртуалізації дозволило практично переконатися у всіх перевагах, запропонованих даної технологією.

В результаті досліджень та експериментів було проведено вивчення самої технології віртуалізації, проведено впровадження її в навчальний процес, на основі створеного алгоритму роботи на базі віртуальних серверів реалізовано локальну віртуалізацію настільних систем в навчальному закладі, зроблено відповідні висновки. А саме:

1. Консолідація серверів значно знизила загальну вартість обладнання, витрати на електроенергію та обслуговування.

2. Віртуалізація програм дозволила прискорити процес розгортання клієнтських програм на робочі станції, спростити їх обслуговування, зробити процес більш гладким та швидким.

3. Підвищилася стійкість до відмови серверів, час простою при збоях скоротився до мінімуму. Завдяки можливості робити копії, відновлення практично будь-якого сервера та віртуальної машини є справою кількох хвилин.

4. В ході кваліфікаційної роботи вдалося наочно з'ясувати всі переваги технології віртуалізації та її зручність, та необхідність у процесі навчання ІТ фахівців, системних адміністраторів та фахівців у галузі баз даних.

Завдяки успішно проведеному експерименту в навчальному закладі “Нововолинський електромаханічний коледж” вдалося побачити переваги застосування даної технології.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Tulloch M. Understanding Microsoft Virtualization Solutions, 3 Desktop to the Datacenter, 2nd Edition - Redmond: Microsoft Press, 2010. - 464 с.
2. Kelbley J., Sterling M. Windows Server 2008 R2 Hyper-V: Insiders Guide до Microsoft's Hypervisor. - Indianapolis: Wiley Publishing, Inc., 2010. - 385 с.
3. Minasi M., Gibson D., Finn A., Henry W., Hynes B. - Mastering Windows Server 2008 R2. - Indianapolis: Wiley Publishing, Inc., 2010. - 1454 с.
4. Міхєєв М. - Адміністрування VMware vSphere 4.1 (Адміністрування та захист) 2012, - 236 с.
5. Стаття Гіпервізор Інтернет енциклопедія URL: <http://wikipedia.org/wiki/> (дата звернення: 15.12.2022).
8. Система віртуальних машин URL: <http://wikipedia.org/wiki/> (дата звернення: 10.12.2022)
6. Історія та особливості розвитку бездротового доступу URL: <http://bestreferat.com/referat-105014.html> (дата звернення: 4.12.2022).
7. Особливості технології віртуалізації URL:<http://osp.com/text/print/302/184272.html> (дата звернення: 14.12.2022).
8. Застосування технології віртуалізації URL:<http://window.edu.ua/resource/848/62848/files/tm2008.html> (дата звернення: 11.12.2022).
9. Технології віртуалізації URL:http://library.by/portalus/modules/computers/print.php?archive=&id=1237562305&start_from=&subaction=showfull&ucat (дата звернення: 4.12.2022).
10. Станек. Microsoft SQL Server 2005 Довідник адміністратора. URL:<http://www.e-reading.org.ua/download.php?book=135150> (дата звернення: 15.12.2022).
11. Максим Л. Технологія віртуалізації. 2013 - 403 с.
12. Insider's guide to microsoft hypervisor (sybex 2009) URL:<https://doc.lagout.org> (дата звернення: 15.12.2022).

13. Harley Stagner Pro Hyper-V. (Apress 2009), 2009, - 401 с.

14. Детально про віртуалізацію: типи, переваги та рішення.

URL:<https://onbiz.biz/about-virtualization/> (дата звернення: 13.12.2022).

15. Типи віртуалізації URL:<https://hvf.com.ua/typy-virtualizatsii/> (дата звернення: 11.12.2022).

Додаток А.
Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

МАТЕРІАЛИ

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

**«ІНФОРМАЦІЙНІ МОДЕЛІ,
СИСТЕМИ ТА ТЕХНОЛОГІЇ»**



7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

Г. Осухівська, А. Волощук ТЕХНОЛОГІЇ ПЕРЕДАВАННЯ ТА ОПРАЦЮВАННЯ ДАНИХ В КОМП'ЮТЕРИЗОВАНИХ СИСТЕМАХ ОБЛІКУ ЕЛЕКТРОЕНЕРГІЇ H. Osukhivska, A. Voloshchuk DATA TRANSMISSION AND PROCESSING TECHNOLOGIES IN COMPUTERIZED ELECTRICITY ACCOUNTING SYSTEMS	136
Ю. Дзюбак, Я. Коненко, Н. Луцк АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ХОСТИНГУ РЕСУРСІВ З ВИКОРИСТАННЯМ ВІРТУАЛІЗАЦІЇ Yu. Dziubak, Ya. Konenko, N. Lutsyk ANALYSIS OF METHODS AND MEANS RESOURCE HOSTING USING VIRTUALIZATION	137
Ю. Дзюбак, Я. Коненко, Я. Войтович ТЕСТУВАННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЛАТФОРМ ВІРТУАЛІЗАЦІЇ Yu. Dziubak, Ya. Konenko, Ya. Voytovych TESTING AND COMPARATIVE ANALYSIS OF VIRTUALIZATION PLATFORM	138
А. Курко, М. Хом'як, К. Урста, А. Шелельо ОПТИМІЗАЦІЯ РОБОТИ ВИПАРНОЇ СТАНЦІЇ ПРИ ВИГОТОВЛЕННІ СОКУ A. Kurko, M. Khomiak, K. Ursta, A. Shelelo OPTIMIZATION OF EVAPORATION STATION DURING JUICE PRODUCTION	139
Х. Ольховецька, Г. Осухівська МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ СИСТЕМИ КОНТРОЛЮ ПРОЦЕСУ ФЕРМЕНТАЦІЇ K. Olkhovetska, H. Osukhivska MATHEMATICAL SUPPORT OF THE COMPUTER SYSTEM FOR CONTROL OF THE FERMENTATION PROCESS	140
О. Прокопюк, Н. Ромашевська, Я. Войтович, Р. Жаровський АВТОМАТИЗАЦІЯ ТА ОПТИМІЗАЦІЯ НАВЧАЛЬНОГО ПРОЦЕСУ В ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ O. Prokopyuk, N. Romashevskaya, Ya. Voytovych, R. Zharovskiy AUTOMATION AND OPTIMIZATION OF THE EDUCATIONAL PROCESS IN HIGHER EDUCATIONAL INSTITUTIONS	141
Н. Ромашевська, О. Прокопюк, Р. Жаровський ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ У ПРОЦЕСІ НАВЧАННЯ СТУДЕНТІВ N. Romashevskaya, O. Prokopyuk, R. Zharovskiy AUTOMATION AND OPTIMIZATION OF THE EDUCATIONAL PROCESS IN HIGHER EDUCATIONAL INSTITUTIONS	142
В. Тимошук, В. Карташов, Р. Королюк, Т. Рубен ОГЛЯД ПРОТОКОЛІВ КЕРУВАННЯ ДЛЯ ПОБУДОВИ АВТОМАТИЗОВАНИХ СИСТЕМ ВІДДАЛЕНОГО УПРАВЛІННЯ V. Tymoshchuk, V. Kartashov, R. Koroliuk, T. Ruben OVERVIEW OF CONTROL PROTOCOLS FOR BUILDING AUTOMATED REMOTE CONTROL SYSTEMS	143
П. Федорів, І. Федорів ВИКОРИСТАННЯ ПНЕВМО-СТРУМЕНЕВИХ ЗАХОПЛЮВАЧІВ В АВТОМАТИЧНИХ СЕПАРАТОРАХ ЛИСТОВОГО МАТЕРІАЛУ P. Fedoriv, I. Fedoriv THE USE OF PNEUMATIC-JET ATTACHERS IN AUTOMATIC SEPARATORS OF SHEET MATERIAL	145

УДК 004.4

О. Прокопюк, Н. Ромашевська, Я. Войтович, Р. Жаровський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АВТОМАТИЗАЦІЯ ТА ОПТИМІЗАЦІЯ НАВЧАЛЬНОГО ПРОЦЕСУ В ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

UDC 004.4

O. Prokopyuk, N. Romashevska, Ya. Voytovych, R. Zharovskyi

AUTOMATION AND OPTIMIZATION OF THE EDUCATIONAL PROCESS IN HIGHER EDUCATIONAL INSTITUTIONS

На сьогоднішній день проекти з віртуалізації IT-інфраструктури активно впроваджуються багатьма провідними компаніями. У процесі віртуалізації IT-інфраструктури створюється віртуальна інфраструктура, що має багато нових можливостей при збереженні існуючої схеми діяльності IT-ресурсів. Компанії-постачальники різних платформ віртуалізації готові надати інформацію про успішні проекти щодо впровадження віртуальної інфраструктури у великих банках, промислових компаніях, лікарнях, освітніх установах. Безліч переваг віртуалізації операційних систем дозволяють компаніям економити на обслуговуванні, персоналі, апаратному забезпеченні, забезпеченні безперебійної роботи.

Суть нашої концепції передбачає, що у кожному університеті чи коледжі має існувати розширюваний і масштабований центр обробки даних (ЦОД).

Переваги концепції:

- ЦОД є центром управління навчальним процесом університету;
- оновлення (upgrade) Hardware & Software проходить лише на ЦОДі, що суттєво економить витрати на комп'ютерне обладнання;
- у комп'ютерних класах використовуються тонкі (thin) та нульові (zero) клієнти;
- обчислювальна потужність ЦОД може використовуватися для наукових досліджень;
- використання віртуалізації збільшує ефективність використання комп'ютерної техніки з 10% до 70–80%;

Заняття відбуваються у комп'ютерних класах, ці класи обладнані тонкими чи нульовими клієнтами. Усі класи підключені до ЦОДу. Для кожної дисципліни створюються спеціальні «образи» для проведення занять з усіх дисциплін, що вивчаються. На перервах між заняттями оператор ЦОД завантажує необхідні «образи» для проведення заняття. Дані образи містять лише необхідне програмне забезпечення та додаткове програмне забезпечення, яке відстежує всі дії студента. Усі студенти отримують однотипні завдання. Відстеження програмного забезпечення після закінчення заняття створить звіт про всі дії студента, за допомогою якого викладач може об'єктивно оцінити студента.

Система для віртуалізації програм Microsoft SoftGrid забезпечує аналогічне «пісочниці» середовище під назвою SystemGuard, в якому програми можуть виконуватися на комп'ютерах користувачів без локальної установки операційної системи.

SystemGuard – віртуальне прикладне середовище, яке містить усі необхідні додатку елементи, такі як файли, дані реєстру, COM-об'єкти та інформація про середовище. Сумісні з SoftGrid програми не потрібно встановлювати в основній операційній системі, але вони взаємодіють з операційною системою відповідно до певних правил, щоб уникнути зайвого дублювання даних у віртуальному просторі.

УДК 004.4

Н. Ромашевська, О. Прокопюк, Р. Жаровський

(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ У ПРОЦЕСІ НАВЧАННЯ СТУДЕНТІВ

UDC 004.4

N. Romashevskaya, O. Prokopyuk, R. Zharovskiy

AUTOMATION AND OPTIMIZATION OF THE EDUCATIONAL PROCESS IN HIGHER EDUCATIONAL INSTITUTIONS

Метою даної роботи є визначити працездатність, стабільність роботи та час витрачений на відновлення працездатності сервера з технологією віртуалізації порівняно із звичайним використанням ПК у процесі навчання.

Проводився експеримент у двох аудиторіях для підготовки фахівців у галузі розробки та створення бази даних у SQL з усім необхідним програмним забезпеченням. В обох аудиторіях встановлюється стандартне програмне забезпечення для навчання фахівців: Мови програмування, Mathcad, AutoCAD, MS Office та інше. Єдиною відмінністю є саме те, що в одній аудиторії встановлюється сервер, налаштовується Active Directory, налаштування домену. Далі - розгортається VMware з 12 віртуальними машинами, на одній встановлюється SQL Server - для навчання розробників, після закінчення установки та налаштування - знімається образ для перекидання на решту 11 віртуальних машин та резервного відновлення на випадок непередбачених проблем.

В іншій аудиторії для навчання розробників – на кожному комп'ютері встановлюється VMware і на одній віртуальній машині встановлюється OS Linux, на якому ставиться SQL Server, налаштовується, після цього зберігається образ однієї віртуальної машини, що розгортається на інші 11 комп'ютерів.

Весь експеримент складається із трьох частин метою яких є:

- підготовка аудиторій, тобто встановлення та налаштування ПЗ.
- експериментальна перевірка працездатності та стабільної роботи двох аудиторій, а також фіксування технічних проблем та фіксування часу на їх усунення.
- підрахунок та обробка всіх отриманих даних.

В результаті проведених досліджень отримано наступні дані та результати.

Допрацьована та повністю налаштована доменна система разом з технологією віртуалізації на базі VMware дозволяє в 3 рази скоротити випадки технічних збоїв, а час усунення цих збоїв – у 5 разів.

Система проста у користуванні та зрозуміла. Проте політики безпеки та винятків потребують ретельного та уважного налаштування.

Система Windows Server 2008 R2 з технологією віртуалізації дозволяє дати доступ до свого власного віртуального сервера і дати повноцінну можливість налаштувати, зіпсувати і відновити її самостійно, без шкоди для інших учасників – викладач або системний адміністратор здатний відновити працездатність SQL Server протягом 5–10 хвилин (на відміну від звичайного методу 40 хвилин або більше).

Віртуалізація програм дозволила спростити розгортання, адміністрування, оновлення та видалення програм, що використовуються під час роботи та навчання.

Серверна віртуалізація дозволяє значно скоротити кількість фізичних серверів шляхом їхньої консолідації: розміщення декількох серверів на одному фізичному обладнанні. Консолідація досягається шляхом розміщення серверів в окремих віртуальних машинах, розташованих на одному фізичному сервері, та керованих гіпервізором.