Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Захищена корпоративна комп'ютерна мережа: створення та конфігурація"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Калушка Роман Володимирович
підпис (прізвище та ініціали)

Керівник Карпінський М.П.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Жаровський Р.М.
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

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

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Калушці Роману Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Захищена корпоративна комп'ютерна мережа: створення та конфігурація

Керівник роботи Карпінський Микола Петрович, доктор технічних наук, професор
професор кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 12.12.2024

3. Вихідні дані до роботи Наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Огляд комп'ютерних мереж
2. Створення захищеної корпоративної комп'ютерної мережі
3. Конфігурація пристроїв і серверів
4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титул. 2. Актуальність теми. 3. Мета дослідження. 4. Завдання дослідження. 5. Об'єкт і предмет дослідження. 6. Наукова новизна. 7. Схема мережі SAN, модель OSI 8. Дані щодо конфігурації віртуальної машини. 9. Логічна схема мережі SAN 10. Конфігурація порту WAN маршрутизатора. 11. Конфігурація порту LAN 12. Серверні накопичувачі SSD. 13. Резервне копіювання та оперативна пам'ять RAM сервера Backup. 14. Мережеві карти та адаптери. 15. Приклад сконфігурованого контролера домену 16. Апаратна конфігурація dhcp-сервера. 17. Апаратна конфігурація файлового сервера 18. Розбиття диска файлового сервера. 19. Висновки. 20. Апробація

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 20.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.11 – 22.11	Виконано
2.	Підбір джерел про захищені корпоративні комп' ютерні		
	мережі	23.11 – 26.11	Виконано
4.	Опрацювання джерел захищені корпоративні		
	комп' ютерні мережі	27.11 – 30.11	Виконано
5.	Виконання дослідження щодо розробки захищеної		
	Корпоративної комп' ютерної мережі	01.12 – 06.12	Виконано
6.	Розробка алгоритмів функціонування мережі	07.12 – 10.12	Виконано
7.	Оформлення розділу «Огляд комп'ютерних мереж»	11.12 – 13.12	Виконано
8.	Оформлення розділу «Створення захищеної		
	корпоративної комп'ютерної мережі»	14.12 – 15.12	Виконано
9.	Оформлення розділу «Конфігурація пристроїв		
	і серверів»	16.12 – 18.12	Виконано
10	Виконання завдання до підрозділу «Охорона праці та		
	безпека в надзвичайних ситуаціях»	06.12 – 16.12	Виконано
11.	Оформлення кваліфікаційної роботи	14.12 – 19.12	Виконано
12.	Попередній захист кваліфікаційної роботи	19.12 – 20.12	Виконано
13.	Захист кваліфікаційної роботи	26.12.2024	

Студент _____ Калушка Р.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Карпінський М.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Захищена корпоративна комп'ютерна мережа: створення та конфігурація // Калушка Роман Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // с. – 62, рис. – 36, табл. – 2, слайд. – 18, бібліогр. – 17.

Ключові слова: комп'ютерна мережа, сервер, віртуальна машина, захист мережі, комутатор, канал зв'язку

У цій роботі застосовано SAN (Storage Area Nework). Всі сервери мають виділений доступ до дискових ресурсів, що забезпечує стійкість комп'ютерної системи. Створені віртуальні машини підтримують високу доступність і масштабованість комп'ютерної мережі. Канали зв'язку між сервером і комутатором дало можливість для розподілу трафіку між ними, використовуючи алгоритми балансування навантаження.

Розроблене рішення може бути впроваджене в корпорації середнього розміру.

ANNOTATION

A secure corporate computer network: development and configuration // Kalushka Roman // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2024 // p. - 62, Fig. - 36, Table - 2, Slides - 19, References - 17.

Keywords: computer network, server, virtual machine, network protection, switch, communication channel

In this work, SAN (Storage Area Nework) is used. All servers have dedicated access to disk resources, which ensures the stability of the computer system. The created virtual machines support high availability and scalability of the computer network. Communication channels between the server and the switch made it possible to distribute traffic between them using load balancing algorithms.

The developed solution can be implemented in a medium-sized corporation.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AD	—	Active Directory
ARP	—	Address Resolution Protocol
CPU	—	Central Processing Unit,
DHCP	—	Dynamic Host Configuration Protocol
DNS	—	Domain Name System
DS	—	Data Storage
ESX	—	Elastic Sky X
FC	—	Fibre Channel
IP	—	Internet Protocol
LAN	—	Local Area Network
LCD	—	Liquid Crystal Display
LTO	—	Linear Tape-Open
MAC	—	Media Access Control
NAS	—	Network Attached Storage
OSI	—	Open Systems Interconnection
PC	—	Personal Computer
RAID	—	Redundant Array of Independent Disks
RAM	—	Random Access Memory
SAN	—	Storage Area Network
SAS	—	Serial Attached SCSI
SSD	—	Solid-State Drive
TCP/IP	—	Transmission Control Protocol/Internet Protocol
UTP	—	Unshielded Twisted Pair
WAN	—	Wide Area Network

ВСТУП

Актуальність теми.

Інформаційні технології нині займають ключову позицію в нашому житті. Це зумовлено, зокрема, тим, що прогрес у галузі електроніки та мережевих технологій розвивається з приголомшливою швидкістю. Мережі комп'ютерів стали невід'ємною частиною діяльності більшості великих компаній, і саме на їх основі зводяться складні інформаційні структури. Сучасні підприємства вже не уявляють собі ефективну роботу без глобальної мережі Інтернет та обчислювальних пристроїв.

Мета і задачі дослідження.

Ця робота має на меті представити, як створити захищену комп’ютерну мережу та на її основі всю комп’ютерну систему, яка може використовуватися в корпорації. Всю мережу буде створено на основі доступних рішень, які дають змогу побудувати, захистити та сконфігурувати мережу.

Завданнями дослідження є:

У роботі буде представлено створення захищеної комп’ютерної мережі для корпорації середнього розміру. Першим елементом буде створення корпоративної комп’ютерної мережі, яка дозволить об’єднати всі пристрої в одну комп’ютерну систему. Надалі буде представлено пристрої, необхідні для створення всієї корпоративної комп’ютерної мережі разом із запропонованими конфігураціями. Вся мережа базуватиметься на віртуальному середовищі VMware. Також висвітлено та обґрунтовано застосування засобів, які забезпечують функціонування мережі. Останнім елементом роботи буде представлення конфігурацій всіх пристроїв (маршрутизатора, серверів, дискового накопичувача тощо), на підставі яких можна реалізувати проєкт у будь-якій компанії. Теж буде описано системні послуги.

Об'єкт дослідження.

Процес захисту корпоративної комп’ютерної мережі від вибіркових атак, які впливають на основні характеристики безпеки корпоративної комп’ютерної

мережі в спеціалізованих застосуваннях.

Предмет дослідження.

Методи та засоби для забезпечення захищеності корпоративної комп’ютерної мережі.

Наукова новизна одержаних результатів кваліфікаційної роботи.

Удосконалення підходів до захисту корпоративної комп’ютерної мережі з урахуванням новітніх технологій у спеціалізованих застосуваннях.

Практичне значення одержаних результатів.

Розробка методів визначення базових характеристик безпеки корпоративної комп’ютерної мережі в умовах впливу вибіркових атак.

Апробація результатів магістерської роботи.

Основні результати досліджень були обговорені на XII науково-технічній конференції «Інформаційні моделі, системи та технології» (18–19 грудня 2024 року, м. Тернопіль, Україна).

Публікації.

Основні результати кваліфікаційної роботи опубліковано в матеріалах конференції. (див. Додаток А).

РОЗДІЛ 1 ОГЛЯД КОМП’ЮТЕРНИХ МЕРЕЖ

На сьогоднішній день основним складником будь-якої корпорації, підприємства, установи або організації є комп'ютерна мережа. Це поняття охоплює надзвичайно широкий спектр, який можна визначити як взаємодію між принаймні двома обчислювальними пристроями з метою обміну інформацією. У більш широкому контексті комп'ютерна мережа представляє собою систему комунікацій, яка може здійснюватися через дротові або бездротові канали, а також включає в себе самі комп'ютери різних призначень та відповідне мережеве обладнання. Для побудови такої мережі використовуються різноманітні елементи, зокрема [1, 2]:

- електропроводка (англ. wiring, cabling);
- мережевий комутатор (англ. switch);
- маршрутизатор (англ. router);
- сервер (англ. server);
- комп'ютер (англ. computer).

1.1 Топологія

Сучасною нормою побудови комп’ютерних мереж в кожній корпорації, фірмі чи організації є топологія «зірка», тому її застосовано в цій роботі. Вона характеризується тим, що всі пристрої в мережі (сервери, комп’ютери, принтери, точки доступу WiFi) під’єднуються до загальної центральної точки, якою є комутатори [1, 2]. Для забезпечення безпеки та безперервності роботи мережі завжди слід використовувати принаймні два комутатори, які забезпечать безперервність роботи системи у ситуації виходу з ладу одного з пристроїв. Пристрої з кількома мережевими картами (сервери, дискові накопичувачі, бібліотеки) під’єднуються до обох комутаторів, а кожна мережева карта — до іншого комутатора. Однак під’єднуємо комп’ютери користувачів лише до одного з комутаторів. На рисунку нижче показано приклад проєкту мережі.

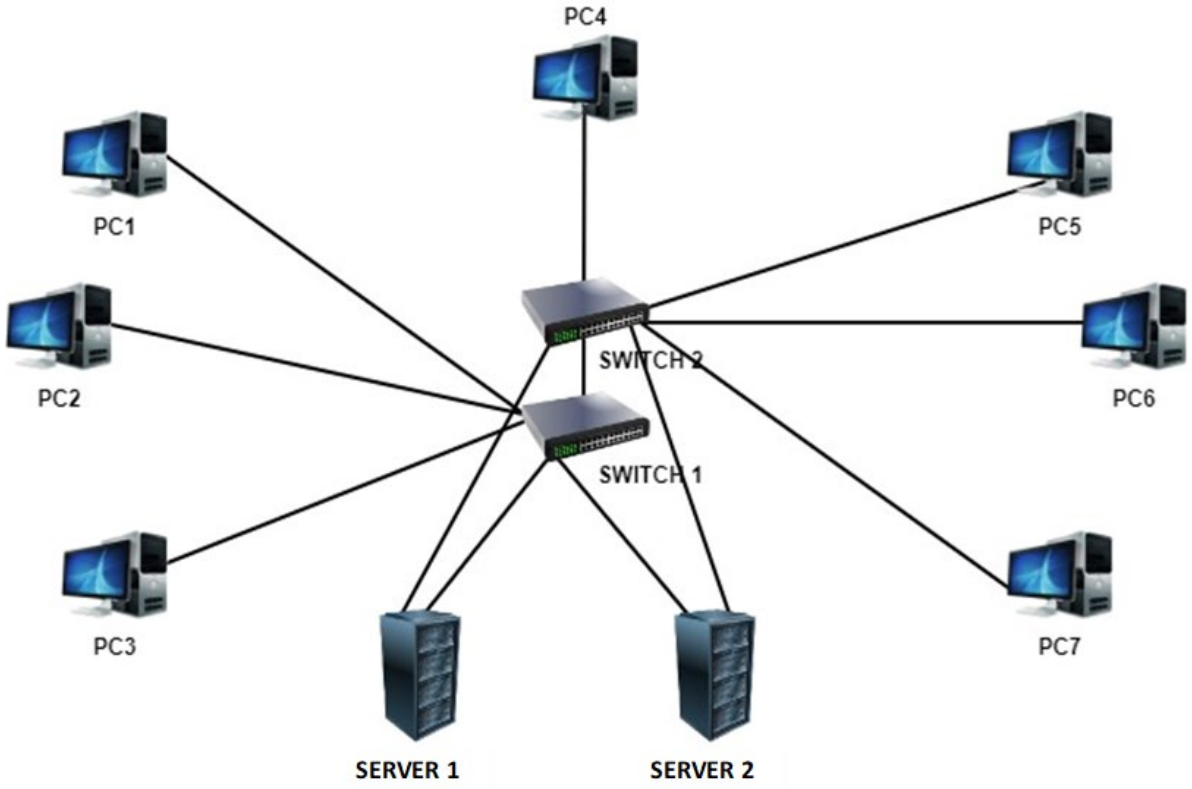


Рисунок 1.1 – Приклад схеми мережі

Як вказано на схемі, вся мережа побудована на двох комутаторах, що забезпечує резервування. Для випадку аварії одного з комутаторів сервери залишаються доступними в мережі, оскільки мережевий трафік автоматично перемикається на інший пристрій. Комутатори з пропускною здатністю 1 ГБ/с є стандартними в локальних мережах. З причини великих обсягів передаваних даних пристрої з меншою пропускною здатністю застосовуються набагато рідше.

Одним з важливих елементів комп'ютерної системи організації повинна бути мережа SAN (Storage Area Network) (див. рисунок 1.2). Це підмережа, фізично відокремлена від локальної мережі, яка з’єднує дискові ресурси (наприклад, дискові масиви, стрічкову бібліотеку) із серверами. Завдяки цьому всі сервери мають виділений доступ до дискових ресурсів, що забезпечує можливість побудови високоефективної, масштабованої та стійкої до збоїв комп’ютерної системи.

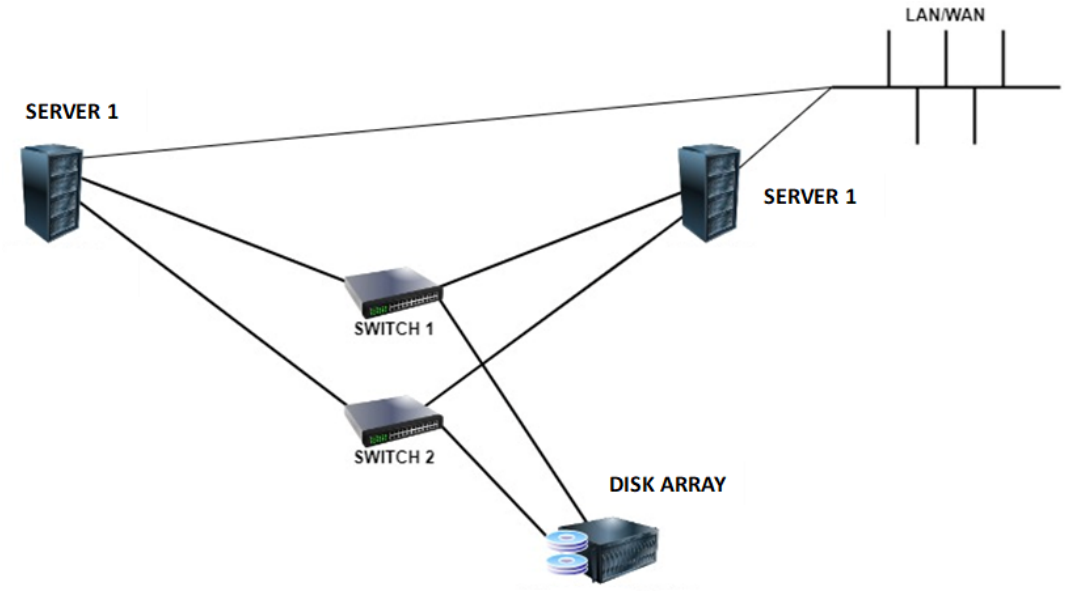


Рисунок 1.2 – Схема мережі SAN

1.2 Пристрої

Для створення комп'ютерної мережі необхідні комутатори, які є основним елементом, що забезпечує подальший розвиток інфраструктури. Їхнє завдання — керування пакетним трафіком у локальній мережі. Комутатори працюють на другому рівні моделі OSI (див. рисунок 1.3) [3].

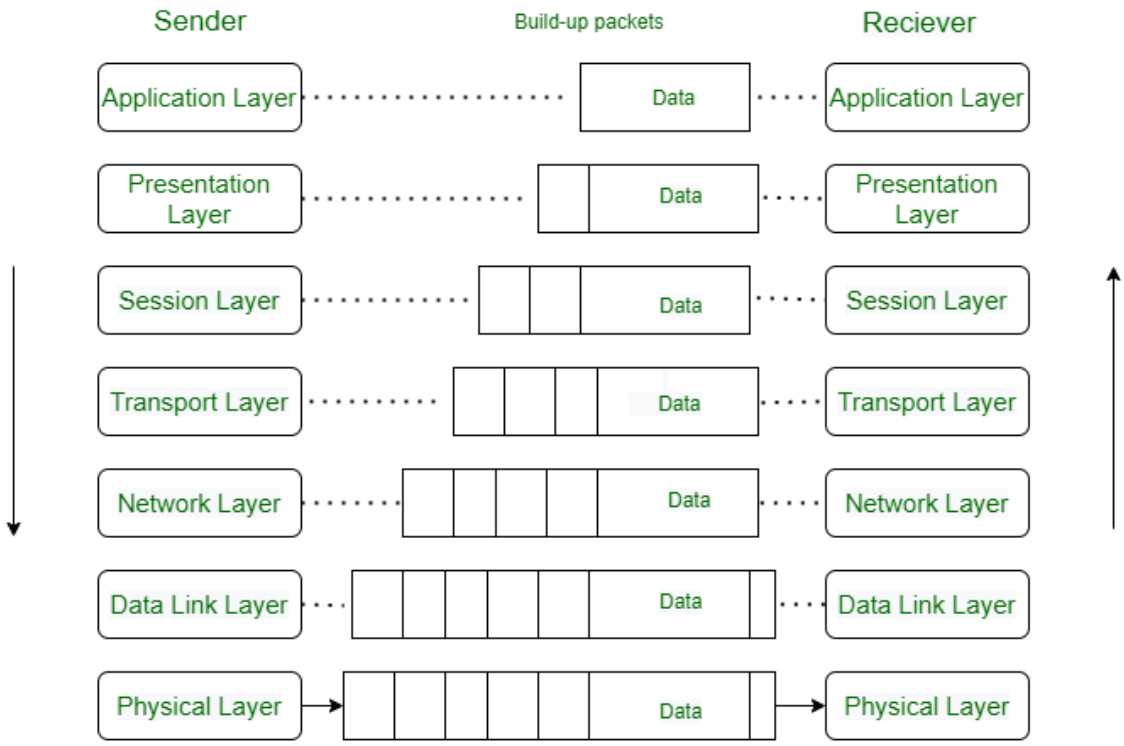


Рисунок 1.3 – Модель OSI

Провідним виробником комутаторів є компанія CISCO, яка має дуже широкий асортимент продукції (див. рисунок 1.4). Ці мережеві комутатори характеризуються, серед іншого:

- широкі можливості реалізації – можна вибрати традиційний режим, керований у хмарі або повний контроль над структурою;
- безпека та риси інтелекту;
- провідний стандарт;
- надійність;
- масштабованість.

Рисунок 1.4 – Приклади комутаторів серії Cisco Business 250

Звичайно, на ринку є й інші виробники комутаторів, наприклад TP-Link або D-Link. На жаль, це виробники, які асоціюються переважно з побутовою технікою. Для побудови корпоративних мереж підходять тільки моделі з групи Business.

1.3 Електропроводка

Усі пристрої в локальній мережі слід під’єднати за допомогою кабелю категорії 6 (CAT 6), відомого як «вита пара» (див. рисунок 1.5) [4]. Кабель типу CAT 6 сумісний із попередніми стандартами CAT 5 та CAT 5e.

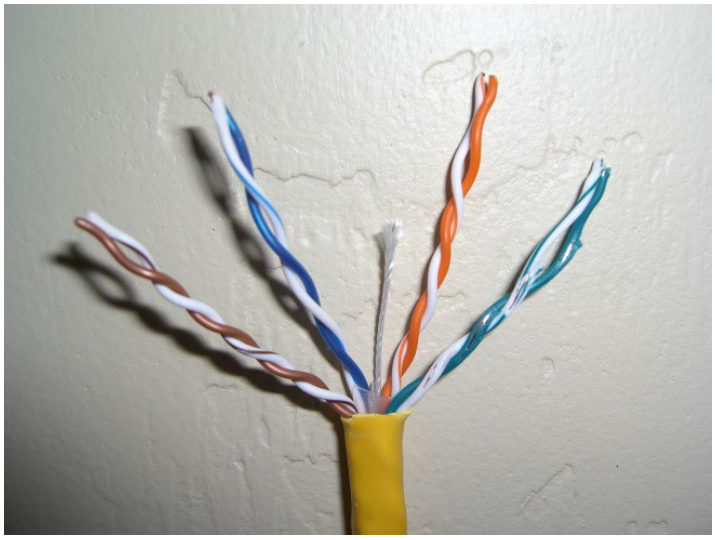


Рисунок 1.5 – Кабель типу UTP CAT 6

Завжди доцільно вибирати електропроводку найвищої якості. Кабелям типу CAT 6 притаманні підвищені вимоги щодо системного шуму та перехресних перешкод порівняно зі своїми попередніми аналогами. Кабель CAT 6 працює в діапазоні до 250 МГц, а CAT 6e аж до 500 МГц. Максимальна довжина кабелю від пристрою до пристрою не може перевищувати 100 м. Якщо потрібно під’єднати пристрої, які знаходяться на більшій відстані один від одного, то слід використовувати активний пристрій (перемикач або підсилювач). Максимальна пропускна здатність кабелю типу CAT 6 становить 1000 Мбіт/с. На потреби нашої роботи цілком достатньо цього типу кабелю, і його застосовано для з’єднання між собою всіх компонентів.

1.4 Маршрутизатор

Маршрутизатор (англ. Router) — це апаратний компонент мережі, призначений для з'єднання комп'ютерних мереж, що використовують різні адресні класи, виконуючи функцію комунікаційного вузла (див. рисунок 1.6). Він функціонує на третьому рівні моделі OSI (див. рисунок 1.3). Завдяки даним, що містяться в пакетах протоколу TCP/IP, маршрутизатор здійснює перенаправлення пакетів між мережами, передаючи їх від однієї до іншої. [2]. Професійні маршрутизатори зазвичай містять два або чотири довільно конфігуровані порти.

Високопродуктивні маршрутизатори – це пристрої, які можуть обробляти значні обсяги інформації за короткий проміжок часу. Маршрутизатор в нашій мережі буде пристроєм, який забезпечить доступ до Інтернету, тобто з'єднає мережу інтернет-провайдера з нашою локальною мережею. Конфігурація брандмауера, а саме Anti ARP Spoofing, також важлива. Це захищає мережу Ethernet від мережевих атак, які дозволяють перехоплювати дані в сегменті локальної мережі.

Рисунок 1.6 – Зовнішній вигляд маршрутизатора організації CISCO

РОЗДІЛ 2 СТВОРЕННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ КОМП'ЮТЕРНЕЇ МЕРЕЖІ

2.1 Віртуальне середовище

Віртуальне середовище — це програмне забезпечення, яке дозволяє створювати окремі комп’ютерні системи на одному чи кількох фізичних серверах [5-8]. Полягає це на створенню віртуальних машин, кожна з яких функціонує як окремий комп’ютер. Програмне забезпечення віртуалізації розділяє ресурси фізичних серверів, наприклад ядра процесора та оперативну пам’ять, і створює віртуальні сервери, які працюють незалежно та не впливають один на одного. На кожному з них можна встановити будь-яку операційну систему (Windows, Linux). Ці незалежні системи працюють на фізичному сервері та видимі для зовнішнього світу як автономні сервери. Загальне використання ресурсів (CPU, RAM) усіх віртуальних машин не може перевищувати ресурсів фізичного сервера.

У цій роботі застосовано віртуальне середовище VMware.

Однією з конфігурацій, які застосовуються для створення віртуального середовища, є використання двох фізичних серверів, які назвемо хостами, та дискового накопичувача, під’єднаного до фізичних серверів через мережу SAN. Ядра процесора та оперативна пам’ять для створення віртуальних машин використовуватимуть фізичні процесори та оперативну пам’ять обох хостів, а масив забезпечуватиме дискові ресурси для цих віртуальних машин. Кожен хост має SSD-накопичувач на 500 ГБ, на якому буде встановлено лише операційну систему VMware під назвою supervisor. Це програмне забезпечення відповідає за віртуалізацію апаратних ресурсів комп’ютера.

IT-систему в організації також можна побудувати без використання віртуального середовища [9]. Тоді кожен сервер є фізичною апаратною одиницею. Кожен з них має окремий блок живлення, процесор і пам'ять. Доступні на даний момент фізичні сервери мають великий надлишок потужності по відношенню до

потреб, які використовуються основними службами (спільний доступ до файлів, спільний доступ до принтера, DNS, DHCP) комп’ютерної системи в мережі організації.

a) Відмовостійкість

Якщо запустити кожен із серверів організації на окремій фізичній машині, апаратний збій такого сервера призведе до відсутності доступу до цього сервісу. Для випадку, наприклад, збою контролера домену Active Directory, усі користувачі втратять доступ до файлових ресурсів і навіть не зможуть увійти. Як бачимо, збій однієї такої послуги призводить до припинення роботи всієї організації. Під час збою одного з фізичних хостів можна швидко запустити той самий віртуальний сервер на іншому хості. Відмовостійкість є найбільшою перевагою віртуального середовища.

b) Доступність

Ще однією перевагою віртуального середовища є висока доступність. Використовується його, якщо потрібно обслуговувати один із хостів. Тоді віртуальне середовище VMware має можливість перемістити всі віртуальні сервери на один хост, не вимикаючи їх. Ця функція називається vMotion і дозволяє переміщувати запущену віртуальну машину з одного хоста на інший. Послуги цієї машини доступні протягом усього часу перенесення.

c) Масштабованість

Важливою перевагою віртуального середовища є масштабованість. Це дозволяє збільшити апаратні ресурси віртуальної машини, такі як кількість ядер, оперативну пам’ять і дискові ресурси, без необхідності придбання додаткового обладнання. Для цього застосовано резерви, розташовані на фізичних серверах. Масштабованість віртуального середовища також використовується механізмом балансування навантаження, який відстежує навантаження на фізичні процесори та пам'ять на хостах. За необхідності він переміщує віртуальні машини таким чином, щоб однаково використовувати апаратні ресурси кожного фізичного сервера.

2.1.1 Планування простору для віртуальних машин

У конкретному випадку нашої роботи створено 6 віртуальних машин, а саме:

- сервер DHCP
- файловий сервер
- сервер друку
- контролер AD (Active Directory)
- сервер бази даних
- сервер додатків

Кожна з них потребує різних апаратних ресурсів, тому в нижченаведеній таблиці 2.1 представлено запропоновані конфігурації кожної віртуальної машини.

Таблиця 2.1 – Дані щодо конфігурації віртуальної машини

Назва віртуальної машини	Кількість ядер процесора (CPU)	Пам'ять RAM	Жорсткі диски
Сервер DHCP	2 CPU(s)	8 ГБ	1 диск: 120 ГБ 2 диск: 12 ГБ
Файловий сервер	2 CPU(s)	8 ГБ	1 диск: 80 ГБ 2 диск: 1500 ГБ 3 диск: 25 ГБ
Сервер друку	4 CPU(s)	8 ГБ	1-й диск: 100 ГБ 2-й диск: 12 ГБ
Контролер AD	2 CPU(s)	8 ГБ	1 диск: 80 ГБ 2 диск: 12 ГБ 3 диск: 25 ГБ
Сервер бази даних	8 CPU(s)	32 ГБ	1 диск: 120 ГБ 2 диск: 48 ГБ 3 диск: 400 ГБ 4 диск: 150 ГБ 5 диск: 100 ГБ 6 диск: 100 ГБ 7 диск: 300 ГБ
Сервер додатків	2 CPU(s)	8 ГБ	1 диск: 100 ГБ

			2 диск: 12 ГБ 3 диск: 500 ГБ

Наведену вище конфігурацію ретельно підготовлено та вона є оптимальна для впровадження в організації середньої величини. Звичайно, слід пам'ятати, що мережу засновано на віртуальних машинах, що забезпечує масштабованість. Це означає, що в будь-який момент, за потреби, можна збільшити апаратні ресурси.

2.1.2 Сервери та хости

Фізичний сервер — це не що інше, як високоефективний комп’ютер, який забезпечує роботу інших послуг, програм або пристроїв, іменованих клієнтами. Його основна мета — надати користувачам дані та ресурси. Сервери, в більшості випадків, монтуються в шафах-стійках (див. рисунок 2.1 нижче) і залишаються ввімкненими 24 години на добу протягом тижня.

Рисунок 2.1 – Серверна шафа типу RACK

Для такої мережі, яку охоплює дана робота, обґрунтовано застосовувати два фізичні сервери типу Lenovo ThinkSystem SR650, які повинні бути змонтовані в стійковій шафі. Обидвом серверам притаманна однакова конфігурація, як показано в таблиці 2.2 нижче.

Таблиця 2.2 – Дані щодо конфігурації сервера

Модель	ThinkSystem SR650
Процесор (CPU)	Intel(R) Xeon(R) Silver 4110 2 x CPUs x 2.1 GHz CPU Cores 2 x 8 cores

Пам'ять RAM	192 ГБ
Жорсткий диск	128 ГБ SSD

Ця конфігурація сервера дозволяє створити передбачувану кількість віртуальних машин і залишає великий запас апаратних ресурсів. Резервне копіювання важливе, оскільки в разі збою або технічного обслуговування воно дозволяє перенести всі віртуальні машини з одного хоста на інший. На рисунку 2.2 нижче показано фізичний сервер, описаний вище.

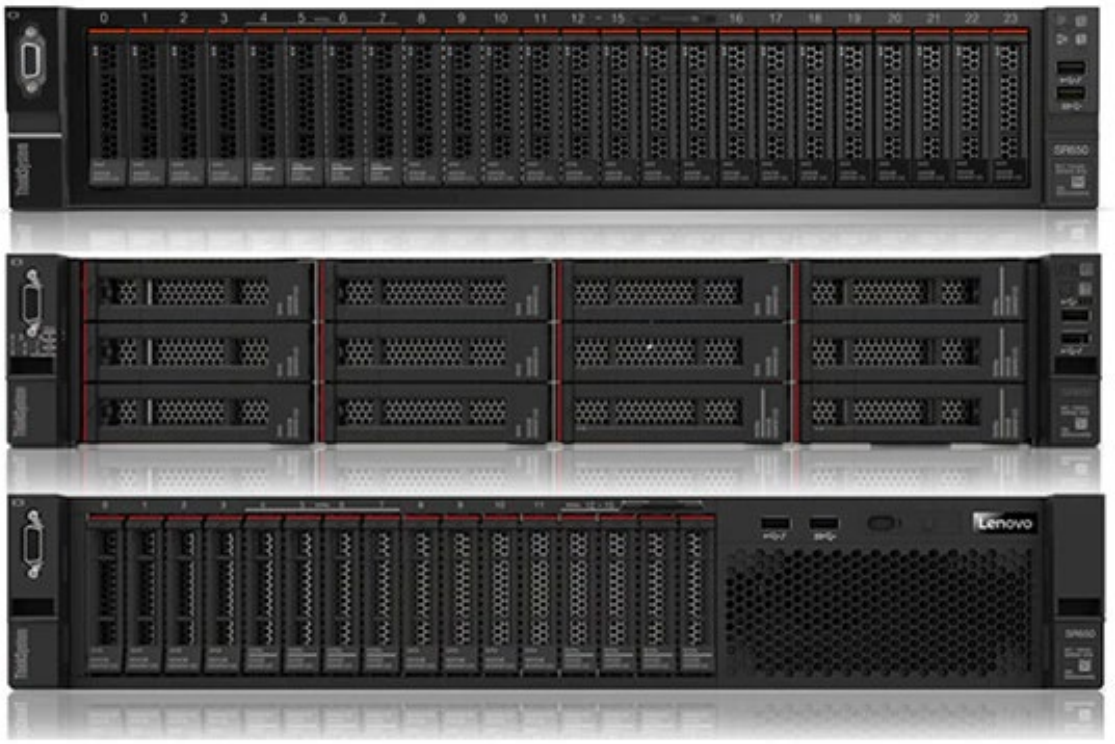


Рисунок 21.2 – Фізичний сервер компанії Lenovo

2.1.3 Дисковий накопичувач

Дисковий накопичувач – це набір дисків, налаштованих таким чином, щоб забезпечити високу стійкість до збоїв і можливість використання дискового простору з кількох дисків як єдиного цілого. Це рішення використовується для підвищення ефективності передачі даних, збільшення дискового простору і, як було наведено вище, стійкості до збоїв і втрати даних. Дискові накопичувачі класифікуються рівнем рівнів та позначаються цілим числом. Окремі рівні накопичувача описані нижче, починаючи з рівня 0, який є основним

накопичувачем [10].

- RAID 0 (черговий том) – накопичувач, що складається мінімум з двох дисків. Дані зберігаються на цьому рівні шляхом поділу їх на т.зв «смуги» і розташовані по черзі на всіх дисках, що входять до складу дискового накопичувача. Перевага цього рішення полягає в покращенні продуктивності запису та читання даних, а недоліком є необхідність використання лише накопичувачів однакової ємності. Збій будь-якого з дисків у цьому рішенні призводить до втрати всієї інформації.
- RAID 1 (дзеркало) – як і у випадку RAID 0, накопичувач повинен складатися як мінімум з двох дисків. Дані зберігаються на всіх дисках паралельно. Як і вище, у цьому рішенні можна використовувати лише диски з однаковою ємністю, оскільки, коли використовуються різні диски, доступний дисковий простір дорівнюватиме ємності найменшого. Перевага цього дискового накопичувача полягає в тому, що надійність зростає геометрично зі збільшенням кількості дисків, тому що ризик виходу з ладу двох дисків становить половину ризику виходу з ладу одного диска. Ризик пошкодження дискового накопичувача зводиться до пошкодження останнього диска дискового накопичувача, тільки в цьому випадку будуть втрачені всі дані.
- RAID 5 – накопичувач повинен складатися як мінімум з трьох дисків. Накопичувачі повинні бути однакової місткості. У цьому рішенні збій будь-якого диска не призводить до втрати даних. Просто виймається пошкоджений диск з дискового накопичувача і вставляється робочий диск. Накопичувач сам перебудується, тобто розподілить дані так, як це було до збою. Недоліком цього рішення є те, що якщо два диски пошкоджені, відновити дані вже неможливо. Є також RAID 5E і 5 EE, які розширюються додатковим диском гарячого резерву. Теоретично вони стійкі до виходу з ладу двох дисків, але на практиці диски не можуть бути пошкоджені одночасно, оскільки, як і у випадку з RAID 5, дані будуть втрачені.
- RAID 6 – це розширена версія накопичувача RAID 5. Має дубльовані блоки парності, що означає, що для його коректної роботи потрібно як мінімум 4

диски, два з яких використовуються для запису даних парності. Система повністю стійка до виходу з ладу двох дисків одночасно. Дисковий накопичувач здатний витримати вихід з ладу другого диска під час відновлення системи після збою першого.

- RAID 10 – це багаторівневий накопичувач, який створює необмежений логічний диск. Для цього використовується під'єднання RAID 0, яке прискорює роботу системи, а RAID 1 забезпечує безпеку. Ця комбінація гарантує найменшу кількість дисків, які потрібно відновити у разі збою диска.

У цій роботі прикладом дискового накопичувача, який використано, є дисковий накопичувач типу DELL (Dell unity 300). Для забезпечення резервування пам'яті прийнято не менше 22 дисків ємністю 1 ТБ кожен. На рисунку (див. рисунок 2.3) нижче показано дисковий накопичувач.

Рисунок 2.3 – Зовнішній вигляд дискового накопичувача на прикладі "Google.com"

2.1.4 Мережа SAN

Як описано вище, мережа SAN – це мережа, що з'єднує дискові ресурси з серверами, відокремленими від локальної мережі [2]. На рисунку 2.4 нижче показано приклад схеми мережі SAN, яку можна застосувати до цієї роботи: в комутаторах Cisco рекомендується використовувати модулі 10 Гбіт/с. У нашій роботі під'єднано ці модулі до виділених мережевих карт на серверах за допомогою оптоволоконних кабелів.

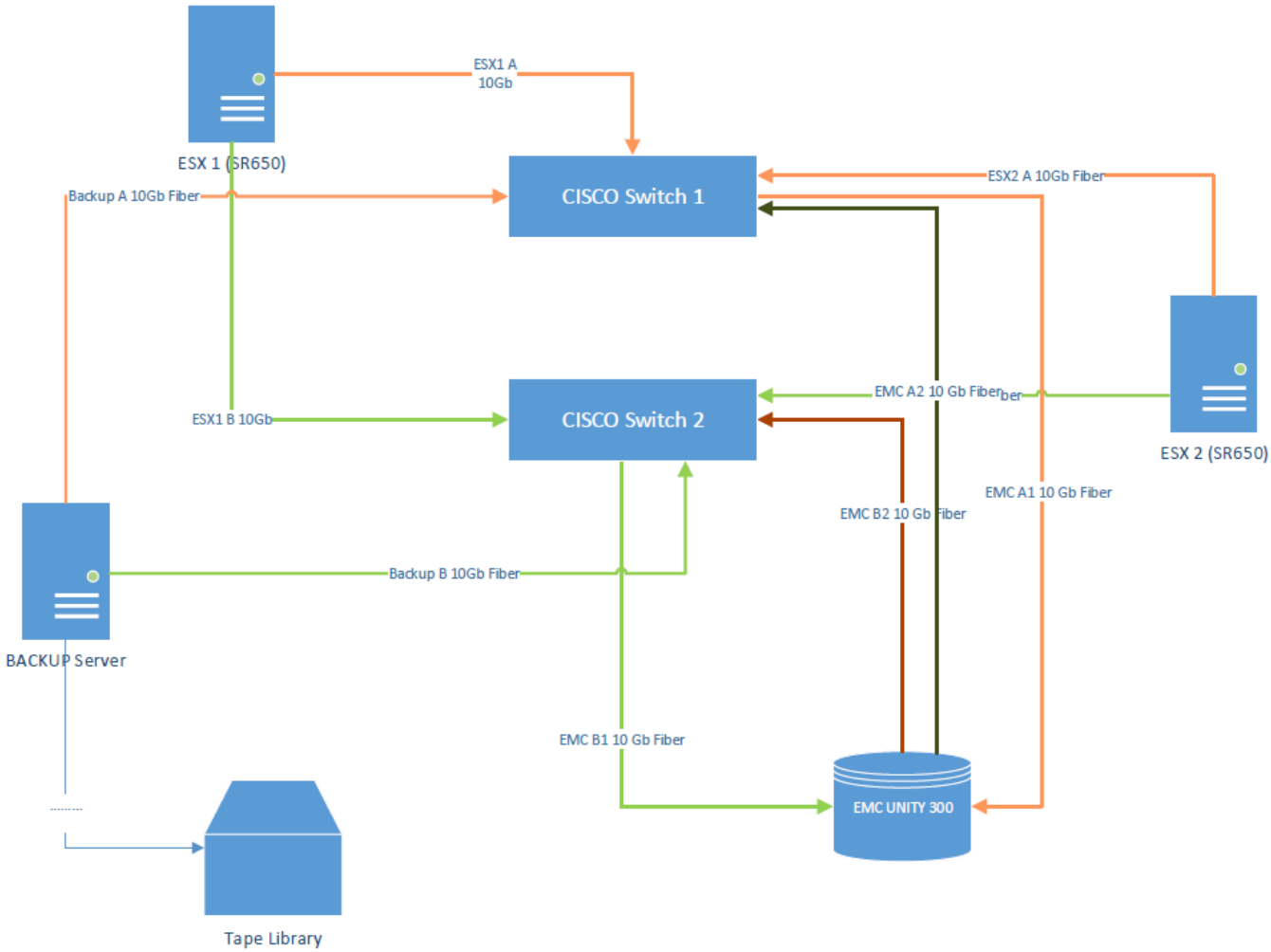


Рисунок 2.4 – Логічна схема мережі SAN

Якщо неможливо використовувати виділені модулі SAN у комутаторах Cisco, то є змога застосувати оптоволоконні комутатори (англ. Fibre Channel (FC)), наприклад, типу Brocade.

На рисунку 2.5 показано приклад під'єднання серверів і дискових накопичувачів за допомогою модулів на серверах типу Cisco.

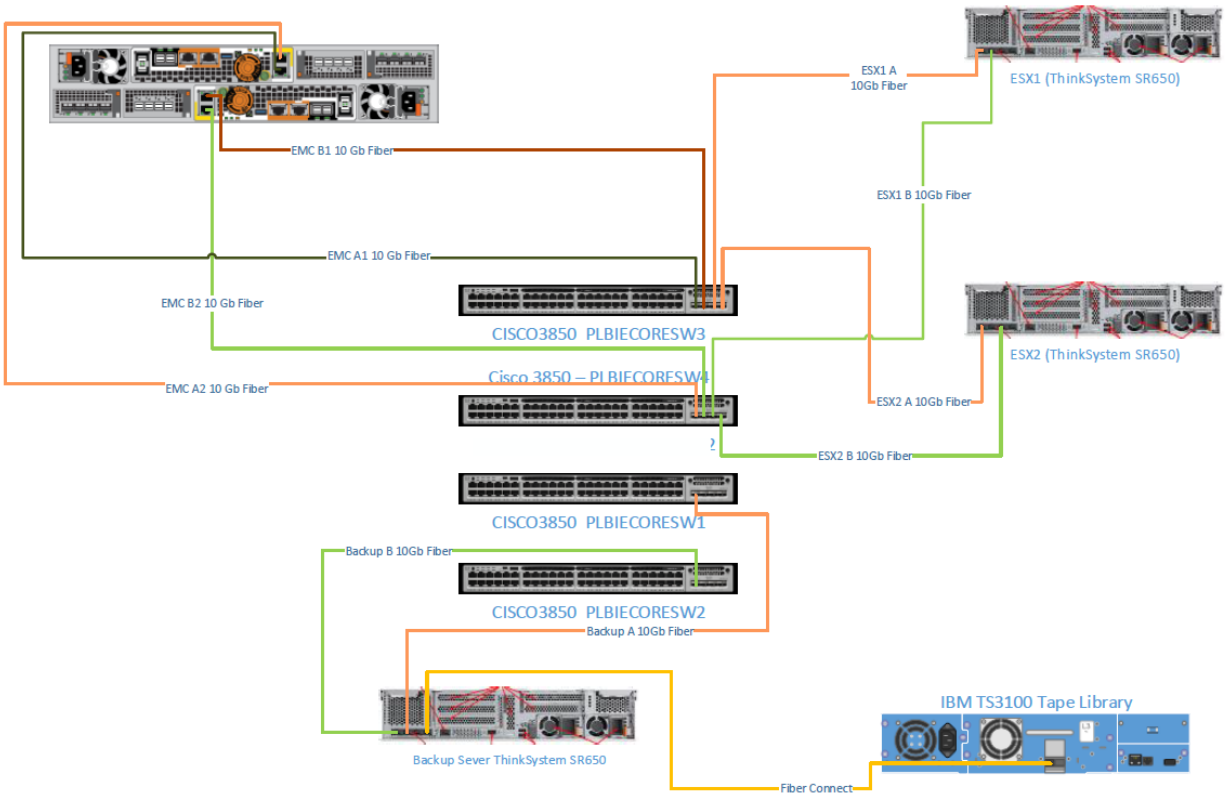


Рисунок 2.5 – Схема мережі SAN

Як показано на вище наведеному рисунку, кожен сервер і дисковий накопичувач під'єднані до двох різних комутаторів. Завдяки такій пропозиції вихід з ладу будь-якого елемента мережі (мережевої карти в сервері або дисковому накопичувачі, порта або модуля в комутаторі, оптоволоконного кабеля) не призведе до недоступності дискового накопичувача для серверів.

2.2 Резервне копіювання

Система резервного копіювання (англ. Backup) — це не що інше, як захист даних для випадку збою обладнання, наприклад, пошкодження жорсткого диска. Згідно з рекомендаціями дані повинні бути захищені відповідно до правила 3-2-1, яке стверджує, що повний захист даних відбувається лише тоді, коли наявні щонайменше три резервні копії на двох різних пристроях. Одна з копій має бути збережена на офлайн-носії. Зараз створення резервних копій у хмарі стає все популярнішим, а це дає змогу гарантувати, що резервна копія не зникне [11-13].

На даний момент виділяють три основні види резервного копіювання: повне, диференційне та інкрементне, які детальніше розглянуто нижче.

- Повне резервне копіювання (англ. Full Backup або L0) – цей тип резервного копіювання дозволяє за наявності збою відновити всю систему до збою. Єдиним істотним недоліком цього рішення є час, який потрібен для створення такої копії, та зайняття великого обсягу дискового простору.
- Диференційне резервне копіювання (англ. Differential Backup або L1) – це накопичувальне резервне копіювання всіх змін, внесених після останньої повної або звичайної резервної копії. Таким чином, резервна копія охоплює лише дані, що були додані або змінені з моменту останнього повного архівування. Цей метод зазвичай займає менше простору, але для відновлення повної інформації після збоїв необхідно використовувати як останню повну резервну копію, так і останню накопичену архівну копію.
- Інкрементне (інакше додаткове) резервне копіювання (англ. Incremental Backup або L2) – це найшвидший метод резервного копіювання, який до того ж займає найменше місця. На жаль, таке резервне копіювання також є найменш повним, а саме – при цьому копіюються лише файли, змінені з моменту останнього інкрементного резервного копіювання. Під час збою, якщо є в наявності лише цей тип резервної копії, то знадобиться не лише остання повна резервна копія, але й усі зменшені. Тому відновлення копій за допомогою цієї системи може зайняти дуже багато часу.

Звичайно, тип системи резервного копіювання має бути ретельно обраний та цьому повинен передувати ретельний розгляд потреб корпорації, планів і бюджету. У нашій роботі запропоновано систему резервного копіювання, яка ґрунтується на фізичному сервері та під’єднаній до нього стрічковій бібліотеці.

2.2.1 Сервер резервного копіювання (Backup сервер)

Для належного функціонування системи резервного копіювання потрібне програмне забезпечення, яке працює на сервері Windows. Воно повинне бути

встановлено на фізичному сервері. У цій роботі запропоновано програмне забезпечення VEEAM. У цьому програмному забезпеченні використовується функція дедуплікації, яка полягає в тому, що під час створення резервної копії обчислюються контрольні суми кожного блоку даних. І якщо система зустрічає інший блок із такою ж контрольною сумою, вона не копіює його, а лише зазначає, що такий сам блок також розташований в іншому місці. Завдяки цьому, якщо створюються резервні копії, наприклад, систем Windows, системі не потрібно кожного разу копіювати системні файли (наприклад, exe, dll), оскільки вони всюди однакові. Ще одна важлива функція VEEAM полягає в тому, що перед створенням резервної копії робиться знімок системи (англ. Snapshot). Це зводиться до того, що програмне забезпечення надсилає сигнал до дискового накопичувача, щоб зробити знімок системи. Завдяки цьому з цього знімка створюється резервна копія, яка містить узгоджені дані з одного моменту часу.

2.2.2 Стрічкова бібліотека

Стрічкові бібліотеки, які ще називаються стримерами, — це пристрої, які застосовуються для зберігання даних за допомогою магнітних носіїв (стрічок). Завдяки своїм властивостям вони найчастіше використовуються для архівації даних. До одних із сучасних, найпопулярніших та застосовуваних на сьогодні можна віднести носії LTO (Linear Tape-Open). Зокрема, останнє покоління LTO-9 має фізичну ємність 18 ТБ для однієї касети. До переваг цього рішення можна віднести можливість розширення за допомогою додаткових складових, стрічкових накопичувачів або об’єднання двох стрічкових бібліотек, які можуть працювати разом. Завдяки своїй масштабованості вони ідеально справляються там, де збільшення обсягу даних для обробки є більшим. Основною перевагою цього рішення є велика ємність, а недоліком – тривалий час запису та зчитування даних.

У нашій роботі вибрано та застосовано стрічкову бібліотеку DELL EMC ML3 (див. рисунок 2.6). Цей продукт підтримує медіа LTO, починаючи від версії LTO-6, що забезпечує широкий вибір медіа. У цій стрічковій бібліотеці також

передбачено можливість дистанційного керування через мережу та рідкокристалічну (LCD) панель керування оператора.

Рисунок 22.6 – Зовнішній вигляд стрічкової бібліотеки DELL EMC ML3 [сайт "Dell.com"]

РОЗДІЛ 3 КОНФІГУРАЦІЯ ПРИСТРОЇВ І СЕРВЕРІВ

3.1 Схема під’єднання серверів і дискового накопичувача до мережі LAN

Одним із елементів комп’ютерної системи є під’єднання всіх її пристроїв (обчислювальні вузли, сховища даних, мережеві переспрямовувачі, мережеві маршрутизатори та інші подібні пристрої) до локальної мережі [1, 2]. На рисунку 3.1 показано під’єднання фізичних серверів ESX (англ. Elastic Sky X), сервера резервного копіювання та дискового накопичувача до комутаторів локальної мережі.

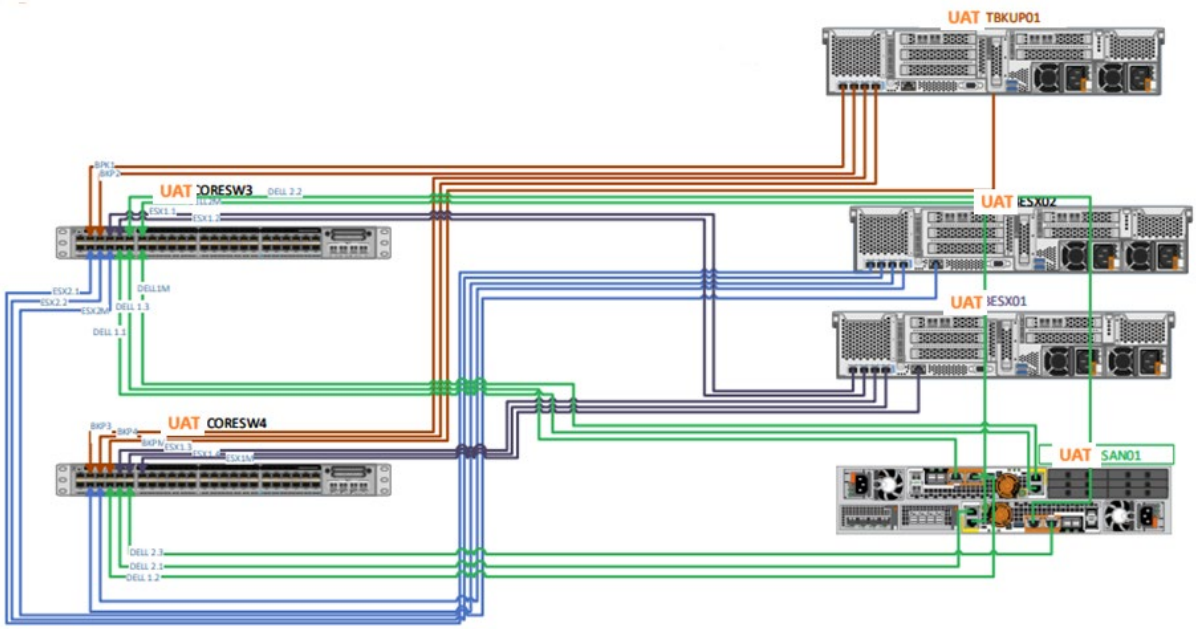


Рисунок 3.1 – Схема мережі LAN

Кожен сервер під’єднано чотирма портами 1 Гбіт/с. Це забезпечує резервування, так що для випадку збою порту в комутаторі або сервері буде забезпечена безперервна робота цих пристроїв. У той же час, для відповідної конфігурації комутаторів, два канали зв'язку між сервером і комутатором можуть застосовуватися для розподілу трафіку між ними, використовуючи алгоритми балансування навантаження.

3.2 Конфігурація маршрутизатора

Прикладом маршрутизатора, який застосовано у нашій роботі, є TP-Link з бізнес-серії (TL-ER5120). Маршрутизатор – це пристрій, який дозволяє з'єднувати дві різні мережі. На нижченаведених рисунках показано найважливіші етапи конфігурації маршрутизатора.

Зокрема, на рисунку 3.2 показано режим WAN. Вибирається, на якому з доступних портів повинна бути активна WAN. Цей маршрутизатор дає змогу здійснити конфігурацію 2 портів WAN одночасно, завдяки чому можна використовувати два Інтернет-провайдери без необхідності придбання іншого пристрою. Це рішення застосовується у великих організаціях, яким потрібне стабільне під'єднання до Інтернету. Це обумовлено тим, що для активних двох WAN-портів (два Інтернет-провайдери) під час збою одного з провайдерів все ще є доступ до мережі, який надається іншим з них.

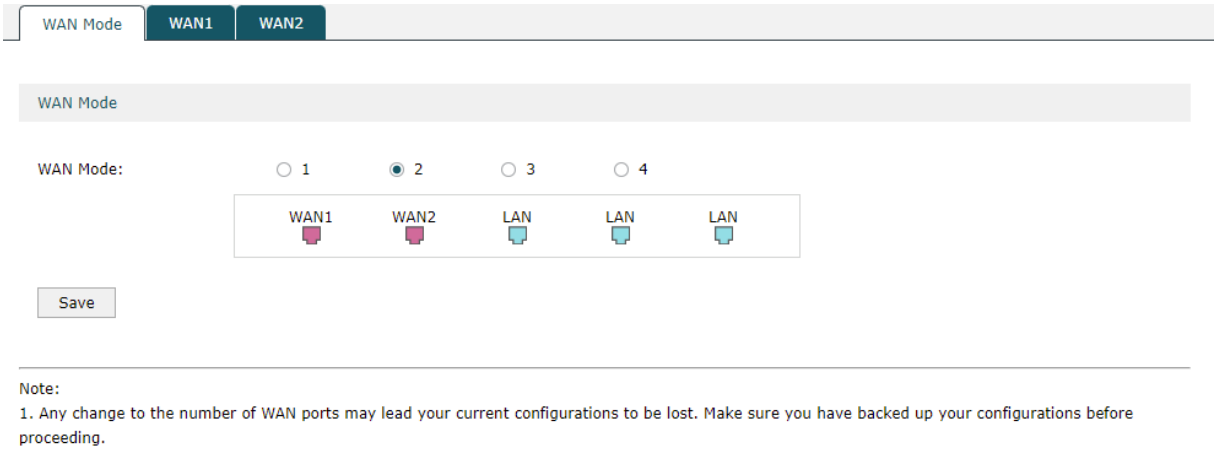


Рисунок 3.2 – Конфігурація порту WAN маршрутизатора
[Емулятор із сайту https://www.tp-link.com/]

Наступним кроком буде встановлення IP-адреси маршрутизатора (див. рисунок 3.3). Тут встановлено, наприклад, 192.168.0.1. Слід пам'ятати, що ця адреса також стає шлюзом мережі за умовчанням. Сервер DHCP не буде встановлено на маршрутизаторі, оскільки його буде здійснено конфігурацію на сервері.

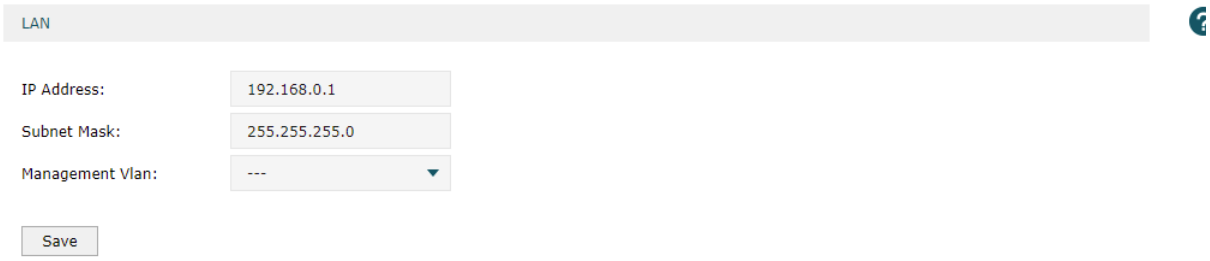


Рисунок 3.3 – Конфігурація порту LAN

Джерело: [Емулятор з сайту https://www.tp-link.com/]

В конфігураціях брандмауера нас цікавить лише вкладка „IP-MAC Binding” (англ. «Прив’язка IP-MAC»), де активовано всі з опцій (див. рисунок 3.4). Цим самим захищається Ethernet від мережевих атак, які дозволяють перехоплювати дані в сегменті локальної мережі.

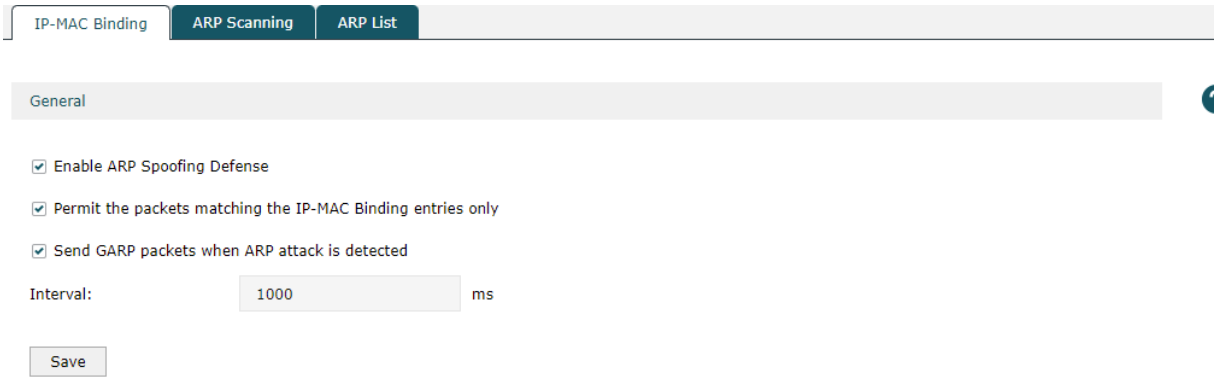


Рисунок 3.4 – Конфігурація брандмауера

[Емулятор з сайту https://www.tp-link.com/]

3.3 Апаратна конфігурація хоста

Для проєкту було сконфігуровано два сервери компанії Lenovo. Апаратні параметри обох серверів ESX були підібрані таким чином, щоб забезпечити 50% перевищення обчислювальної потужності центрального процесора та ємності оперативної пам'яті. Слід зазначити, що гіпервізор ESX дає змогу розділити

ресурси фізичного комп'ютера на логічні компоненти, звані віртуальними машинами. Містить засоби керування віртуальними машинами та ресурсами. Загалом гіпервізор представляє собою програмне забезпечення, яке призначене для розгортання віртуальних середовищ і дає змогу здійснювати запуск декількох операційних систем на єдиному апаратному сервері. Завдяки цьому можна осягнути оптимізації ресурсів, покращити захищеність інформації, надійність функціонування IT-інфраструктури та її здатність до масштабування [14].

З іншої сторони, гіпервізор можна уявити також процесом, який відокремлює опереаційну систему та додатки комп’ютера від апаратного обладнання [7,8]. Завдяки цьому, для випадку збою одного з хостів або ремонтних робіт на одному з хостів, усі віртуальні сервери можуть працювати на одній машині. На нижченаведених рисунках нижче показано детальну конфігурацію кожного сервера ESX, оскільки обидві машини ідентичні.

Кожен хост повинен мати принаймні 2 процесори з 8 ядрами кожен. У цьому випадку можна використовувати процесори, наприклад Inter(R) Xeon(R) 4110 з тактовою частотою 2,10 ГГц кожен, як показано на рисунку 3.5.

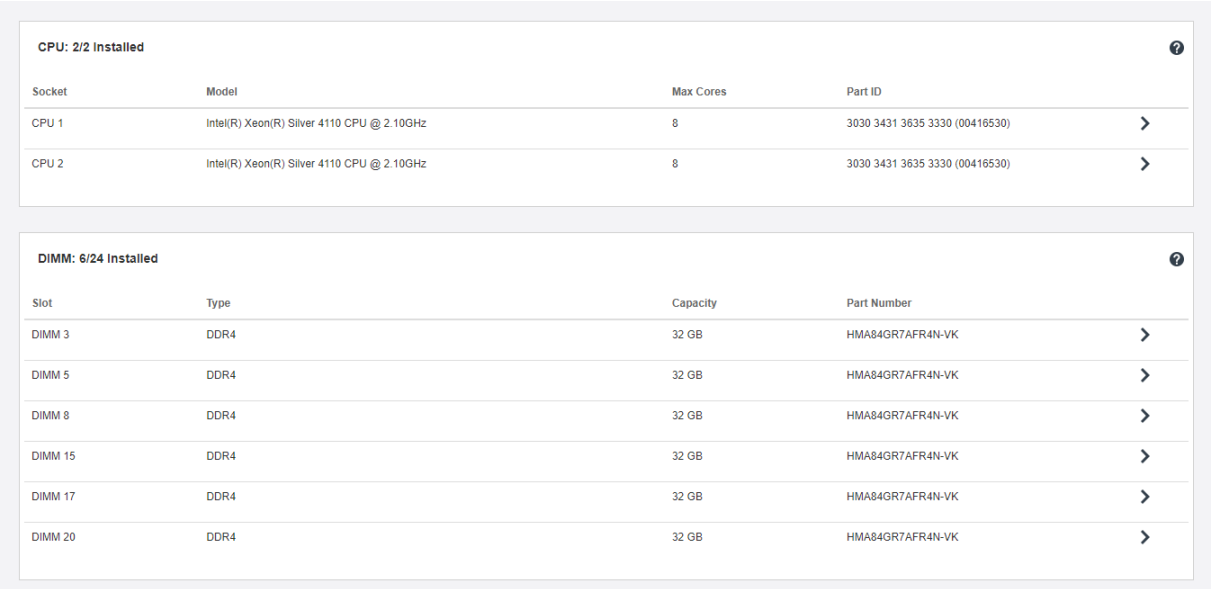


Рисунок 3.5 – Процесори та оперативна пам'ять на сервері

Кожен сервер містить 192 ГБ оперативної пам'яті в 6 складових 32 ГБ кожна.

На кожному сервері повинні бути встановлені диски (див. рисунок 3.6), на які буде встановлена система супервізора VMware. Проєкт передбачає встановлення двох SSD накопичувачів ємністю по 32 ГБ кожен.

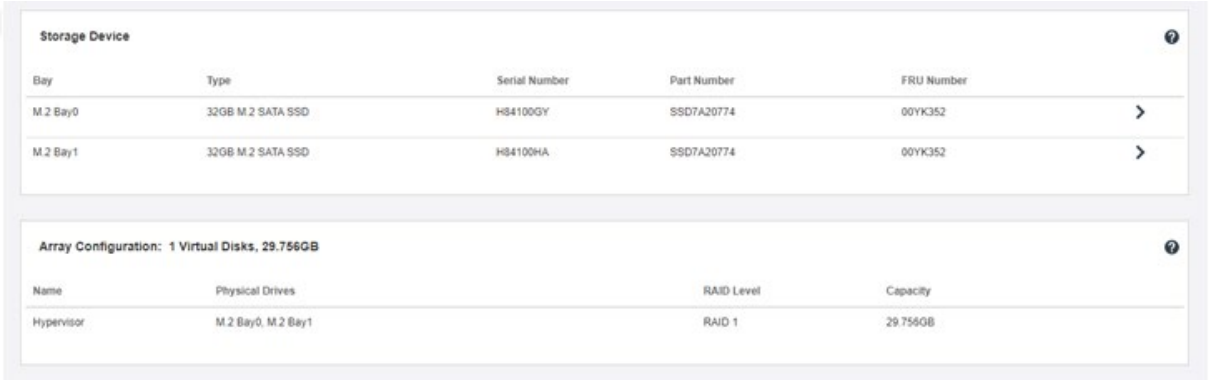


Рисунок 3.6 – Серверні накопичувачі SSD

Обидва диски з'єднані в дисковий масив RAID 1, також відому як mirroring, завдяки чому, навіть якщо один з дисків буде пошкоджено, сервер продовжить працювати.

Для живлення серверів слід використовувати принаймні два джерела живлення, щоб забезпечити резервування живлення (див. рисунок 3.7). Завдяки цьому, під час виходу з ладу одного з них, сервер все одно функціонуватиме.

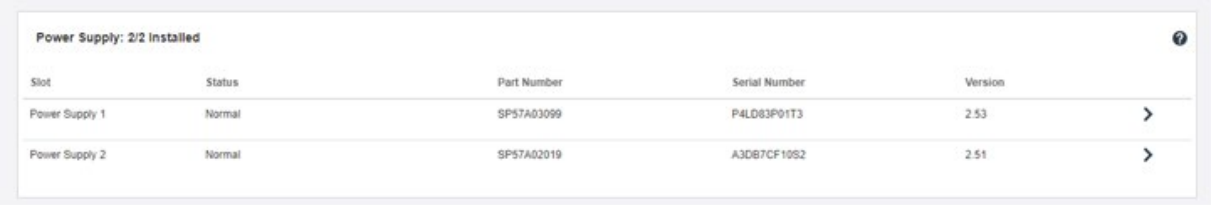
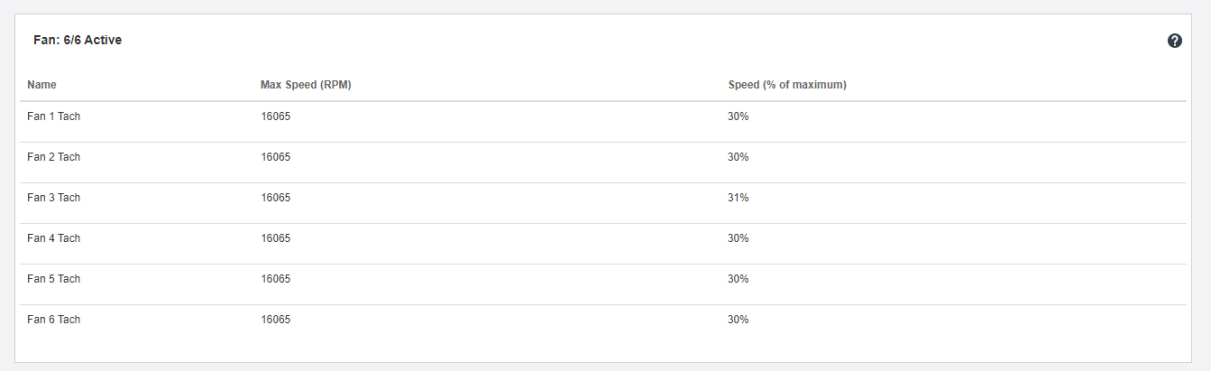


Рисунок 3.7 – Блоки живлення, що використовуються для сервера

На серверах повинно бути встановлено не менше 6 вентиляторів, по два з яких змонтовано на кожному процесорі та по чотири внутрі сервера, що забезпечує відведення тепла, яке природним чином виділяється електричними пристроями під час роботи (див. рисунок 3.8). Для належного охолодження цілодобово діючих серверів у серверній також встановлено два кондиціонери, які працюватимуть безперервно.

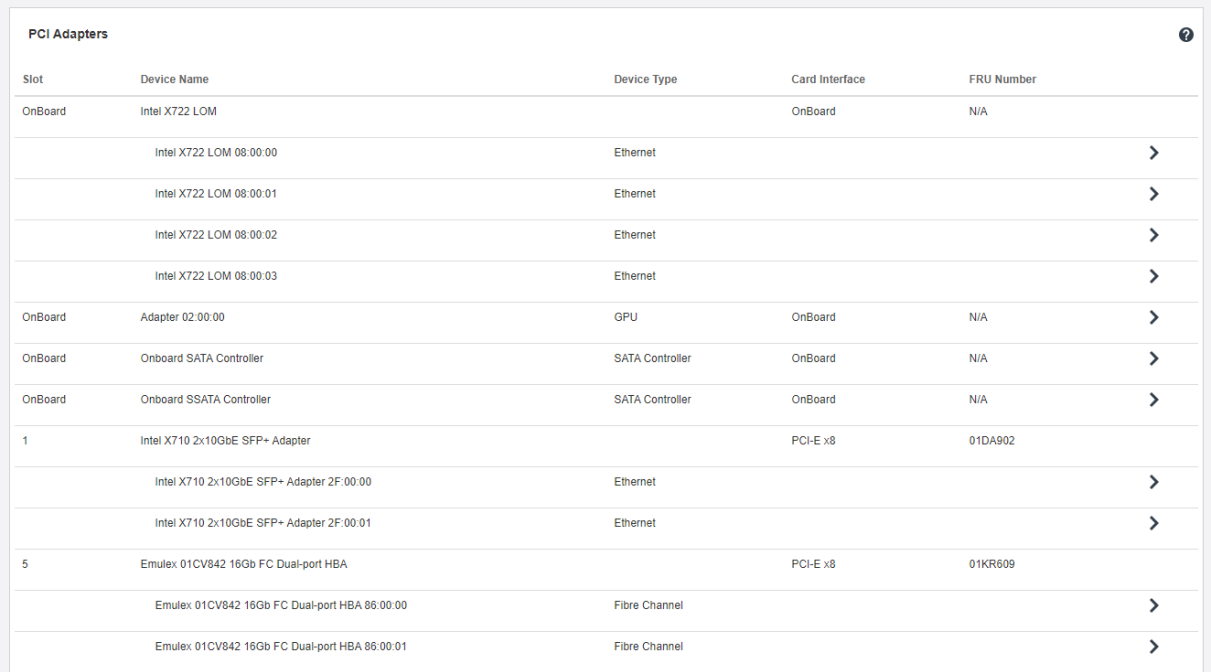


Fan: 6/6 Active

Name	Max Speed (RPM)	Speed (% of maximum)
Fan 1 Tach	16065	30%
Fan 2 Tach	16065	30%
Fan 3 Tach	16065	31%
Fan 4 Tach	16065	30%
Fan 5 Tach	16065	30%
Fan 6 Tach	16065	30%

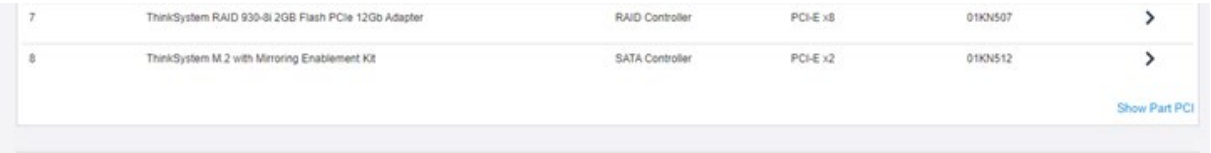
Рисунок 3.8 – Охолодження серверів

Кожна машина ESX повинна містити 4 карти Ethernet, які дозволять під’єднати сервер до двох портів Ethernet на кожному комутаторі. Сервер також містить дві карти Ethernet 10 ГБ/с і 2 карти FC, які в нашому випадку будуть використовуватися для під’єднання серверів до накопичувача в мережі SAN (див. рисунок 3.9). Крім того, сервер повинен містити контролер RAID, який забезпечує можливість конфігурація дисковий накопичувачу RAID1 на внутрішніх дисках сервера.



PCI Adapters

Slot	Device Name	Device Type	Card Interface	FRU Number
OnBoard	Intel X722 LOM		OnBoard	N/A
	Intel X722 LOM 08:00:00	Ethernet		
	Intel X722 LOM 08:00:01	Ethernet		
	Intel X722 LOM 08:00:02	Ethernet		
	Intel X722 LOM 08:00:03	Ethernet		
OnBoard	Adapter 02:00:00	GPU	OnBoard	N/A
OnBoard	Onboard SATA Controller	SATA Controller	OnBoard	N/A
OnBoard	Onboard SSATA Controller	SATA Controller	OnBoard	N/A
1	Intel X710 2x10GbE SFP+ Adapter		PCI-E x8	01DA902
	Intel X710 2x10GbE SFP+ Adapter 2F:00:00	Ethernet		
	Intel X710 2x10GbE SFP+ Adapter 2F:00:01	Ethernet		
5	Emulex 01CV842 16Gb FC Dual-port HBA		PCI-E x8	01KR609
	Emulex 01CV842 16Gb FC Dual-port HBA 86:00:00	Fibre Channel		
	Emulex 01CV842 16Gb FC Dual-port HBA 86:00:01	Fibre Channel		



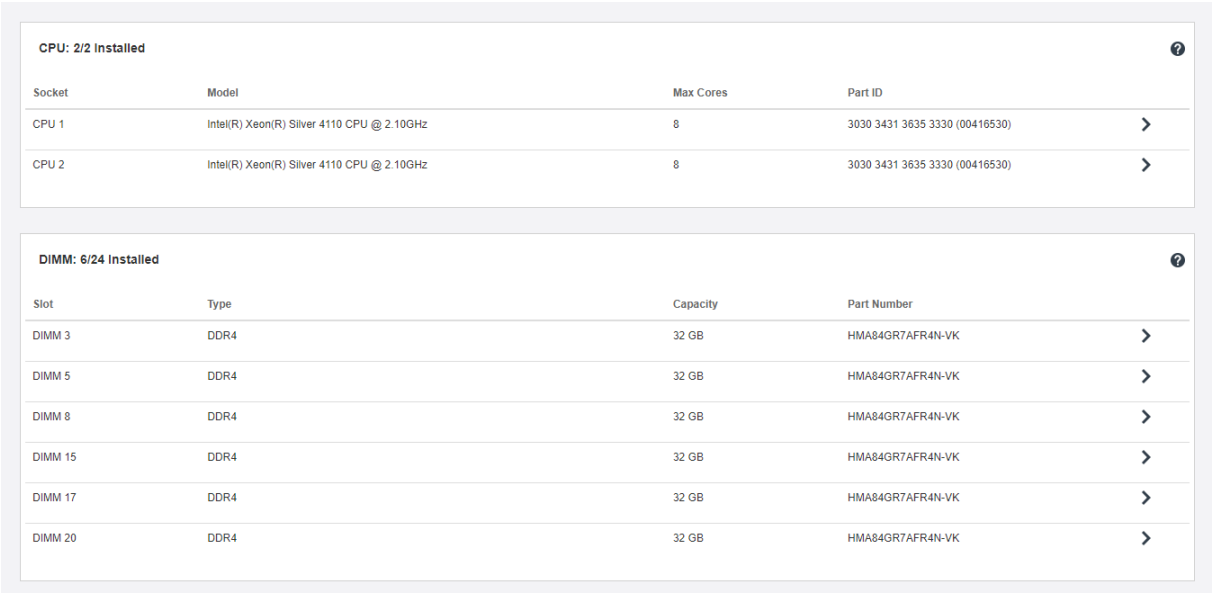
7	ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	RAID Controller	PCI-E x8	01KN507	>
8	ThinkSystem M.2 with Mirroring Enablement Kit	SATA Controller	PCI-E x2	01KN512	>

Show Part PCI

Рисунок 3.9 – Мережеві карти на сервері

3.4 Конфігурація резервного сервера

Третій фізичний сервер має бути сервером, який виконуватиме роль резервного сервера. Програмне забезпечення для резервного копіювання повинно працювати в операційній системі (Windows або Linux), яке буде встановлено на фізичному сервері, оскільки воно виконуватиме резервне копіювання віртуального середовища та, отже, не може бути віртуальною машиною. Крім цього, сервер резервного копіювання під’єднано безпосередньо до стрічкової бібліотеки через окреме з’єднання в мережі SAN (див. рисунок 3.10).



CPU: 2/2 Installed

Socket	Model	Max Cores	Part ID	
CPU 1	Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz	8	3030 3431 3635 3330 (00416530)	>
CPU 2	Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz	8	3030 3431 3635 3330 (00416530)	>

DIMM: 6/24 Installed

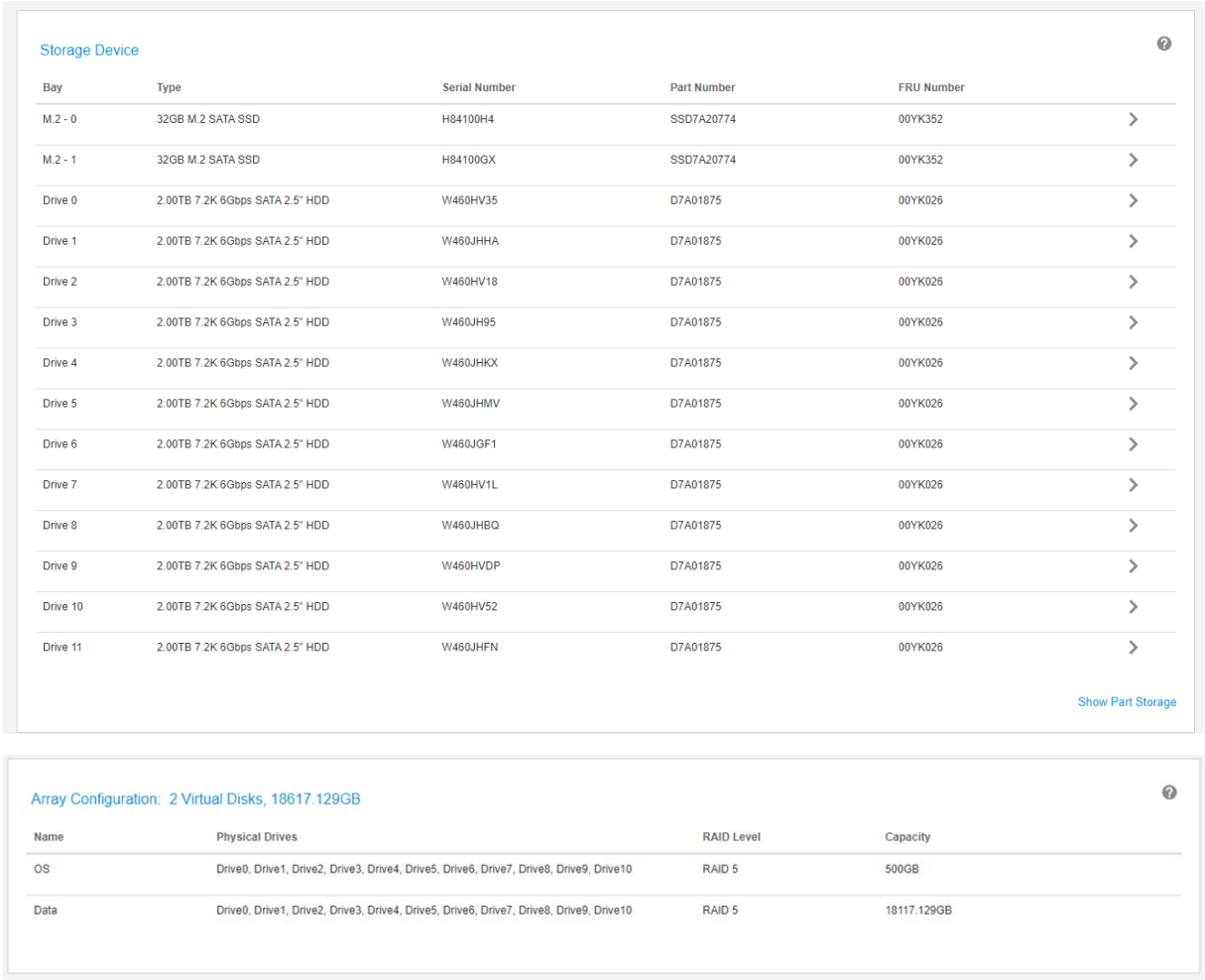
Slot	Type	Capacity	Part Number	
DIMM 3	DDR4	32 GB	HMA84GR7AFR4N-VK	>
DIMM 5	DDR4	32 GB	HMA84GR7AFR4N-VK	>
DIMM 8	DDR4	32 GB	HMA84GR7AFR4N-VK	>
DIMM 15	DDR4	32 GB	HMA84GR7AFR4N-VK	>
DIMM 17	DDR4	32 GB	HMA84GR7AFR4N-VK	>
DIMM 20	DDR4	32 GB	HMA84GR7AFR4N-VK	>

Рисунок 3.10 – Резервне копіювання та оперативна пам'ять RAM сервера Backup

Як згадувалося вище, процесори та оперативна пам’ять сервера такі ж, як і в сервері ESX. Це недарма, адже об'єднання серверів, що використовуються в одній серверній кімнаті, має свою мету. Це дає нам можливість замінити

компонент сервера між сервером резервного копіювання та сервером ESX. Прикладом може бути збій ЦП сервера ESX. У такій ситуації ми маємо можливість замінити один із процесорів резервного сервера на сервер ESX. Для резервного копіювання не потрібне таке потужне обладнання, тому до тих пір, поки процесор не відремонтують, він може легко працювати лише на одному з них. Така ж ситуація і з оперативною пам'яттю. Тому що, при проблемах з наявністю деталі, її можна використовувати і як запасний елемент.

Різниця між сервером ESX і сервером резервного копіювання полягає в дисках, як можна побачити на рисунку 3.10. Цей сервер має два диски SSD і 11 жорстких дисків, які в кінцевому підсумку утворюють дисковий масив RAID 5. На ньому було утворено два віртуальні диски: один ємністю 500 ГБ для операційної системи, а інші для даних, тобто резервних копій.



Storage Device

Bay	Type	Serial Number	Part Number	FRU Number
M.2 - 0	32GB M.2 SATA SSD	H84100H4	SSD7A20774	00YK352
M.2 - 1	32GB M.2 SATA SSD	H84100GX	SSD7A20774	00YK352
Drive 0	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV35	D7A01875	00YK026
Drive 1	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHHA	D7A01875	00YK026
Drive 2	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV18	D7A01875	00YK026
Drive 3	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JH95	D7A01875	00YK026
Drive 4	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHKX	D7A01875	00YK026
Drive 5	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHMV	D7A01875	00YK026
Drive 6	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JGF1	D7A01875	00YK026
Drive 7	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV1L	D7A01875	00YK026
Drive 8	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHBQ	D7A01875	00YK026
Drive 9	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HVDP	D7A01875	00YK026
Drive 10	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV52	D7A01875	00YK026
Drive 11	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHFN	D7A01875	00YK026

Show Part Storage

Array Configuration: 2 Virtual Disks, 18617.129GB

Name	Physical Drives	RAID Level	Capacity
OS	Drive0, Drive1, Drive2, Drive3, Drive4, Drive5, Drive6, Drive7, Drive8, Drive9, Drive10	RAID 5	500GB
Data	Drive0, Drive1, Drive2, Drive3, Drive4, Drive5, Drive6, Drive7, Drive8, Drive9, Drive10	RAID 5	18117.129GB

Рисунок 3.10 – Резервні серверні диски

Як і для випадку з серверами ESX, резервний сервер повинен мати два джерела живлення, які забезпечують резервування живлення у ситуації відмови одного з них (див. рис. 3.11).

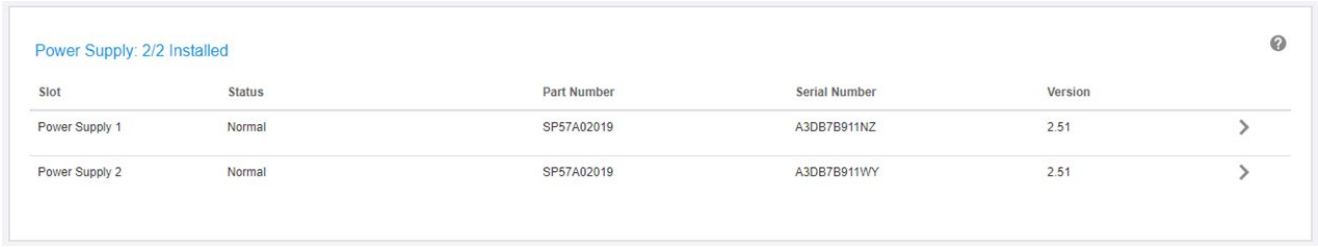


Рисунок 3.11 – Блоки живлення резервного сервера

Резервний сервер має 6 вентиляторів, у тому числі по одному на кожному процесорі та чотири, що забезпечують вільний потік повітря всередині машини (див. рис. 3.12).

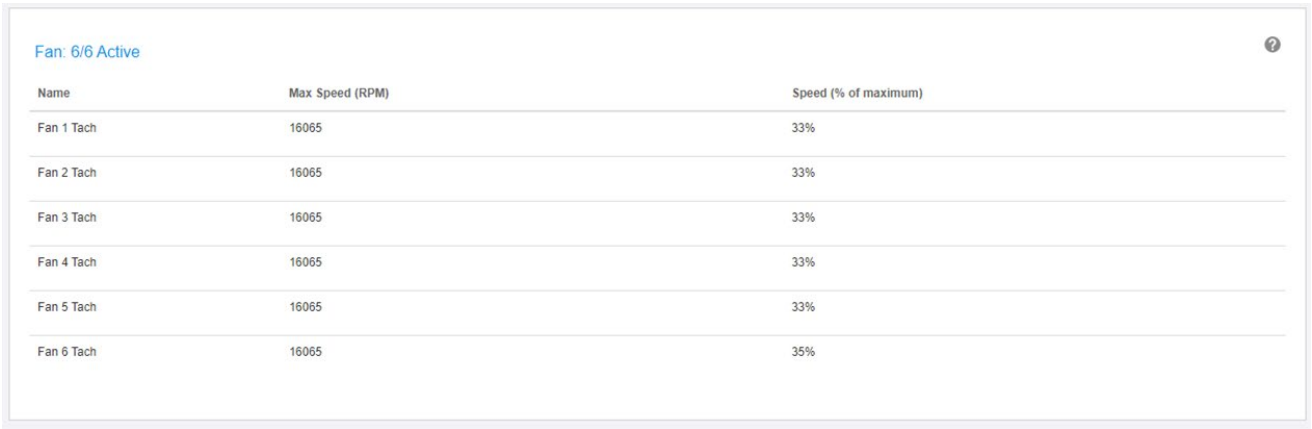
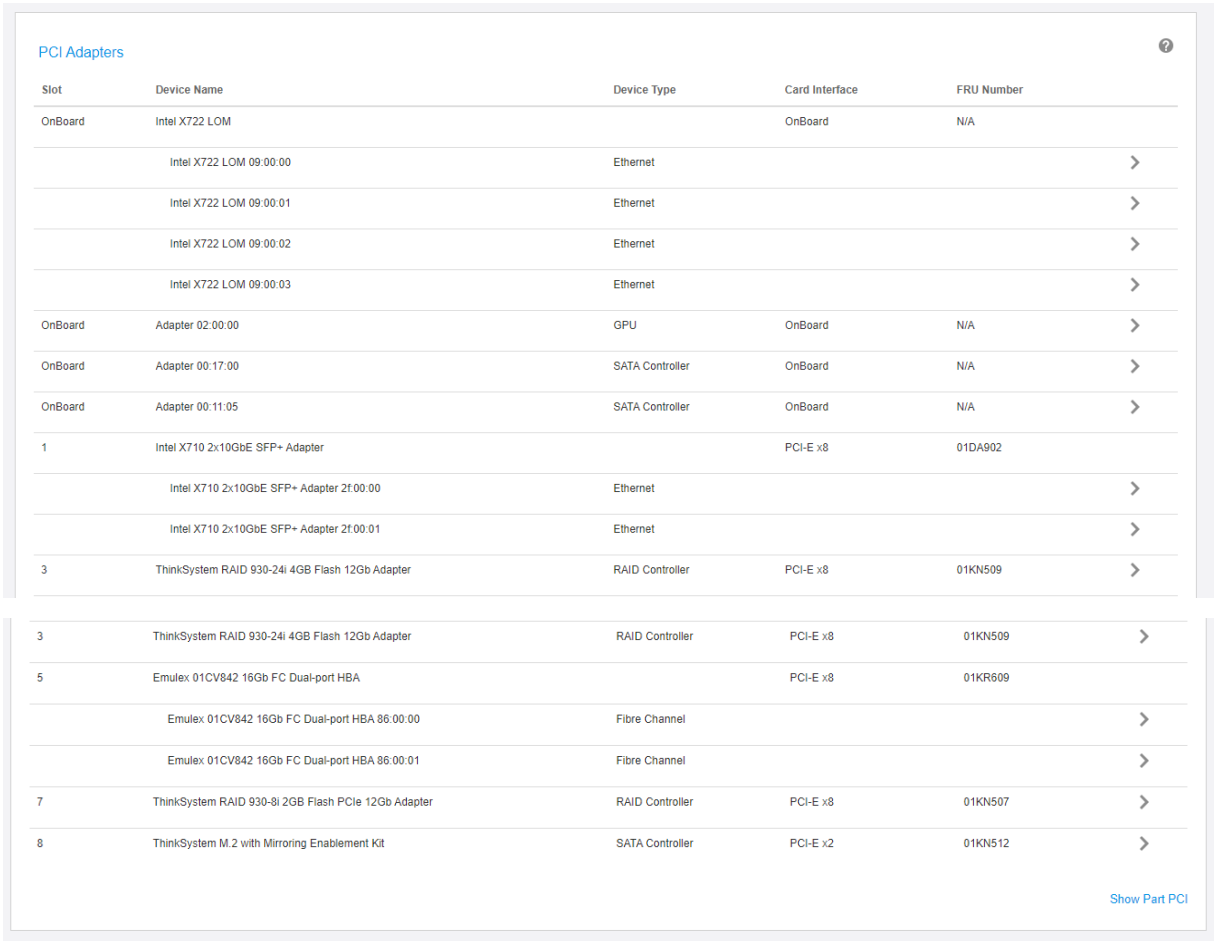


Рисунок 3.12 – Вентилятори резервного сервера

Резервний сервер, як і сервер ESX, має кілька портів Ethernet для під’єднання до комутаторів (див. рис. 3.13). Відмінність між сервером ESX і сервером резервного копіювання полягає в тому, що сервер резервного копіювання має контролери RAID, що відповідають за утворення дискового масиву RAID 5, відповідальної за резервне копіювання.



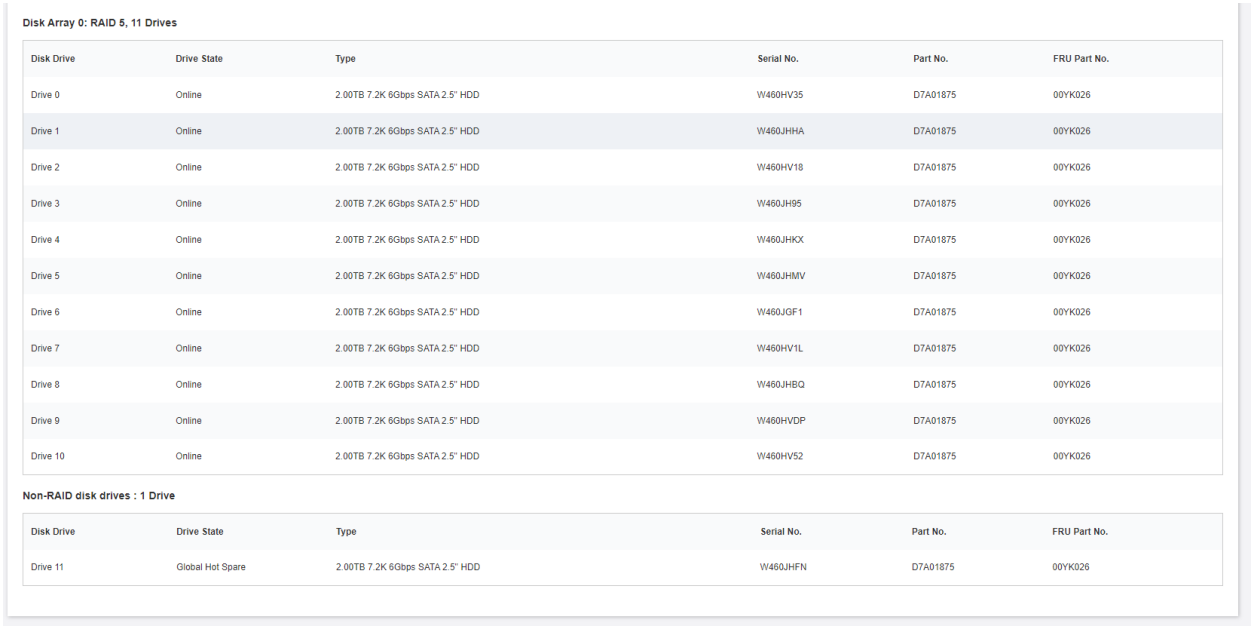
PCI Adapters

Slot	Device Name	Device Type	Card Interface	FRU Number
OnBoard	Intel X722 LOM		OnBoard	N/A
	Intel X722 LOM 09:00:00	Ethernet		
	Intel X722 LOM 09:00:01	Ethernet		
	Intel X722 LOM 09:00:02	Ethernet		
	Intel X722 LOM 09:00:03	Ethernet		
OnBoard	Adapter 02:00:00	GPU	OnBoard	N/A
OnBoard	Adapter 00:17:00	SATA Controller	OnBoard	N/A
OnBoard	Adapter 00:11:05	SATA Controller	OnBoard	N/A
1	Intel X710 2x10GbE SFP+ Adapter		PCI-E x8	01DA902
	Intel X710 2x10GbE SFP+ Adapter 2f:00:00	Ethernet		
	Intel X710 2x10GbE SFP+ Adapter 2f:00:01	Ethernet		
3	ThinkSystem RAID 930-24i 4GB Flash 12Gb Adapter	RAID Controller	PCI-E x8	01KN509
3	ThinkSystem RAID 930-24i 4GB Flash 12Gb Adapter	RAID Controller	PCI-E x8	01KN509
5	Emulex 01CV842 16Gb FC Dual-port HBA		PCI-E x8	01KR609
	Emulex 01CV842 16Gb FC Dual-port HBA 86:00:00	Fibre Channel		
	Emulex 01CV842 16Gb FC Dual-port HBA 86:00:01	Fibre Channel		
7	ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	RAID Controller	PCI-E x8	01KN507
8	ThinkSystem M.2 with Mirroring Enablement Kit	SATA Controller	PCI-E x2	01KN512

Show Part PCI

Рисунок 3.13 – Мережеві карти та адаптери

На рисунку 3.14 показано конфігурацію RAID 5 сервера резервного копіювання. Як бачимо, диски 0-10 утворюють дисковий накопичувач RAID 5, а диск 11 є диском гарячої заміни (з англ. Hot Spare). Диск Hot Spare працює таким чином, що не зберігає жодних даних, але якщо один із основних дисків дискового масиву RAID 5 виходить з ладу, програмне забезпечення контролера RAID виключає несправний диск, а диск Hot Spare автоматично під’єднується до дискового масиву в місце пошкодженого. Протягом цього часу дисковий масив перебудовується та завдяки цьому залишається повністю функціональною.



Disk Array 0: RAID 5, 11 Drives

Disk Drive	Drive State	Type	Serial No.	Part No.	FRU Part No.
Drive 0	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV35	D7A01875	00YK026
Drive 1	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHHA	D7A01875	00YK026
Drive 2	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV18	D7A01875	00YK026
Drive 3	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JH95	D7A01875	00YK026
Drive 4	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHKX	D7A01875	00YK026
Drive 5	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHMV	D7A01875	00YK026
Drive 6	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JGF1	D7A01875	00YK026
Drive 7	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV1L	D7A01875	00YK026
Drive 8	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHBQ	D7A01875	00YK026
Drive 9	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HVDP	D7A01875	00YK026
Drive 10	Online	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460HV52	D7A01875	00YK026

Non-RAID disk drives : 1 Drive

Disk Drive	Drive State	Type	Serial No.	Part No.	FRU Part No.
Drive 11	Global Hot Spare	2.00TB 7.2K 6Gbps SATA 2.5" HDD	W460JHFN	D7A01875	00YK026

Рисунок 3.14 – Конфігурація RAID

3.5 Конфігурація дискового накопичувача

У проекті пристроєм, відповідальним за зберігання даних у віртуальному середовищі, є дисковий масив типу Dell Unity 300. Цей дисковий масив повинен містити 23 диски, які будуть працювати в режимі RAID 5 (див. рис. 3.15).

Диски в дисковий накопичувачі можна об’єднати в пул (див. рис. 3.15). Все сховище накопичувача можна розділити на кілька пулів. У нашому випадку достатньо лише одного (POOL01).

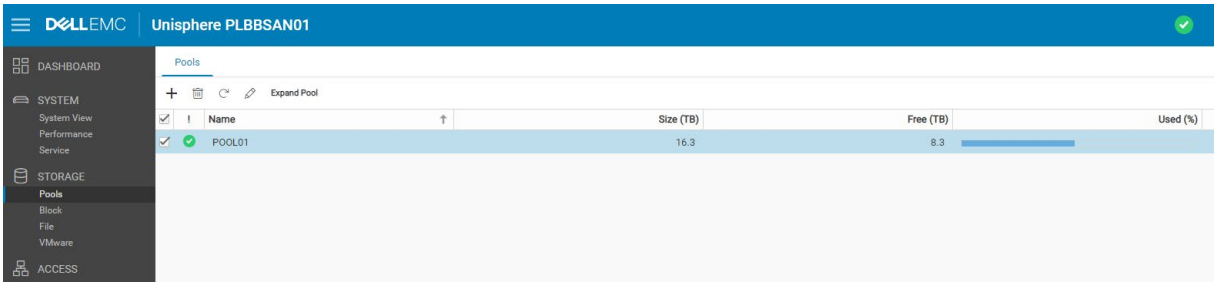
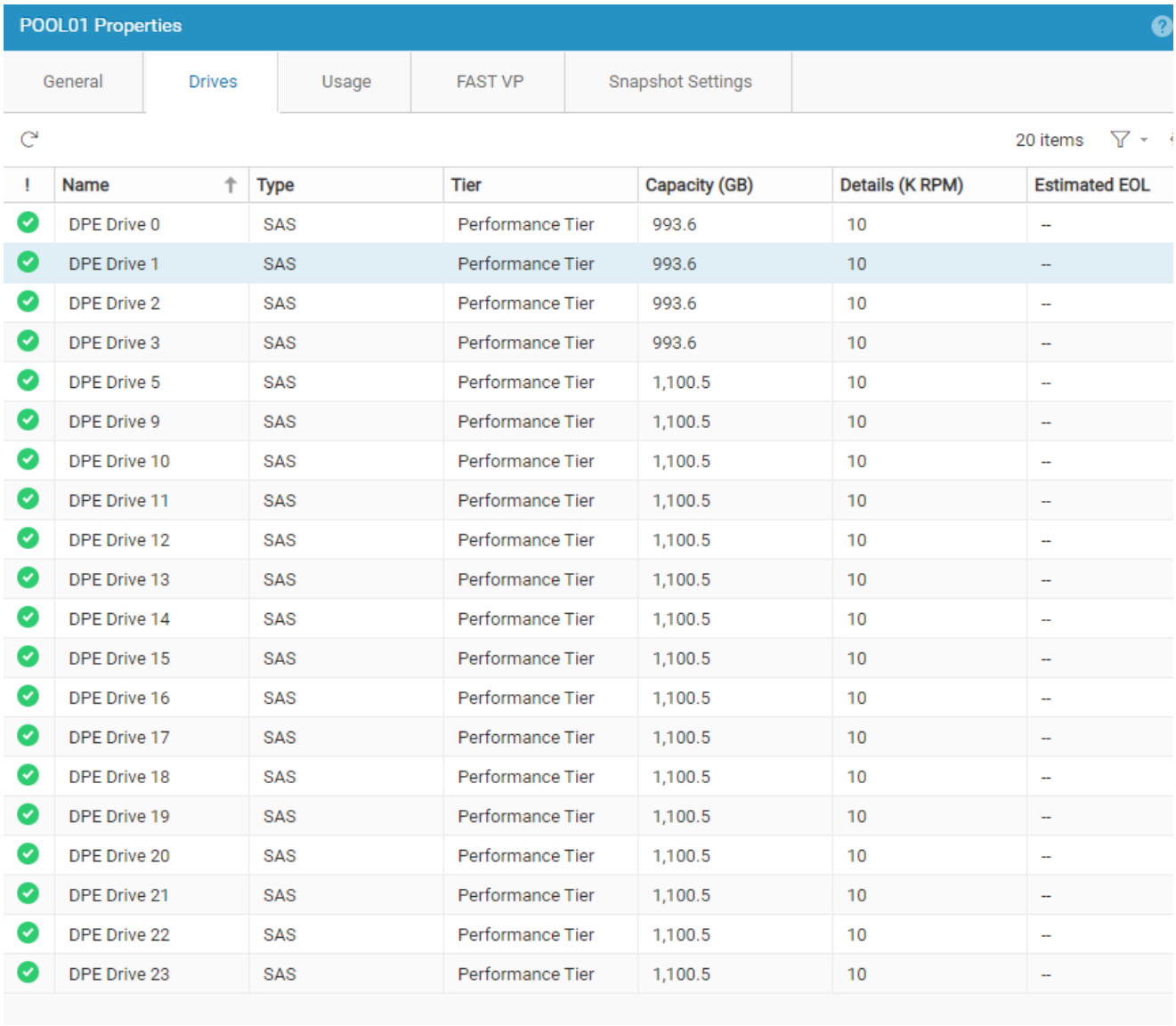


Рисунок 3.15 – Пули дискового масиву

Як вказано на рисунку 3.16, використано 23 диски типу SAS. Всі вони працюють зі швидкістю 10 000 обертів, що забезпечує адекватну ефективність такого зберігання.



!	Name	Type	Tier	Capacity (GB)	Details (K RPM)	Estimated EOL
✓	DPE Drive 0	SAS	Performance Tier	993.6	10	--
✓	DPE Drive 1	SAS	Performance Tier	993.6	10	--
✓	DPE Drive 2	SAS	Performance Tier	993.6	10	--
✓	DPE Drive 3	SAS	Performance Tier	993.6	10	--
✓	DPE Drive 5	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 9	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 10	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 11	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 12	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 13	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 14	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 15	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 16	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 17	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 18	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 19	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 20	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 21	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 22	SAS	Performance Tier	1,100.5	10	--
✓	DPE Drive 23	SAS	Performance Tier	1,100.5	10	--

Рисунок 3.16 – Всі використані приводи

Дисковий пул був внутрішньо розділений на 4 розділи (англ. disk partition) (див. рисунок 3.17). Завдяки цьому кожен з них – це фізично розділені області диска. Перші два розділи створено для VMware Data storage. Наступні два призначені для сервера NAS. Слід також пам'ятати про те, щоб залишити в резерві близько 20 відсотків невикористаного дискового простору. Завдяки цьому його можна за необхідності швидко збільшити.

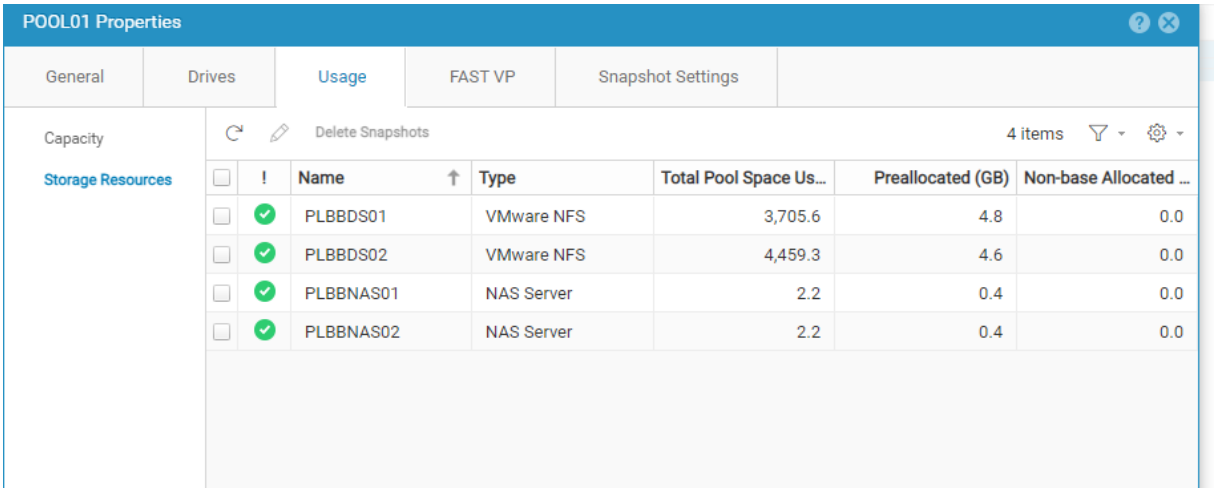


Рисунок 3.17 – Вміст дискового масиву

Ще один важливий параметр — це параметри знімка (англ. snapshot). Вибраний елемент призводить до того, що коли диск заповнюється на 95%, дисковий накопичувач починає автоматично видаляти невикористані знімки, щоб вивільнити дискові ресурси (див. рисунок 3.18).

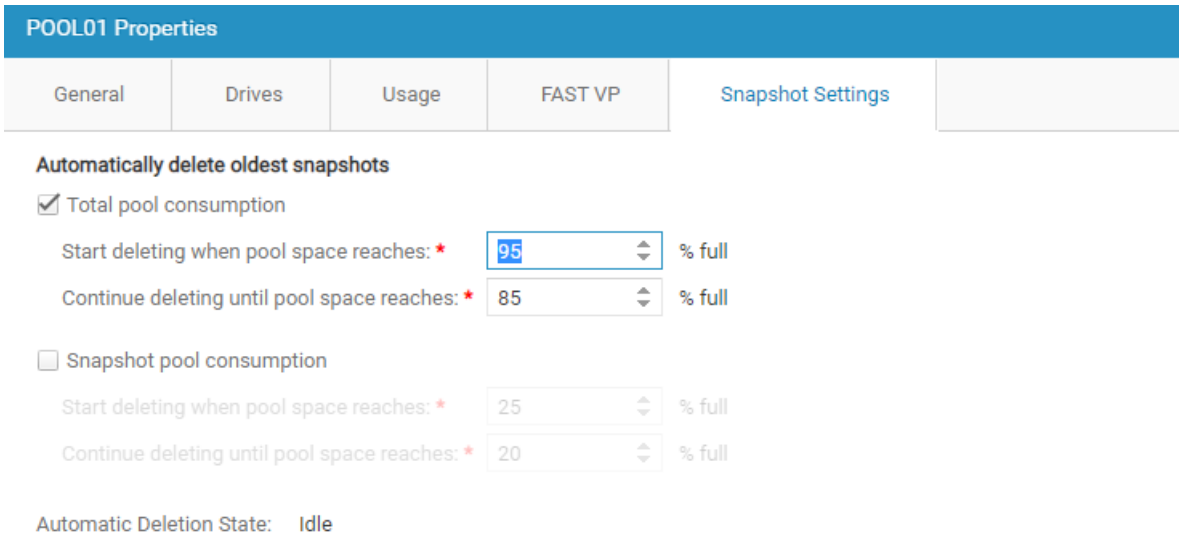


Рисунок 3.18 – Конфігурація знімка

Як випливає з рисунка 3.19, весь DS01 має 8 ТБ дискового простору, тоді як для використання заявлено лише 3,6 ТБ. Це дозволяє адміністратору в будь-який момент додати додатковий простір і водночас запобігає переповненню диска.

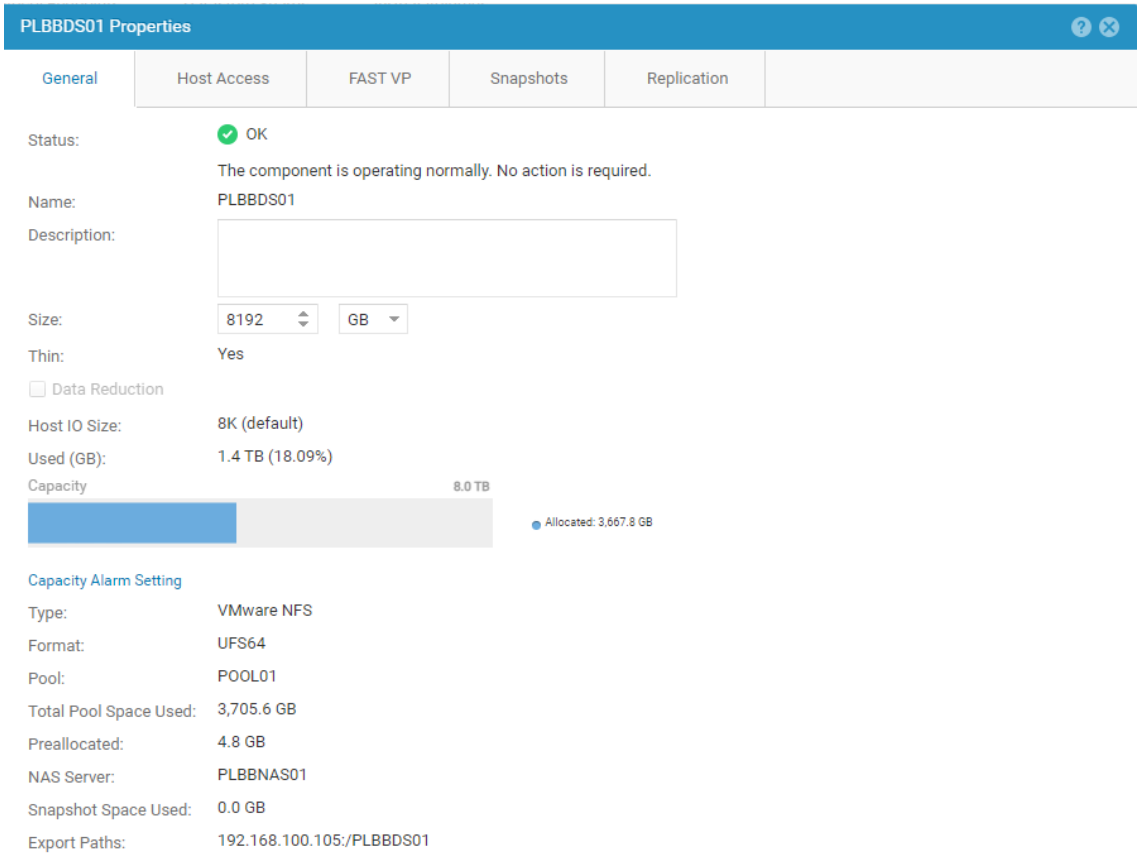


Рисунок 3.19 – Конфігурація Data Storage 01

На вкладці «Доступ до хосту» (Host Access) здійснюється конфігурація, які сервери мають доступ до сховища даних і можуть ним користуватися. У нашому випадку це два сервери ESX (див. рисунок 3.20).

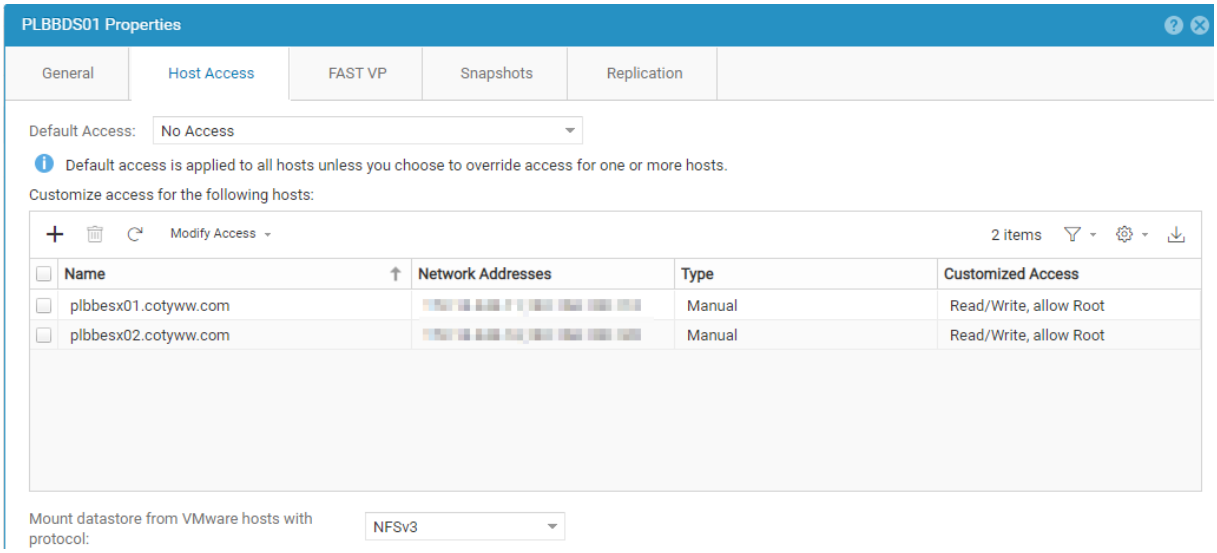


Рисунок 3.20 – Доступ до хоста (Host access)

На вкладці Datastore Shares можна перевірити, до яких сховищ даних було надано спільний доступ і за яким шляхом (див. рисунок 3.21).

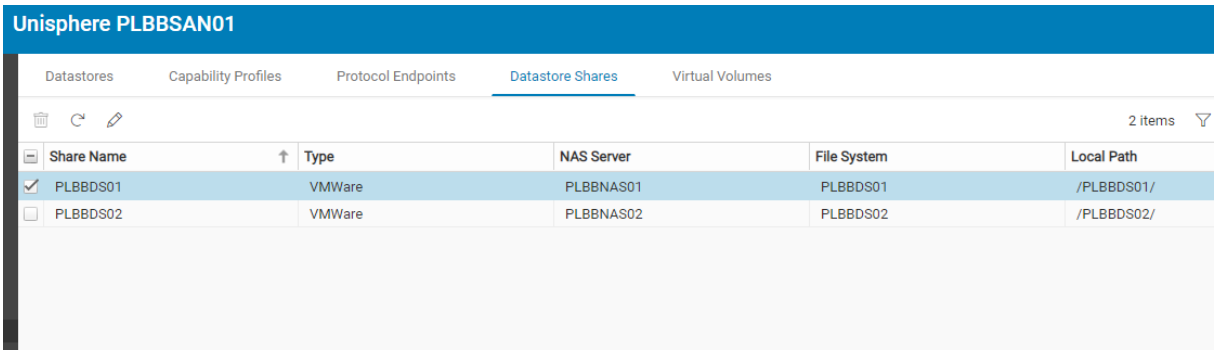


Рисунок 3.21 – Вкладка Datastore Shares

3.6 Конфігурація віртуальної машини контролера домену

3.6.1 Апаратна конфігурація віртуальної машини

У віртуальному середовищі здійснено конфігурацію контролер домену AD (Active Directory). На рисунку 3.22 показано виділені для нього ресурси диска, оперативної пам’яті RAM та центрального процесора CPU. Цих апаратних параметрів цілком достатньо для коректної роботи контролера домену.

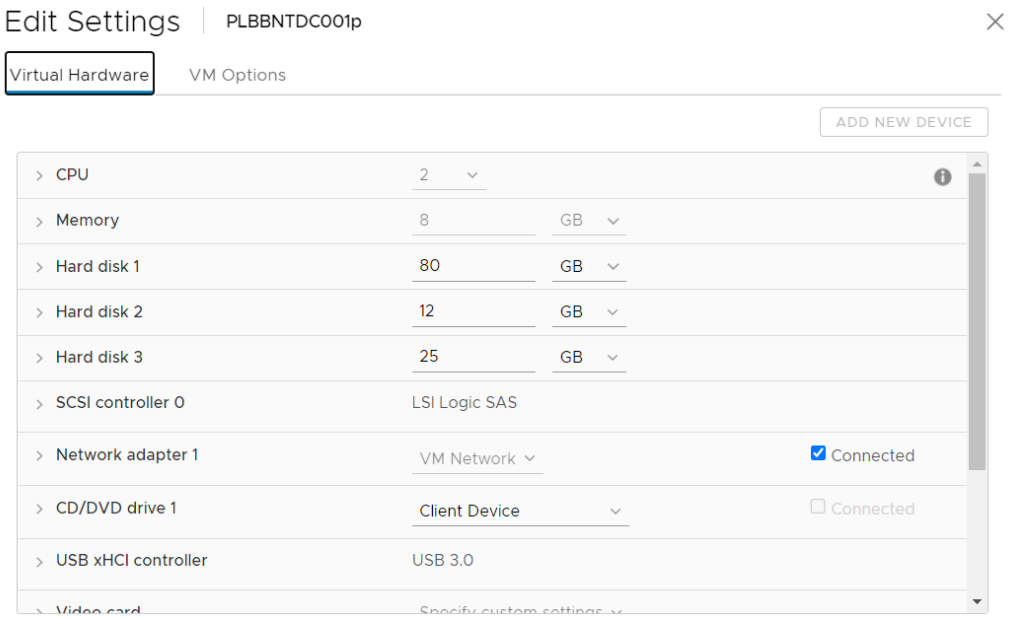


Рисунок 3.22 – Приділені параметри для контролера домену

Джерело: Власне дослідження

3.6.2 Конфігурація активного каталогу

Інтелектуальна служба каталогів Active Directory була сконфігурована у віртуальному середовищі, в якому на одній із машин було встановлено Windows Server. Контролер домену дозволяє користувачам створювати облікові записи домену, які вони використовуватимуть під час роботи в організації. Таке рішення полегшує організацію роботи всієї організації, оскільки співробітник IT-відділу має повне уявлення про те, скільки людей на даний момент мають облікові записи. Можна легко додати або видалити такі облікові записи. На рисунку 3.23 показано приклад сконфігурованого контролера домену Active Directory.

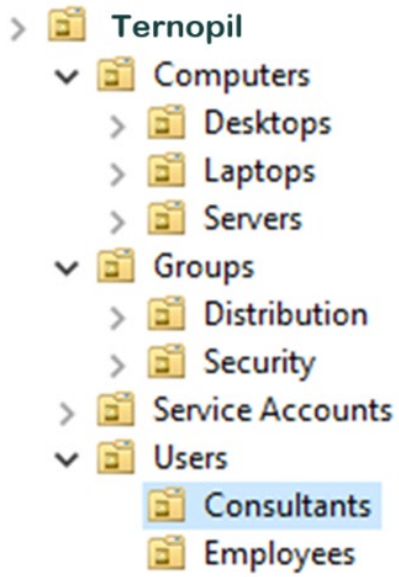


Рисунок 3.23 – Приклад сконфігурованого контролера домену

3.7 Конфігурація DHCP

3.7.1 Апаратна конфігурація послуги DHCP

Для сервера DHCP передбачено 2 ядра віртуального процесора, 8 ГБ оперативної пам’яті RAM та два диски (один на 12 ГБ, а другий на 120 ГБ). Цих параметрів цілком достатньо для коректної роботи DHCP-сервера на машині [15].

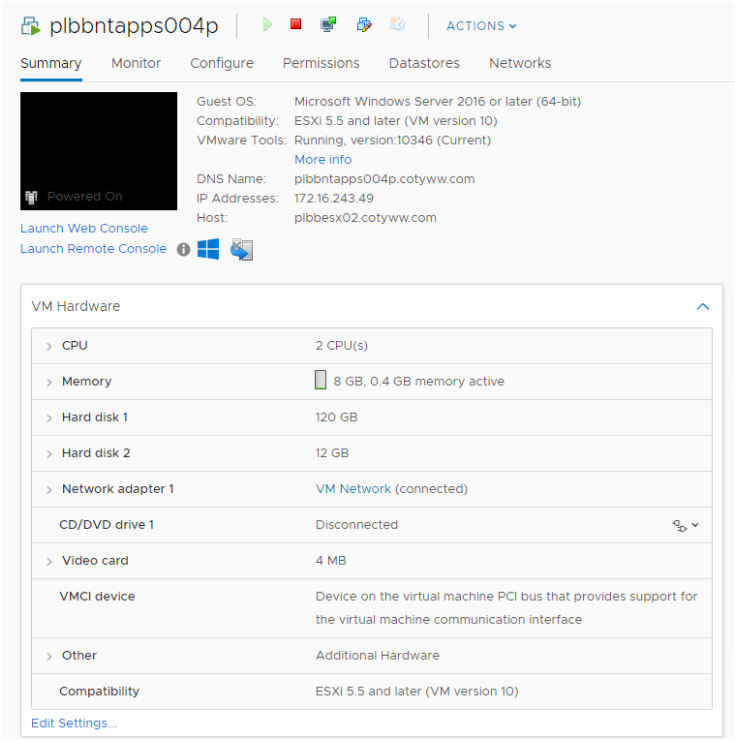


Рисунок 3.24 – Апаратна конфігурація DHCP-сервера.

3.7.2 Загальна конфігурація послуги DHCP

Послуга DHCP відповідає за автоматичне призначення IP-адрес клієнтським пристроям. Звичайно, можна зарезервувати адресу на вибраних пристроях, щоб вони завжди мали ту саму IP-адресу [15].

На рисунку 3.25 показано приклад IP-адрес, приділених пристроям. Як бачимо, більшість цих адрес було призначено автоматично, тоді як, наприклад, адреса 172.16.242.17 була зарезервована для одного конкретного пристрою. Усі приділені IP-адреси повинні належати до одного класу адрес.

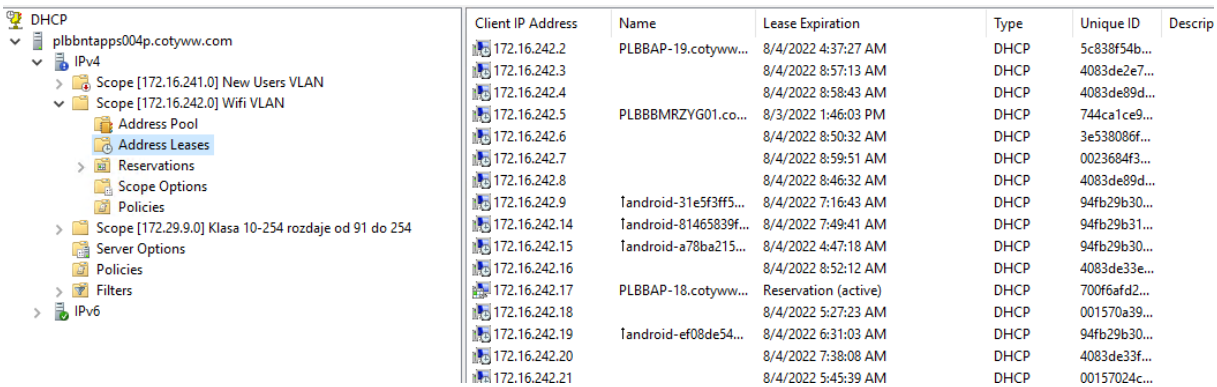


Рисунок 3.25 – Приклад адресування пристроїв

На рисунку 3.26 показано пули адрес, які можуть бути призначені сервером DHCP. Як бачимо, адреси, які наведені під першою адресою, виключено, і сервер не може автоматично призначити їх жодному пристрою в мережі.

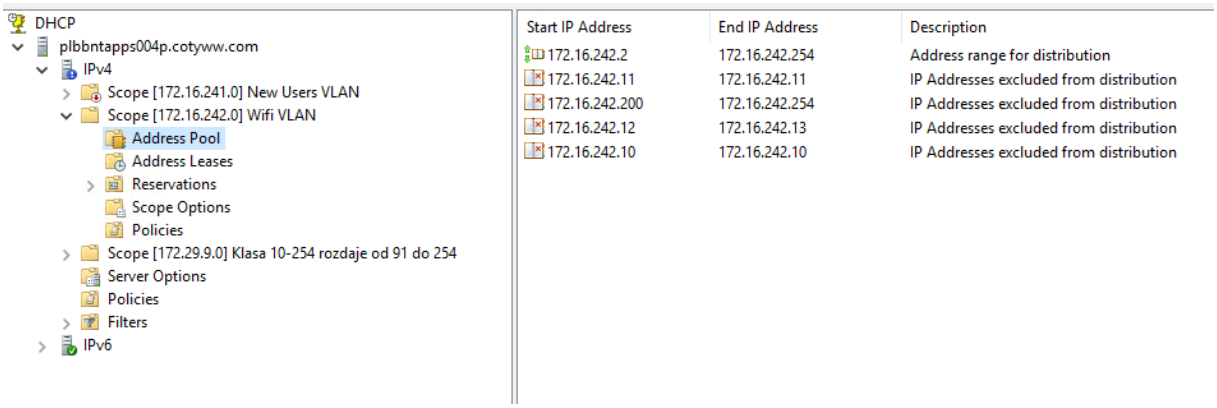


Рисунок 3.26 – Приклад №1 пулів адрес

На рисунку 3.27 також показано пули адрес, які можна приділити, але вони належать до іншої підмережі. Тут сервер призначає лише адреси з 172.29.9.10-172.29.9.254, оскільки інші адреси виключено (зарезервовано) та їх можна приділити лише вручну.

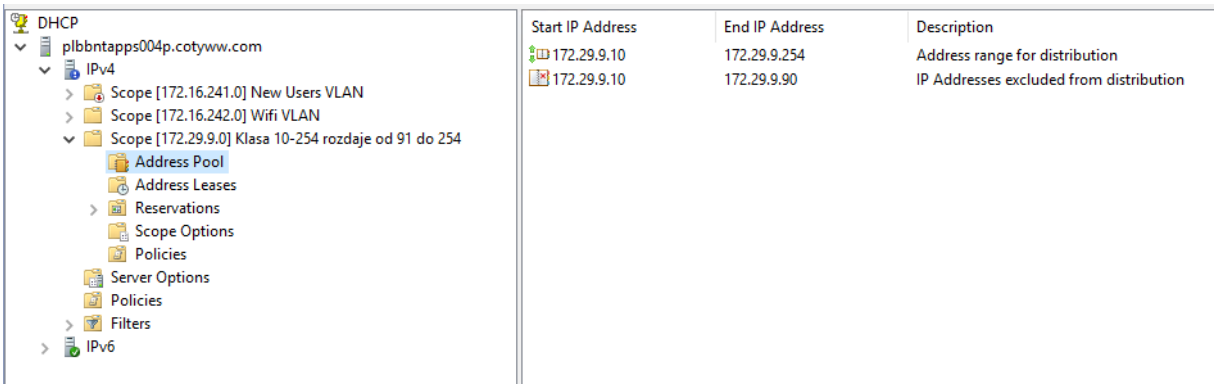


Рисунок 3.27 – Приклад №2 пулів адрес

3.8 Конфігурація файлового сервера

3.8.1 Апаратна конфігурація файлового сервера

На відміну від контролера домену, для файлового сервера потрібно набагато більше місця на жорсткому диску. Він застосовується, як випливає з назви, для зберігання та обміну файлами користувачами. На рисунку 3.28 показано апаратну конфігурацію файлового сервера у віртуальному середовищі:

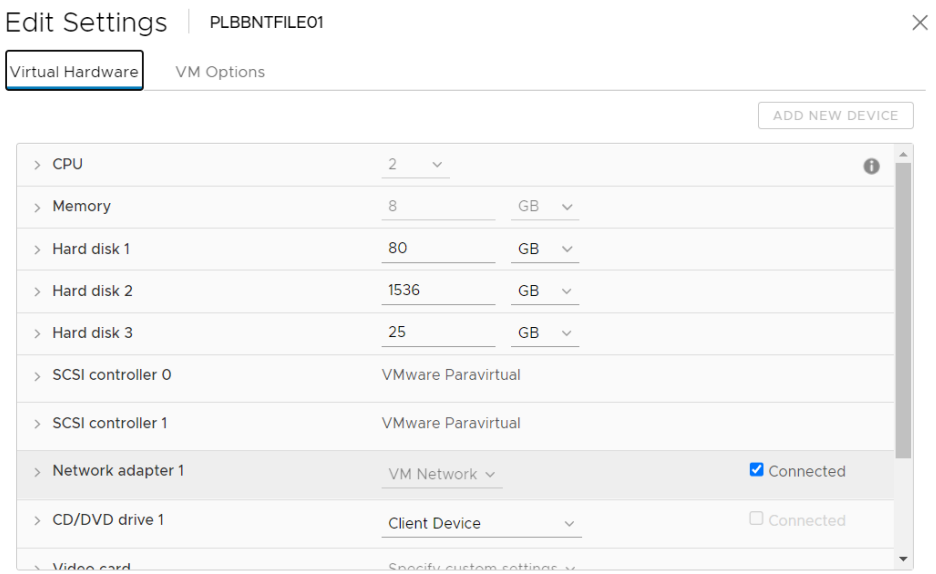


Рисунок 3.28 – Апаратна конфігурація файлового сервера

Як вбачається з вище наведеного, файловий сервер використовує 2 ядра віртуального процесора, 8 ГБ оперативної пам’яті RAM та 3 диски. Один з них має 80 ГБ (системний диск), другий – 1563 ГБ і застосовується для зберігання файлів, та наявний останній додатковий диск ємністю 25 ГБ.

3.8.2 Конфігурація послуги файлового сервера

Зі сторони користувача файловий сервер відповідає за надання файлових ресурсів (папок і файлів) користувачам домену. Для того, щоб користувачі мали доступ до вибраних папок, розташованих на диску сервера, вони повинні мати відповідні дозволи.

На нижченаведеному рисунку 3.29 показано приклад поділу файлів на дві групи (IT і Люди):

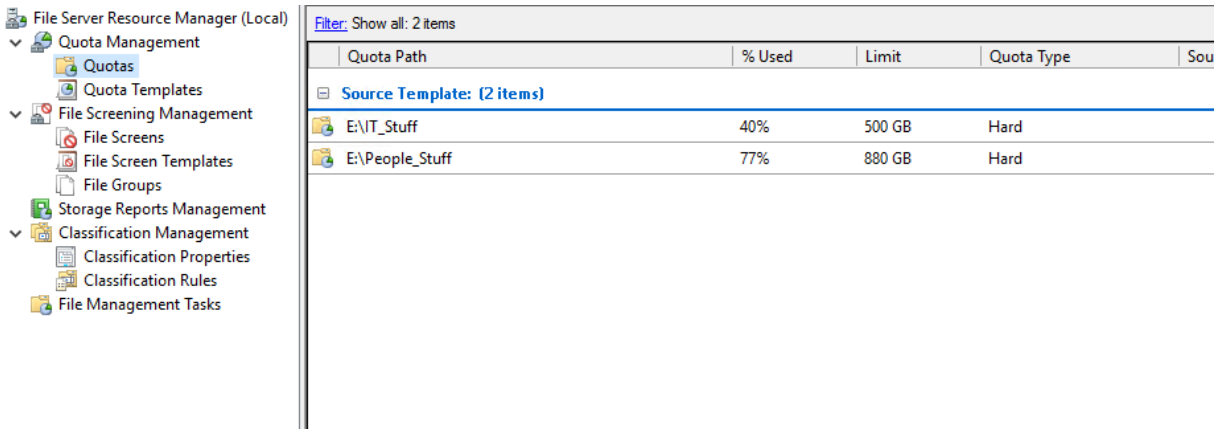


Рисунок 3.29 – Поділ файлів на дві групи

Іншим важливим елементом є створення дискових томів таким чином, щоб спільний том мав відповідний обсяг простору. На рисунку 3.30 наведено приклад поділу диска.

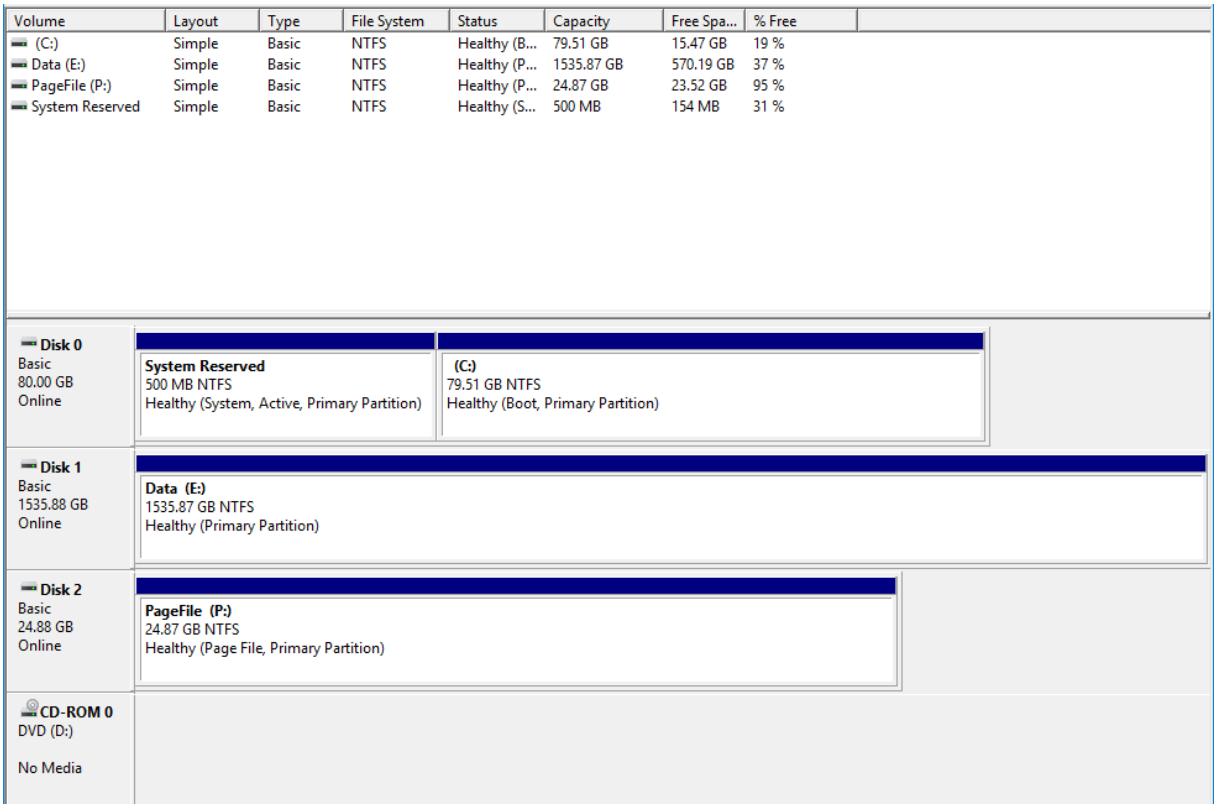


Рисунок 3.30 – Розбиття диска файлового сервера

Останнім елементом конфігурації, який представлено, є папки зі спільним доступом. На нижче наведеному рисунку 3.31 визначити, до яких папок було

надано спільний доступ для вибраної групи користувачів і як. Тут також варто зазначити, що деякі зі спільних папок мають знак «$». Це так звані приховані папки, до яких потрібно знати стежку доступу.

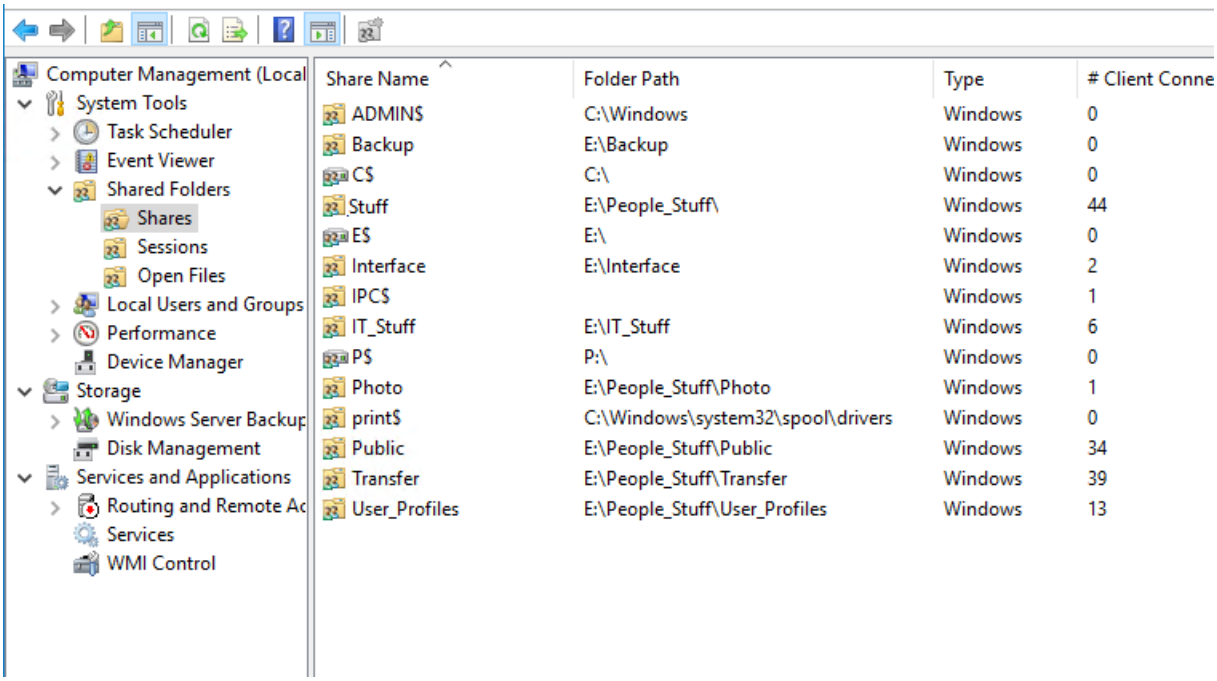


Рисунок 3.31 – Папки зі спільним доступом

3.9 Конфігурація сервера друку

3.9.1 Апаратна конфігурація сервера друку

Сервер друку не вимагає багато апаратних ресурсів, таких як оперативна пам'ять RAM або жорсткий диск. Однак, на відміну, наприклад, від файлового сервера, він має аж 4 віртуальні ядра процесора. Це потрібно для того, щоб сервер міг безпроблематично обслуговувати декілька операцій одночасно. На нижченаведеному рисунку 3.32 показано детальну конфігурацію обладнання для сервера друку.

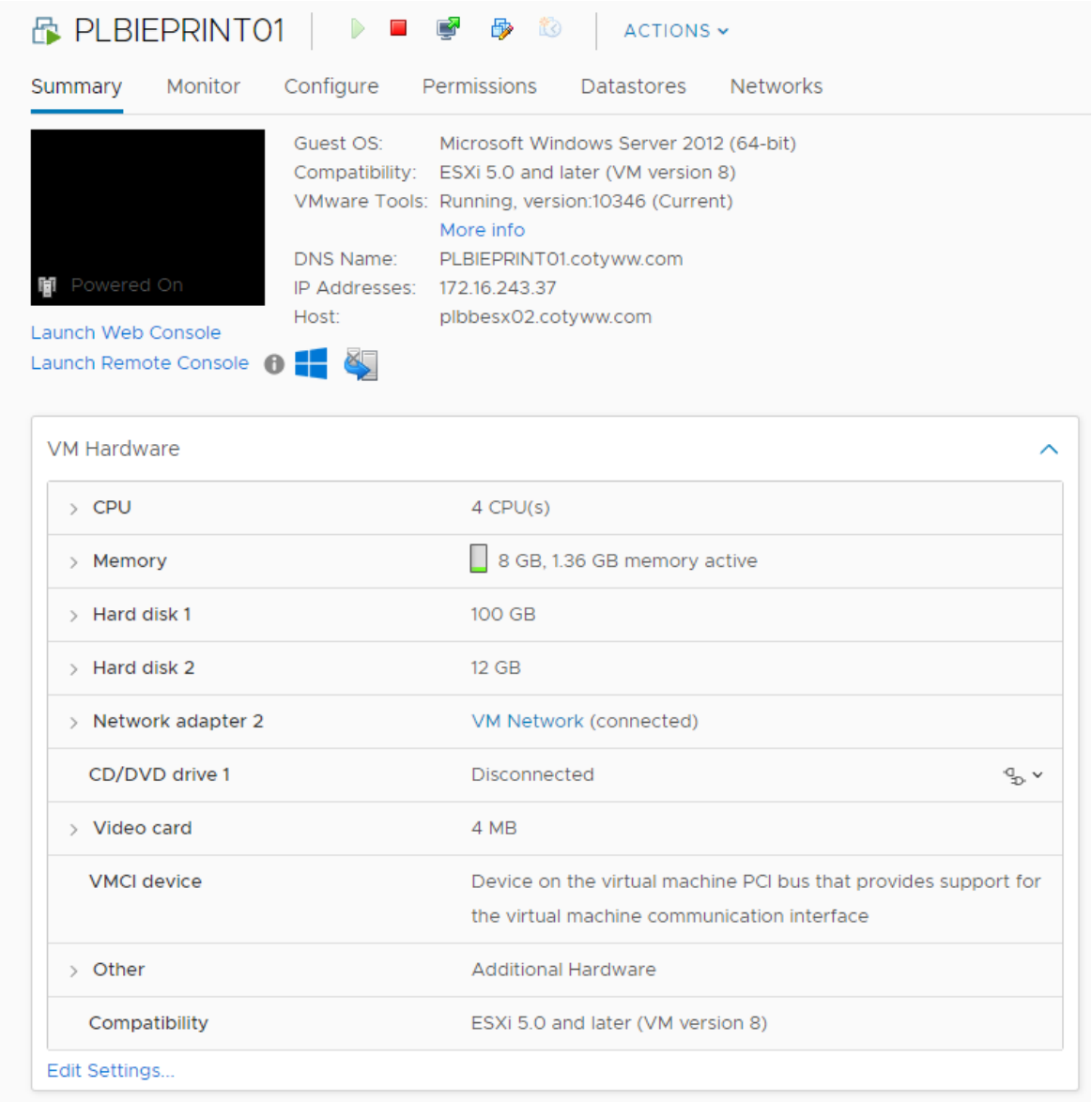


Рисунок 3.32 Конфігурацію обладнання для сервера друку

3.9.2 Конфігурація послуги сервера друку

Здійснити конфігурацію сервера друку відносно нескладно. Вона зводиться до встановлення сервера друку (англ. Print Management) на Windows Server, а потім додання до нього мережевих принтерів. Це рішення добре тим, що в ситуації простого збою або заклинювання принтера IT-співробітник може, наприклад, перезавантажити пристрій з сервера. На нижче наведених рисунках показано приклад здійснення конфігурації сервера друку (принтери та порти).

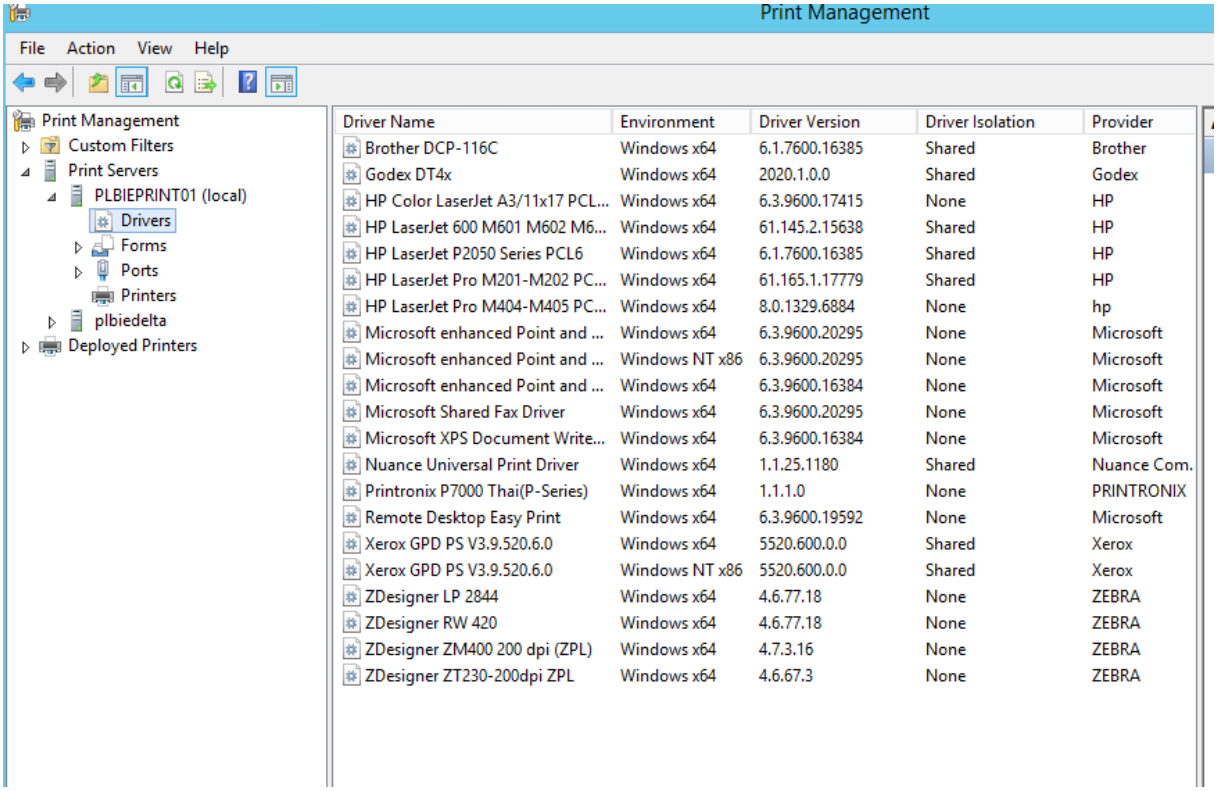


Рисунок 3.33 Приклад здійснення конфігурації сервера друку (принтери)

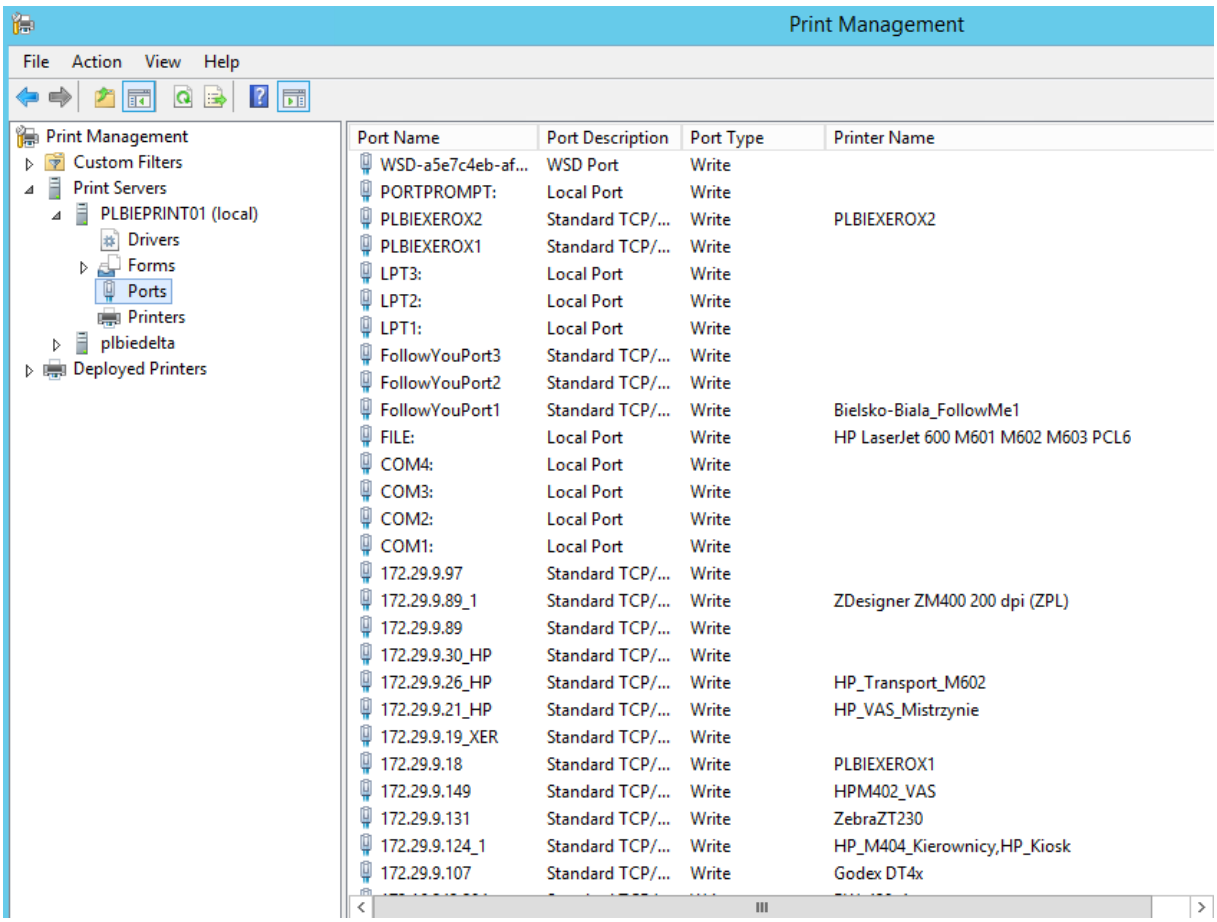


Рисунок 3.34 Приклад здійснення конфігурації сервера друку (порти)

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Метою кваліфікаційної роботи магістра є створення захищеної комп'ютерної мережі та на її основі всієї комп'ютерної системи, яка може використовуватися в корпорації. Всю мережу буде створено на основі доступних рішень, які дають змогу побудувати, захистити та сконфігурувати її. Оскільки, проведення таких видів робіт передбачає застосування комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників зі створення захищеної комп'ютерної мережі та на її основі всієї комп'ютерної системи, яка може використовуватися в корпорації. В, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [16]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог;

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд.

Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який

може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним. Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА 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». Відстань від екрана до ока фахівців, які працюють за комп’ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп’ютера,

зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп'ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців зі створення захищеної комп'ютерної мережі та на її основі всіє\ комп'ютерної системи, яка може використовуватися в корпорації.

4.2. Вплив електромагнітного імпульсу ядерного вибуху на елементи виробництва та заходи захисту

У воєнний час при застосуванні ядерної зброї проти України на електронно-обчислювальне обладнання в першу чергу буде впливати електромагнітний імпульс (ЕМІ) ядерного вибуху у вигляді короткого імпульсу, який вражає головним чином електричну та електронну апаратуру. ЕМІ виникають в основному в результаті взаємодії гамма-випромінювання з атомами навколишнього середовища. На утворення ЕМІ йде невелика кількість ядерної енергії, але він здатен викликати високі імпульси струмів та напруг в кабелях повітряних і підземних ліній зв'язку, сигналізації, управління, електропередачі, в антенах радіостанцій. Вплив ЕМІ може привести до згортання чутливих електронних та електричних елементів, зв'язаних з великими антенами чи відкритими дротами, а також до порушень в обчислювальних пристроях. Вплив ЕМІ необхідно враховувати для всіх електричних та електронних систем [17].

Особливістю ЕМІ, як вражаючого фактору є його здатність розповсюджуватись на десятки і сотні кілометрів в оточуючому середовищі. Тому ЕМІ може вплинути своєю дією на об'єкти, там де вибухова хвиля, світлове випромінювання, проникаюча радіація втрачають своє значення, як вражаючі фактори. При наземних та низьких повітряних вибухах в лініях зв'язку та електрозабезпечення виникають напруги, які можуть викликати пробій ізоляції провідників та кабелів відносно землі, пробій ізоляції елементів приладів підключених до повітряних і підземних ліній..

Найбільш піддані впливу ЕМІ системи зв'язку, сигналізації, управління. Використані в цих системах кабелі та апаратура мають обмежену електричну міцність не більше 10кВ імпульсної напруги, тоді як наведені імпульси напруги від ЕМІ можуть перевищувати ці значення. Найбільш піддана впливу ЕМІ апаратура виконана на напівпровідниках та інтегральних схемах, працюючих на малих струмах і напругах, і значить відчутних до впливу зовнішніх електричних і магнітних кіл, в тому числі і елементи програмного засобу для управління процесом міграції віртуальних машин в обчислювальній хмарі. ЕМІ пробиває ізоляцію, спалює елементи електричних схем радіоапаратури, викликає коротке замикання в радіопристроях, іонізацію діелектриків, змінює або повністю стирає магнітний запис. ЕМІ пошкоджує також резистори, викликає іскріння в їх міжконтактних з'єднаннях і деяких областях провідної поверхні. Найбільшу небезпеку ЕМІ представляє для апаратури, яка встановлена в особливо міцних спорудах, які витримують великі тиски ударної хвилі. В цих спорудах апаратура не виходить з ладу від механічних пошкоджень, але ЕМІ може вивести з ладу всю незахищену апаратуру системи зв'язку, сигналізації і керування. Найбільших значень досягають напруги, які наводяться між кабелем і землею.

Розглянемо можливі шляхи рішення задачі захисту від ЕМІ. Ідеальним захистом від ЕМІ виявилося б повне укриття приміщення, в якому розміщена радіоелектронна апаратура, металевим екраном [17]. Водночас зрозуміло, що практично забезпечити такий захист у ряді випадків неможливо, тому що для роботи апаратури часто потрібно забезпечити її електричний зв'язок із зовнішніми пристроями. Тому використовуються менш надійні засоби захисту, такі, як струмопровідні сітки, або плівкові покриття для вікон, щільникові металеві конструкції для повітрезабірників і вентиляційних отворів і контактні пружинні прокладки, розміщувані по периметру дверей і люків.

Більш складною технічною проблемою рахується захист від проникнення ЕМІ в апаратуру через різноманітні кабельні входи. Радикальним рішенням даної проблеми міг би стати перехід від електричних мереж зв'язку до практично не схильних до впливу ЕМІ волоконно-оптичних. Проте заміна напівпровідникових приладів у всьому спектрі виконуваних ними функцій

електронно-оптичними пристроями можлива тільки у віддаленому майбутньому. Тому в даний час в якості засобів захисту кабельних входів найбільші широко використовуються фільтри, у тому числі волоконні, а також іскрові розрядники, металлоокисні варистори і високошвидкісні зенеровські діоди [75].

Всі ці засоби мають як переваги, так і недоліки. Так, ємнісно-індуктивні фільтри достатньо ефективні для захисту від ЕМІ малої інтенсивності, волоконні фільтри захищають у відносно вузькому діапазоні надвисоких частот. Іскрові розрядники мають значну інерційність й в основному придатні для захисту від перевантажень, що виникають під впливом напруг і струмів, що наводяться в обшивці літака, кожусі апаратури й оплетенні кабеля.

Металоокисні варистори є напівпровідниковими приладами, що різко підвищують свою провідність при високій напрузі. Проте, при застосуванні цих приладів у якості засобів захисту від ЕМІ варто враховувати їх недостатньо високу швидкодію і погіршення характеристик при кількаразовому впливі навантажень. Ці недоліки відсутні у високошвидкісних зенеровських діодах, дія яких заснована на різкій лавиноподібній зміні опору від високого значення практично до нуля, при перевищенні прикладеної до них напруги граничного розміру. Крім того на відміну від варисторів характеристики зенеровських діодів після багатократних впливів високих напруг і переключень режимів не погіршуються.

Найбільш раціональним підходом до проектування засобів захисту від ЕМІ кабельних входів є створення таких роз'ємів у конструкції яких передбачені спеціальні заходи, що забезпечують формування елементів фільтрів і установку вмонтованих зенеровських діодів. Подібне рішення сприяє одержанню дуже малих значень ємності й індуктивності, що необхідно для забезпечення захисту від імпульсів, що мають незначну тривалість і, отже, потужну високочастотну складову.Складність рішення задачі захисту від ЕМІ і висока вартість розроблених для цього засобів і методів змушують піти по шляху їхнього вибіркового застосування в особливо важливих системах зброї і військової техніки. Проте основним методом вирішення проблеми спеціалісти вважають створення так званих розподілених мереж зв'язку [17].

ВИСНОВКИ

Створення корпоративної комп’ютерної системи, представленої у цій роботі, є лише теоретичною роботою. Хоча вона містить обґрунтування вибору та застосування зразків моделей обладнання та пристроїв, вона не містить цінової пропозиції, яка може бути важливою для більшості клієнтів.

Опрацьовано теоретичну частину роботи, в якій описано всі запропоновані рішення. У цій частині значну увагу приділено обґрунтуванню та опису застосованих засобів і встановлених на них систем. Для найкращої ілюстрації обговорюваних питань також представлені схеми мереж.

У практичній частині висвітлено конкретні пристрої, за допомогою яких здійснено реалізацію запропонованої захищеної комп’ютерної мережі. Також представлено апаратну та системну конфігурації розглянутих завдань.

Розроблене у цій роботі рішення надається для впровадження в корпорації середнього розміру. Його підготовлено за новітніми технологіями, що дає можливість подальшого розвитку проєкту.

Підсумовуючи, роботу реалізовано відповідно до попередніх припущень. Завдяки такому масштабному проекту отримано нові знання та досвід, які дозволять розвиватися в напрямку комп’ютерних мереж. Проєкт виконаної роботи створювався від початку (комп'ютерна система) до завершення, кінцевим результатом якого є повнофункціональна захищена корпоративна комп’ютерна мережа.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Микитишин, А.Г., Митник, М.М., Стухляк, П.Д., Пасічник, В.В. (2013). Комп'ютерні мережі [навчальний посібник]. Львів, «Магнолія 2006».
2. Peterson, L., Davie B. (2019). Computer Networks: A Systems Approach. Publisher: Larry Peterson and Bruce Davie. https://open.umn.edu/opentextbooks/textbooks/771
3. What is OSI Model? – Layers of OSI Model. https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/
4. Вибір кабелю типу вита пара: UTP або FTP? https://deps.ua/ua/knowegable-base/articles/8680.html
5. Що таке віртуалізація сервера? https://introserv.com/ua/blog/shho-take-virtualizacziya-servera/
6. Яка різниця між VMware vSphere, ESXi та vCenter. https://introserv.com/ua/blog/yaka-rizniczya-mizh-vmware-vsphere-esxi-ta-vcenter/
7. Що таке гіпервізор та його роль у віртуалізації. https://vps.ua/blog/ukr/hypervizor-and-virtualization/
8. Що таке гіпервізор: визначення, типи та можливості. https://gigacloud.ua/blog/navchannja/scho-take-gipervizor-viznachennja-tipi-ta-mozhlivosti
9. Горбенко, І. Д., Гриненко, Т. О. (2004). Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації. Харків: ХНУРЕ.
10. RAID. https://en.wikipedia.org/wiki/RAID
11. Kuznetsov, O., Poluyanenko, N., Frontoni, E., Kandiy, S., Karpinski, M., & Shevchuk, R. (2024). Enhancing Cryptographic Primitives through Dynamic Cost Function Optimization in Heuristic Search. Electronics, 13(10), 1-52. doi: 10.3390/electronics13101825.

12. Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., Kozak, R., Shevchuk, R. (2023). Technique for Searching Data in a Cryptographically Protected SQL Database. Applied Sciences, 13(20), art. no. 11525, 1-21. doi: 10.3390/app132011525.

13. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni E., Veselska, O., & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. Information, 14(5), art. no. 259, 1-16. doi: 10.3390/info14050259.

14. Yakymenko, I., Karpinski, M., Shevchuk, R., & Kasianchuk, M. (2024). Symmetric Encryption Algorithms in a Polynomial Residue Number System. Journal of Applied Mathematics, art. id 4894415, 1-12. doi: 10.1155/2024/4894415.

15. Droms, R., Lemon, T. (2003). The DHCP Handbook. Sams. https://books.google.com.ua/books/about/The_DHCP_Handbook.html?id=FV9rlGsIXZkC&redir_esc=y

16. Зеркалов Д.В. Охорона праці в галузі: Загальні вимоги. Навчальний посібник. К.: Основа. 2011. 551 с.

17. Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання / укл.: Стручок В. С. Тернопіль: ФОП Паляниця В. А., 2022. 156 с.

Додаток А Публікація

УДК 004.7
Роман Калушка, Микола Карпінський (докт. техн. наук, проф.)
(Тернопільський національний технічний університет імені Івана Пулюя)

ЗАХИЩЕНА КОРПОРАТИВНА КОМПЮТЕРНА МЕРЕЖА

Roman Kalushka, Mykola Karpinskyi (Dr. Prof.)

A SECURE CORPORATE COMPUTER NETWORK

В даний час базовим елементом корпорації є комп'ютерна мережа. Для створення захищеної комп’ютерної мережі використано різні компоненти, зокрема електропроводку. мережевий комутатор, маршрутизатор, сервер, комп'ютери тощо [1]. Сучасною нормою побудови комп’ютерних мереж в кожній корпорації є топологія «зірка», тому її застосовано в цій роботі. Засоби з кількома мережевими картами (сервери, дискові накопичувачі, бібліотеки) під’єднуються до обох комутаторів. Для випадку аварії одного з комутаторів сервери залишаються доступними в мережі, оскільки мережевий трафік автоматично перемикається на інший пристрій.

Одним з важливих елементів комп'ютерної системи корпорації застосовано мережу SAN (Storage Area Network). Це підмережа, фізично відокремлена від локальної мережі, яка з’єднує дискові ресурси (дискові масиви, стрічкову бібліотеку) із серверами. Завдяки цьому всі сервери мають виділений доступ до дискових ресурсів, що забезпечує можливість побудови високоефективної, масштабованої та стійкої до збоїв комп’ютерної системи.

У цій роботі застосовано віртуальне середовище VMware. В конфігурації, яку застосовано для створення віртуального середовища, використано два фізичні сервери, які названо хостами, та дисковий накопичувач, під’єднаний до фізичних серверів через мережу SAN. Ядра процесора та оперативна пам’ять для створення віртуальних машин використовують фізичні процесори та оперативну пам’ять обох хостів, а дисковий масив забезпечує дискові ресурси для цих віртуальних машин. Слід зазначити, що відмовостійкість є найбільшою перевагою віртуального середовища. Ще однією перевагою віртуального середовища є висока доступність і масштабованість.

У конкретному випадку нашої роботи створено 6 віртуальних машин, а саме: сервер DHCP, файловий сервер, сервер друку, контролер активного каталогу AD (Active Directory), сервер бази даних, сервер додатків. В роботі розроблено схему під’єднання серверів і дискового накопичувача до мережі LAN. Кожен сервер під’єднано чотирма портами. Це забезпечує резервування, так що для випадку збою порту в комутаторі або сервері буде забезпечена безперервна робота цих пристроїв. У той же час, для відповідної конфігурації комутаторів, два канали зв'язку між сервером і комутатором застосовано для розподілу трафіку між ними, використовуючи алгоритми балансування навантаження.

В роботі проведено конфігурації маршрутизатора, хоста, резервного сервера, дискового накопичувача, віртуальної машини контролера домену, DHCP, файлового сервера та сервера друку. Маршрутизатором застосовано TP-Link з бізнес-серії. Для проєкту було здійснено конфігурацію двох серверів компанії Lenovo.

Розроблене у цій роботі рішення надається для впровадження в корпорації середнього розміру. Його підготовлено за новітніми технологіями, що дає можливість подальшого розвитку проєкту.

Література

1. Peterson, L., Davie B. (2019). Computer Networks: A Systems Approach. Publisher: Larry Peterson and Bruce Davie.