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

бакалавр
(освітній рівень)

на тему: " Розробка та налаштування безпечної IT-інфраструктурі на базі Hyper-V в Windows Server Core "

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Вівчарівський Назарій Ігорович
підпис (прізвище та ініціали)

Керівник Кульчицький Т. Р.
підпис (прізвище та ініціали)

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

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

Рецензент
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 Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Вівчарівському Назарію Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка та налаштування безпечної IT-інфраструктурі на базі Hyper-V в Windows Server Core

Керівник роботи Кульчицький Тарас Русланович, доктор філософії, старший викладач кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 15 » 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 12.06.2024

3. Вихідні дані до роботи Вимоги до безпеки IT-інфраструктури. Windows Server Core Гіпервізор Hyper-V, брандмауер та маршрутизатор IPFire, NAS Openmediavault

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд технології віртуалізації
2. Налаштування лабораторного середовища створення віртуалізованої іт-інфраструктури
3. Розгортання та тестування віртуалізованої іт-інфраструктури
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі. Основні принципи віртуалізації. Огляд технології Hyper-V. Архітектура гіпервізора Hyper-V. Розробка Архітектури безпечної IT-інфраструктури. Схема лабораторного тестового середовища. Коротко про Windows Server 2022 Core. Початкова налаштування Windows Server 2022 Core. Встановлення та налаштування Hyper-V. Огляд роботи компонентів Hyper-V. Створення та налаштування віртуальних комутаторів. Віртуальні мережеві адаптери. Встановлення та налаштування брандмауера IPFire в віртуалізованому середовищі. Встановлення та налаштування NAS сервера Openmediavault. Встановлення та налаштування Windows Server 2022 Desktop. Тестування віртуалізованої інфраструктури. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2024	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд технології віртуалізації»	21.02 – 10.03	
4.	Оформлення розділу «Налаштування лабораторного середовища створення віртуалізованої ІТ-інфраструктури»	11.03 – 25.03	
5.	Оформлення розділу «Розгортання та тестування віртуалізованої ІТ-інфраструктури»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	26.06.2024	

Студент _____ Вівчарівський Н. І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Кульчицький Т. Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка та налаштування безпечної IT-інфраструктурі на базі Hyper-V в Windows Server Core // Кваліфікаційна робота ОР «Бакалавр» // Вівчарівський Назарій Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2024 // С. 58, рис. – 30, табл. – 1, кресл. – 17, додат. – 0.

Ключові слова: Hyper-V, IPFire, NAS, Openmediavault, NAT, гіпервізор, віртуалізація, Windows, брандмауер.

В кваліфікаційній роботі бакалавра було проведено аналіз технології віртуалізації з фокусом на гіпервізорі Hyper-V. Висвітлено основні принципи віртуалізації. Проведено аналіз та опис архітектури Hyper-V. Показано що апаратна підтримка віртуалізації (Intel VT-x і AMD-V) зменшує накладні витрати, покращує продуктивність віртуальних машин на платформі Hyper-V та забезпечує ефективну ізоляцію між ними. Було створено лабораторне середовище, встановлено та налаштовано Windows Server 2022 Core з ролю Hyper-V. Розглянуто налаштування брандмауера IPFire, NAS Openmediavault та Windows Server 2022 в віртуалізованому середовищі. Продемонстровано їх взаємодію та стабільну роботу у віртуалізованій інфраструктурі.

Проведено тести, що підтверджують успішність реалізації та високу ефективність віртуалізованої інфраструктури. Робота важлива для практичного використання в бізнесі, де вимагається стабільність та безпека IT-систем.

ANNOTATION

Development and configuration of a secure IT infrastructure based on Hyper-V in Windows Server Core // Thesis of educational level "Bachelor"// Nazarii Vivcharivskyi // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-42 // Ternopil, 2024 // P. 58, fig. - 30, tab. - 1, chair. - 17, added. – 0.

Keywords: Hyper-V, IPFire, NAS, Openmediavault, NAT, hypervisor, virtualization, Windows, firewall.

The bachelor's thesis analyzed virtualization technologies with a focus on the Hyper-V hypervisor. The basic principles of virtualization are highlighted. The analysis and description of the Hyper-V architecture was carried out. It is shown that hardware support for virtualization (Intel VT-x and AMD-V) reduces overhead, improves the performance of virtual machines on the Hyper-V platform, and provides effective isolation between them. A lab environment was created and Windows Server 2022 Core with Hyper-V role was installed and configured. Considered setting up an IPFire firewall, Openmediavault NAS, and Windows Server 2022 in a virtualized environment. Their interaction and stable operation in a virtualized infrastructure is demonstrated.

Tests have been conducted that confirm the successful implementation and high efficiency of the virtualized infrastructure. The work is important for practical use in business where stability and security of IT systems is required.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

NAS	—	Network Attached Storage
ADDC	—	Active Directory Domain Controller
SMB	—	Server Message Block
NFS	—	Network File System
BM	—	Віртуальна машина
DEP	—	Data Execution Prevention
IOMMU	—	Input Output Memory Management Unit
VSP	—	Virtualization Service Provider
LAN	—	Local Area Network
WAN	—	Wide Area Network
VMM	—	Virtual Machine Monitor
TCP	—	Transmission Control Protocol
GUI	—	Graphical User Interface
VSC	—	Virtualization Service Client
DHCP	—	Dynamic Host Configuration Protocol
APIC	—	Advanced Programmable Interrupt Controller
VMBus	—	Virtual Machine Bus
IC	—	Integration component
MSR	—	Memory Service Routine
VID	—	Virtualization Infrastructure Driver
VM	—	Virtual Machine
VMMS	—	Virtual Machine Management Service
DNS	—	Domain Name System
VMWP	—	Virtual Machine Worker Process
ADDS	—	Active Directory Domain Services
TLS	—	Transport Layer Security
WinHv	—	Windows Hypervisor Interface Library
WMI	—	Windows Management Instrumentation

SConfig	—	Server Configuration tool
WebUI	—	Web User Interface
IPS	—	Intrusion Prevention System
OMV	—	Openmediavault

ВСТУП

Сучасна динаміка розвитку телекомунікаційної сфери призводить до непередбачуваних викликів у сфері безпеки. Забезпечення високого рівня безпеки та оптимального функціонування корпоративних мереж вимагає нових підходів та рішень. В даному контексті, розробка та налаштування безпечної IT-інфраструктури на базі гіпервізора Hyper-V в Microsoft Windows Server стає актуальним завданням для підприємств, організацій та інших суб'єктів, що прагнуть до забезпечення надійності та конфіденційності своїх даних.

Метою даного дослідження є розробка та налаштування IT-інфраструктури на базі гіпервізора Hyper-V в Microsoft Windows Server Core з використанням віртуальних машин IPFire, Microsoft Windows Server 2022 та NAS Openmediavault. Головні задачі включають встановлення та налаштування Microsoft Windows Server Core з функцією Hyper-V, встановлення та конфігурування віртуальних машин IPFire, Microsoft Windows Server 2022 та Openmediavault, налаштування маршрутизації та безпеки за допомогою IPFire, встановлення та налаштування Windows Server 2022 як контролер домену а також підключення та використання NAS Openmediavault для забезпечення ефективного та безпечного зберігання даних.

Об’єктом дослідження є IT-інфраструктура на базі гіпервізора Hyper-V в Microsoft Windows Server Core, яка включає в себе віртуальні машини, маршрутизатор IPFire, Windows Server 2022 як контролер домену та NAS openmediavault. Дослідження спрямоване на оптимізацію цієї інфраструктури з метою підвищення безпеки та ефективності її функціонування.

Предметом дослідження є конкретні аспекти розробки та налаштування IT-інфраструктури: віртуалізація за допомогою гіпервізора Hyper-V в Microsoft Windows Server Core, використання IPFire як маршрутизатора (включаючи IPS, NAT та брандмауер) та Windows Server 2022 як ADDC а також роль NAS Openmediavault як сервісу зберігання даних з підтримкою SMB та NFS.

Отримані результати передбачається використовувати для покращення безпеки та ефективності роботи IT-інфраструктур у сучасних умовах. Розроблені

та налаштовані компоненти можуть бути використані як підґрунтя для створення безпечних мережевих інфраструктур для різноманітних організацій, що прагнуть до високого рівня захисту та продуктивності в обробці та зберіганні даних.

РОЗДІЛ 1 ОГЛЯД ТЕХНОЛОГІЇ ВІРТУАЛІЗАЦІЇ

1.1 Основні принципи віртуалізації

Віртуалізація полягає в розділенні фізичних ресурсів (процесорів, пам'яті, зберігання) на віртуальні, що надає можливість ефективніше використовувати доступні ресурси та розділяти їх між віртуальними середовищами [1]. Віртуальні машини повинні бути ізольовані одна від одної, щоб уникнути конфліктів та забезпечити стійкість роботи всіх ВМ. Кожна ВМ має свою власну операційну систему та додаткове програмне забезпечення, що робить її незалежною від інших. Також має підтримуватись можливість міграції (перенесення) віртуальних машин між різними фізичними серверами без необхідності переконфігурації. Можливість міграції забезпечує високу доступність та зручність управління ресурсами. Віртуалізація спрямована на максимально ефективне використання ресурсів фізичного сервера. Забезпечення високої завантаженості та оптимального розподілу ресурсів між віртуальними машинами. Віртуалізація передбачає централізоване управління віртуальними ресурсами, включаючи можливості моніторингу, автоматизації та резервного копіювання, що спрощує адміністрування та забезпечує зручність управління. Можливість резервування та відновлення ВМ дозволяє швидко адаптуватися до змін у вимогах до обчислювальних ресурсів.

Важливий аспект віртуалізації - забезпечення безпеки та відокремлення віртуальних середовищ. Це включає в себе заходи захисту від можливих атак на рівні віртуальних шарів.

Гіпервізор (VMM) - це програмне забезпечення, яке дозволяє створювати та управляти віртуальними машинами на фізичному обладнанні. Існують два основних типи гіпервізорів: гіпервізори 1-го та 2-го типу.

Гіпервізор 1-го типу (native, bare-metal) встановлюється безпосередньо на апаратне забезпечення сервера [2]. Приклади: VMware ESXi, Microsoft Hyper-V, Xen та KVM. Зазвичай є більш продуктивним, оскільки працює безпосередньо на апаратному рівні. Незалежний від операційних систем хоста, що забезпечує

вищу стабільність. Більш ефективне використання ресурсів, оскільки не потребує операційної системи хоста. Зазвичай використовується у великих дата-центрах та для корпоративних IT-інфраструктур [3].

Гіпервізор 2-го типу (hosted) встановлюється як програмне забезпечення на операційну систему хоста. Приклади: Oracle VirtualBox, VMware Workstation. Може мати деяку додаткову втрату продуктивності, оскільки працює поверх операційної системи хоста. Залежить від операційної системи хоста, інтегрується з нею. Може потребувати додаткових ресурсів через операційну систему хоста. Зручний для розробки та тестування, а також для освітніх цілей.

За допомогою цих принципів та понять віртуалізація стає потужним інструментом для оптимізації роботи серверних систем та надання ефективних та гнучких IT-інфраструктур для різноманітних завдань.

1.2 Огляд технології Hyper-V

Hyper-V - це гіпервізор від компанії Microsoft, який надає можливість віртуалізації операційних систем на платформі Windows [4]. Кожна віртуальна машина діє як повний комп’ютер, на якому працює операційна система та програми. Коли потрібні обчислювальні ресурси, віртуальні машини надають вам більше гнучкості, допомагають заощадити час і гроші та є більш ефективним способом використання обладнання, ніж просто запуск однієї операційної системи на фізичному обладнанні. Hyper-V запускає кожну віртуальну машину у власному ізольованому просторі, що означає, що можна одночасно запускати більше однієї віртуальної машини на одному обладнанні. Це дозволяє уникнути таких проблем, як збій, що впливає на інші робочі навантаження, а також дозволяє надати різним людям, групам або службам доступ до різних систем.

Hyper-V у Windows Server замінює старі продукти віртуалізації обладнання, такі як Microsoft Virtual PC, Microsoft Virtual Server і Windows Virtual PC. Hyper-V пропонує функції мережі, продуктивності, зберігання та безпеки, недоступні в цих старих продуктах.

Hyper-V і більшість програм віртуалізації сторонніх виробників, які потребують тих самих функцій процесора, несумісні. Включно з таким програмами, як VMware Workstation і VirtualBox. Ці програми можуть не запускати віртуальні машини або працювати в повільному режимі емуляції.

Багато програм віртуалізації залежать від апаратних розширень віртуалізації (Intel VT-x і AMD-V), які доступні на більшості сучасних процесорів. Лише один компонент програмного забезпечення може використовувати це обладнання одночасно. Апаратне забезпечення не може бути спільним для програм віртуалізації. Щоб використовувати інше програмне забезпечення віртуалізації, потрібно вимкнути Hyper-V hypervisor.

Віртуальна машина Hyper-V включає ті ж базові частини, що й фізичний комп'ютер, наприклад пам'ять, процесор, сховище та мережу. Усі ці частини мають функції та параметри, які можна налаштувати різними способами для задоволення різних потреб. Зберігання та мережі можна розглядати як окремі категорії, оскільки їх можна налаштувати багатьма способами.

Для аварійного відновлення Hyper-V Replica створює копії віртуальних машин, призначені для зберігання в іншому фізичному місці, щоб можна було відновити віртуальну машину з копії. Для резервного копіювання Hyper-V пропонує два типи. Один використовує збережені стани, а інший використовує службу тіньового копіювання томів (VSS), щоб можна було створювати сумісні резервні копії для програм, які підтримують VSS.

Кожна підтримувана гостьова операційна система має налаштований набір служб і драйверів, які називаються службами інтеграції, які спрощують використання операційної системи у віртуальній машині Hyper-V.

Такі функції, як оперативна міграція, міграція сховища та імпорт/експорт, спрощують переміщення або розповсюдження віртуальної машини.

Hyper-V включає Virtual Machine Connection, інструмент віддаленого підключення для використання як з Windows, так і з Linux. На відміну від Remote Desktop, цей інструмент надає доступ до консолі, тож можна бачити, що відбувається в гостьовій системі, навіть якщо операційна система ще не завантажена.

Захищене завантаження (secure boot) та захищені віртуальні машини (shielded virtual machines) допомагають захистити від шкідливих програм та іншого несанкціонованого доступу до віртуальної машини та її даних.

Hyper-V доступний у x64-версій Windows Server як роль сервера. Він також доступний як окремий серверний продукт Microsoft Hyper-V Server.

Багато операційних систем можуть бути встановлені як віртуальні, зокрема ті, які використовують архітектуру x86, можна запускати на гіпервізорі Hyper-V. Не всі операційні системи, які можуть бути віртуалізовані, пройшли офіційне тестування та підтримку від Microsoft.

Microsoft офіційно підтримує версії дистрибутивів Windows Server, Windows, Linux і FreeBSD для запуску у віртуальних машинах як гостьові операційні системи.

Hyper-V має певні вимоги до обладнання, і деякі з його функцій потребують додаткового обладнання. Для встановлення компонентів віртуалізації Hyper-V потрібно мати 64-розрядний процесор з технологією трансляції адрес другого рівня (SLAT), мінімум 4 ГБ оперативної пам'яті та активовану підтримку віртуалізації у BIOS або UEFI таку як Intel VT або AMD-V.

Також важливо мати включену функцію апаратного запобігання виконанню даних (DEP). Для систем Intel це біт XD (біт відключення виконання), а для систем AMD - біт NX (без біта виконання). Усі ці вимоги допомагають забезпечити ефективну та безпечну роботу Hyper-V.

1.3 Архітектура Hyper-V

Гіпервізор є основою віртуалізації. Це платформа віртуалізації для конкретного процесора, яка дозволяє кільком ізольованим операційним системам спільно використовувати одну апаратну платформу.

Hyper-V підтримує ізоляцію у вигляді розділу. Розділ - це логічна одиниця ізоляції, яка підтримується гіпервізором, у якій виконуються операційні системи. Гіпервізор Microsoft повинен мати принаймні один батьківський або кореневий розділ під керуванням Windows [5]. Стек керування віртуалізацією працює в

батьківському розділі та має прямий доступ до апаратних пристроїв. Потім кореневий розділ створює дочірні розділи, на яких розміщуються гостьові операційні системи. Кореневий розділ створює дочірні розділи за допомогою hypercall (гіпер викликів) інтерфейсу API.

Дочірні розділи в Hyper-V мають віртуальний характер, не маючи прямого доступу до фізичного процесора та не обробляючи переривання процесора. Замість цього вони працюють з віртуальним процесором та функціонують в області адрес віртуальної пам'яті, що є приватною для кожного гостьового розділу. Гіпервізор відповідає за обробку переривань процесора та направляє їх до відповідного розділу.

Крім того, Hyper-V може використовувати апаратне прискорення для трансляції адрес між різними віртуальними адресними просторами гостьових операційних систем. Це досягається за допомогою блоку керування пам'яттю введення-виведення (IOMMU), який діє незалежно від апаратного забезпечення керування пам'яттю, що використовується центральним процесором. IOMMU використовується для перенаправлення адрес фізичної пам'яті на адреси, що використовуються в дочірніх розділах, що сприяє ефективній роботі віртуальних машин у середовищі Hyper-V.

Дочірні розділи, які не мають прямого доступу до фізичних апаратних ресурсів представлені у вигляді віртуальних пристроїв (VDevs). Запити до цих віртуальних пристроїв перенаправляються через механізми VMBus або гіпервізор на пристрої в батьківському розділі, де вони обробляються. VMBus представляє собою логічний канал зв'язку між розділами.

Постачальники послуг віртуалізації (VSP) знаходяться в батьківському розділі. Вони взаємодіють через VMBus для обробки запитів щодо доступу до пристроїв від дочірніх розділів. У свою чергу, дочірні розділи містять споживачів служб віртуалізації (VSC), які направляють запити пристроїв до VSP у батьківському розділі через VMBus. Весь цей процес відбувається прозоро для гостьової операційної системи, забезпечуючи ефективну та безпечну віртуалізацію ресурсів.

Важливою особливістю віртуалізації в Windows Server є використання функції Enlightened I/O для підсистем зберігання, мережі, графіки та введення віртуальних пристроїв. Enlightened I/O представляє собою спеціалізовану реалізацію комунікаційних протоколів високого рівня, таких як SCSI, яка підтримує віртуалізацію та безпосередньо використовує VMBus. Це забезпечує ефективний обмін даними, оминаючи будь-який рівень емуляції пристрою.

Використання Enlightened I/O дозволяє зробити комунікацію між віртуальною машиною та гіпервізором більш ефективною, але для коректної роботи віртуальна машина повинна бути свідомою про те, що вона віртуалізована та про наявність гіпервізора та VMBus. Це оптимізовує взаємодію та забезпечує високу продуктивність в середовищі віртуалізації.

Компоненти Enlightened I/O і ядро з підтримкою гіпервізора в Hyper-V надаються через встановлення служб інтеграції Hyper-V. Ці компоненти включають в себе драйвери VSC та інші складові, які оптимізують взаємодію між гостьовою операційною системою і гіпервізором.

Крім того, важливою вимогою є наявність процесора з апаратною віртуалізацією, такою як технологія Intel VT або AMD-V. Це є ключовим елементом для забезпечення ефективної віртуалізації та оптимізації продуктивності в середовищі Hyper-V.

На рисунку 1.1 наведено архітектуру середовища Hyper-V.

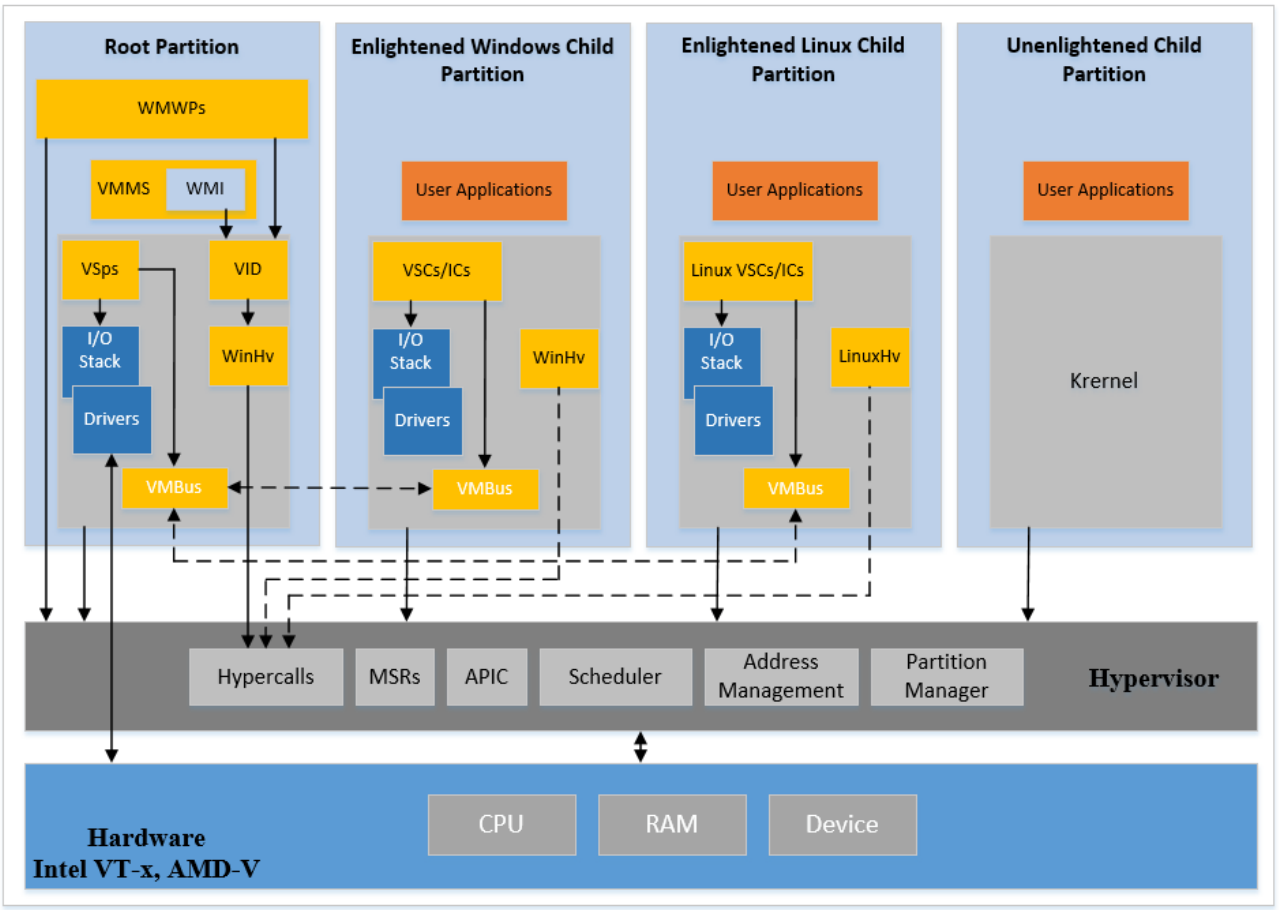

Рисунок 1.1 – Загальна архітектура гіпервізора Hyper-V

Основні компоненти архітектури наступні:

- APIC - пристрій, який дозволяє призначати рівні пріоритету для переривань.

- Child Partition - розділ, на якому розміщено гостьову операційну систему. Весь доступ до фізичної пам’яті та пристроїв дочірнього розділу надається через шину віртуальної машини (VMBus) або гіпервізор.

- Hypercall - інтерфейс для зв’язку з гіпервізором надає доступ до оптимізацій, наданих гіпервізором.

- Hypervisor – рівень програмного забезпечення, який знаходиться між апаратним забезпеченням і однією або кількома віртуальними операційними системами. Його основна робота полягає в забезпеченні ізольованих середовищ виконання, які називаються розділами. Гіпервізор керує доступом до апаратного забезпечення, що лежить в його основі.

- IC - компонент інтеграції, який дозволяє дочірнім розділам спілкуватися з іншими розділами та гіпервізором.

- I/O stack - стек введення/виведення.

- MSR - процедура обслуговування пам’яті.

- Root Partition - керує функціями на рівні фізичної машини, такими як драйвери пристроїв, керування живленням і гаряче додавання/видалення пристрою. Кореневий розділ - це єдиний розділ, який має прямий доступ до фізичної пам’яті та пристроїв..

- VID - надає служби керування розділами, служби керування віртуальним процесором і служби керування пам’яттю для розділів.

- VMBus - механізм зв’язку на основі каналів, який використовується для зв’язку між розділами та нумерації пристроїв у системах із кількома активними віртуалізованими розділами. VMBus інсталюється разом зі службами інтеграції Hyper-V (Hyper-V Integration Services).

- VMMS - служба керування віртуальними машинами відповідає за керування станом усіх віртуальних машин у дочірніх розділах.

- VMWP - робочий процес віртуальної машини це компонент стека віртуалізації в режимі користувача. Робочий процес надає служби керування віртуальною машиною у батьківському розділі до гостьових операційних систем у дочірніх розділах. Служба керування віртуальною машиною створює окремий робочий процес для кожної запущеної віртуальної машини.

- VSC - клієнт служби віртуалізації це екземпляр синтетичного пристрою, який знаходиться в дочірньому розділі. VSC використовують апаратні ресурси, надані VSP у батьківському розділі. Вони спілкуються з відповідними VSP у батьківському розділі через VMBus, щоб задовольнити запити пристроїв введення/виведення дочірніх розділів.

- VSP - постачальник послуг віртуалізації, який знаходиться в кореневому розділі та забезпечує підтримку синтетичних пристроїв для дочірніх розділів через VMBus.

- WinHv - бібліотека інтерфейсу гіпервізора Windows є мостом між драйверами операційної системи та гіпервізором, який дозволяє драйверам викликати гіпервізор за допомогою стандартних умов виклику Windows

- WMI це інструментарій керування Windows для керування та контролю віртуальних машин, який надається службою VMMS.

Гіпервізор забезпечує механізм виклику для гостей. Такі виклики називаються гіпервикликами (hypercall). Кожен гіпервиклик визначає набір вхідних і/або вихідних параметрів. Ці параметри задаються в термінах структури даних на основі пам'яті. Усі елементи вхідних і вихідних структур даних доповнюються до природних кордонів до 8 байт (тобто двобайтові елементи повинні бути на двобайтових межах тощо).

Існує два класи гіпервикликів: прості та повторні. Простий гіпервиклик виконує одну операцію та має набір вхідних і вихідних параметрів фіксованого розміру. Гіпервиклик повторний діє як серія простих гіпервикликів. Окрім набору вхідних і вихідних параметрів фіксованого розміру повторні гіпервиклики включають список вхідних і/або вихідних елементів фіксованого розміру.

Коли гість спочатку викликає повторний гіпервиклик він визначає кількість повторів, яка вказує на кількість елементів у списку вхідних і/або вихідних параметрів. Гості також вказують індекс початку повторення, який вказує на наступний вхідний та/або вихідний елемент, який має бути використаний. Гіпервізор обробляє параметри повторних гіпервикликів згідно списку, тобто шляхом збільшення індексу елемента.

Для наступних викликів гіпервиклику повторення індекс початку повторення вказує, скільки елементів було завершено і, у поєднанні зі значенням кількості повторень, скільки елементів залишилося. Наприклад, якщо абонент вказує кількість повторень 25, а лише 20 ітерацій завершено в межах часових обмежень, гіпервиклик повертає керування віртуальному процесору після оновлення індексу початку повторення до 20. Коли гіпервиклик виконується повторно, гіпервізор відновить роботу з елемента 20 і завершить роботу з рештою 5 елементів.

Якщо під час обробки елемента виникає помилка, надається відповідний код стану разом із підрахунком завершених повторень, що вказує на кількість елементів, які були успішно оброблені до того, як сталася помилка.

Гіпервиклик можна розглядати як складну інструкцію, яка займає багато циклів. Гіпервізор намагається обмежити виконання гіпервиклику до 50 мкс або менше, перш ніж повернути керування віртуальному процесору, який викликав гіпервиклик. Деякі операції гіпервикликів є досить складними, тому важко отримати гарантію 50 мкс. Таким чином, гіпервізор покладається на механізм продовження гіпервикликів для деяких гіпервикликів, включаючи всі форми повторюваних гіпервикликів.

Механізм продовження гіпервиклику здебільшого прозорий для гостей. Якщо гіпервиклик не може завершитися протягом установленого ліміту часу, керування повертається назад до гостя, але вказівник інструкції не просувається далі інструкції, яка викликала гіпервиклик. Це дозволяє обробляти очікувані переривання та планувати інші віртуальні процесори. Коли початковий потік виклику відновить виконання, він повторно виконає інструкцію гіпервиклику та просуватиметься до завершення операції.

Більшість простих гіпервикликів гарантовано буде виконано протягом встановленого терміну. Однак невелика кількість простих гіпервикликів може потребувати більше часу. Ці гіпервиклики використовують продовження гіпервикликів подібно до повторних гіпервикликів. У таких випадках операція передбачає два або більше внутрішніх станів. Перший виклик переводить об’єкт (наприклад, розділ або віртуальний процесор) в один стан, а після повторних викликів стан остаточно переходить у кінцевий стан.

За винятком випадків, коли це зазначено, дія, що виконується гіпервикликом, є атомарною щодо всіх інших гостьових операцій (наприклад, інструкцій, що виконуються в гостьовій системі), а також усіх інших гіпервикликів, які виконуються в системі. Простий гіпервиклик виконує одну атомарну дію а повторюваний гіпервиклик виконує кілька незалежних атомарних дій.

Прості гіпервиклики, які використовують продовження гіпервикликів, можуть включати кілька внутрішніх станів, видимих зовні. Такі виклики містять кілька атомарних операцій.

Кожна дія гіпервиклику може читати вхідні параметри та/або записувати результати. Вхідні дані для кожної дії можна прочитати з будь-якою деталізацією та в будь-який час після здійснення гіпервиклику та до виконання дії. Результати (тобто вихідні параметри), пов’язані з кожною дією, можуть бути записані з будь-якою деталізацією та в будь-який час після виконання дії та до повернення гіпервиклику.

Гість повинен уникати перевірки та/або маніпулювання будь-якими вхідними або вихідними параметрами, пов’язаними з виконанням гіпервиклику. Хоча віртуальний процесор, який виконує гіпервиклик, не зможе це зробити (оскільки його гостьове виконання призупинено, доки гіпервиклик не повернеться), ніщо не завадить іншим віртуальним процесорам зробити це. Гості, які поводяться таким чином, можуть вийти з ладу або спричинити пошкодження свого розділу.

Гіпервиклики можна викликати лише з режиму гостьового процесора з найбільшими привілейованими правами. На платформах x64 це означає захищений режим із нульовим поточним рівнем привілеїв (CPL). Хоча код реального режиму виконується з ефективним CPL, рівним нулю, гіпервиклики не дозволені в реальному режимі.

Усі гіпервиклики мають бути викликані через архітектурно визначений інтерфейс гіпервикликів. Спроба викликати гіпервиклик будь-яким іншим способом (наприклад, скопіювати код із кодової сторінки гіпервиклику в інше місце та виконати його звідти) може призвести до виняткової ситуації.

1.4 Висновки до розділу

В першому розділі було розглянуто основні принципи віртуалізації та вплив технології віртуалізації на управління та використання апаратного забезпечення.

Поведено огляд технології Hyper-V. Було проаналізовано та описано архітектура гіпервізора Hyper-V. Показано що гіпервізор типу 1 Hyper-V від компанії Microsoft надає можливість ефективно використовувати ресурси фізичного сервера, дозволяючи одночасно запускати та управляти кількома віртуальними машинами на одному фізичному обладнанні. Було показано що апаратна підтримка віртуалізації (Intel VT-x і AMD-V) зменшує накладні витрати, поліпшує продуктивність віртуальних машин на платформі Hyper-V та допомагає забезпечити ефективну ізоляцію між віртуальними машинами та зменшити взаємовплив між ними.

РОЗДІЛ 2 НАЛАШТУВАННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА СТВОРЕННЯ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ

2.1 Схема лабораторного тестового середовища

На схемі (див.рисунок 2.1) зображено лабораторне середовище для створення віртуалізованої ІТ-інфраструктури з використанням гіпервізора Hyper-V.

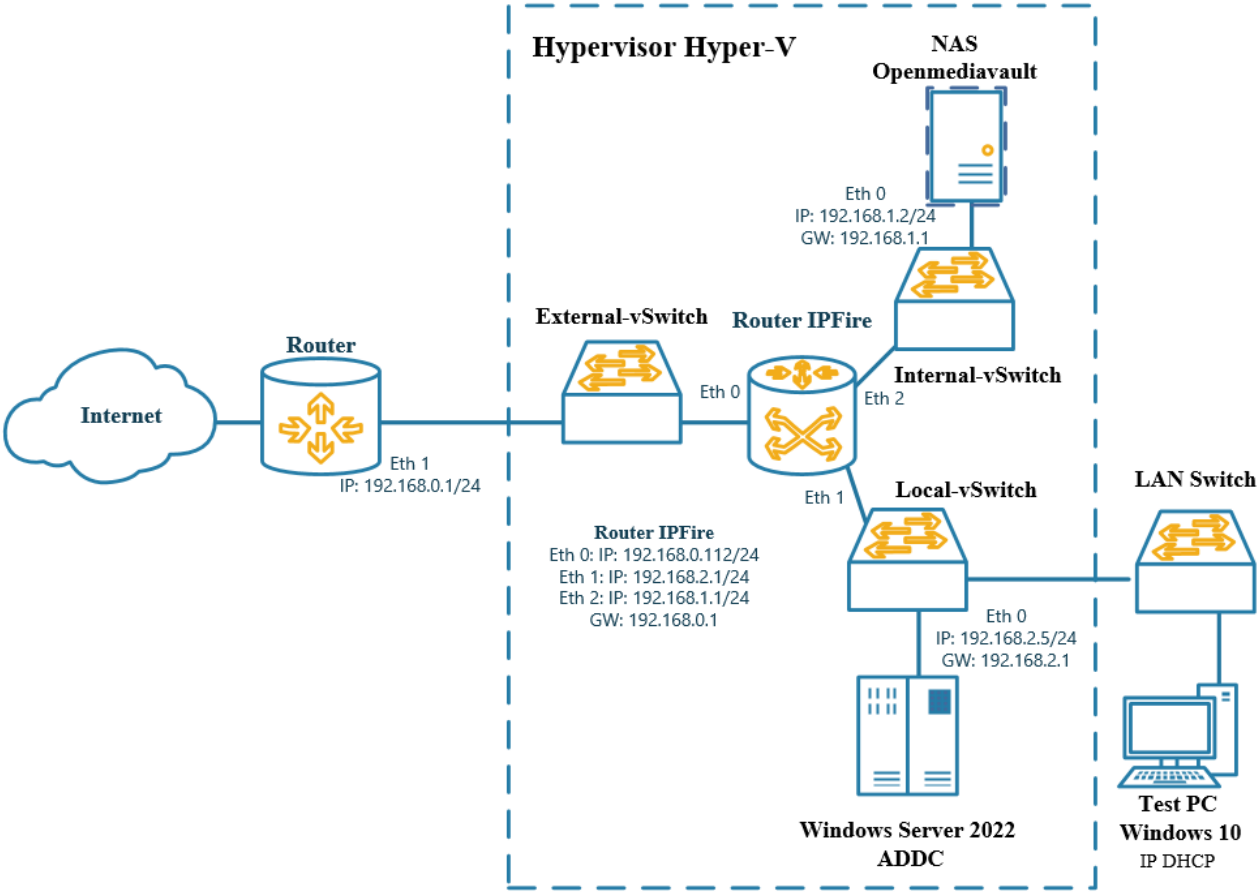

Рисунок 2.1 – Схема лабораторного тестового середовища

На схемі тестового середовища Router - це фізичний маршрутизатор з IP-адресою 192.168.0.1/24 на інтерфейсі Eth1. Маршрутизатор забезпечує доступ до Інтернету для віртуалізованого середовища.

Маршрутизатор Router IPFire – це віртуальна машина, яка виконує функції маршрутизатора та брандмауера в віртуалізованому середовищі. Даний маршрутизатор має три мережеві інтерфейси (Eth0, Eth1, Eth2) та налаштований шлюз за замовчуванням 192.168.0.1.

Фізичний LAN Switch підключений до віртуального комутатора Local-vSwitch та Test PC. LAN Switch забезпечує зв’язок з мережею LAN та через Local-vSwitch з віртуальними машинами Router IPFire, системою зберігання даних NAS Openmediavault та контролером домену Windows Server 2022 ADDC.

Test PC - це клієнтський комп'ютер з Windows 10, який отримує IP конфігурацію через DHCP з маршрутизатора Router IPFire.

2.2 Налаштування Windows Server Core

Windows Server Core представляє собою облегшену версію операційної системи, яка доступна під час встановлення версій Windows Server Standard або Datacenter [6]. Цей варіант містить більшість, але не всі ролі сервера, та характеризується меншою поверхнею атак завдяки скороченій кодовій базі.

Під час установки Windows Server можна обрати лише певні ролі, що допомагає зменшити загальний обсяг функціоналу операційної системи. Однак параметр установки Server with Desktop Experience все ще встановлює численні служби та інші компоненти, які часто не є необхідними для конкретного сценарію використання.

Інсталяція Server Core немає будь-яких служб та функцій, які не є обов'язковими для підтримки конкретних ролей сервера, які часто використовуються. Наприклад, сервер Hyper-V не вимагає графічного інтерфейсу користувача (GUI), оскільки ним можна повністю керувати з командного рядка за допомогою Windows PowerShell або віддалено за допомогою диспетчера Hyper-V.

Основна різниця між варіантами установки Server with Desktop Experience і Server Core полягає в наявності чи відсутності робочого столу. У випадку Server Core робочого столу немає. Замість цього Server Core призначений для дистанційного керування, використовуючи командний рядок, PowerShell або графічний інтерфейс (RSAT або Windows Admin Center).

У таблиці 2.1 наведено ролі, які є в параметрі встановлення Server Core.

Таблиця 2.1

Ролі включені в Server Core

Роль	Ім'я	Встановлено за умовчанням.
Служби сертифікації Active Directory	AD-Certificate	Ні
Доменні служби Active Directory	AD-Domain-Services	Ні
Служби федерації Active Directory	ADFS-Federation	Ні
Полегшені служби каталогів Active Directory	ADLDS	Ні
Служби керування правами Active Directory	ADRMS	Ні
Атестація справності пристрою	DeviceHealthAttestationService	Ні
Сервер DHCP	DHCP	Ні
Сервер DNS	DNS	Ні
Служби файлів і зберігання	FileAndStorage-Services	Так
Hyper-V	Hyper-V	Ні
Послуги друку та документації	Print-Services	Ні
Віддалений доступ	RemoteAccess	Ні
Служби віддаленого робочого столу	Remote-Desktop-Services	Ні
Послуги корпоративної активації	VolumeActivation	Ні
Веб-сервер IIS	Web-Server	Ні
Служби оновлення Windows Server	UpdateServices	Ні

На початковому етапі налаштування Server Core використаємо інструмент конфігурації сервера (SConfig). При встановленні Windows Server у варіанті Server Core, інструмент SConfig є основним методом для налаштування та управління загальними параметрами операційної системи (див.рисунок 2.2).

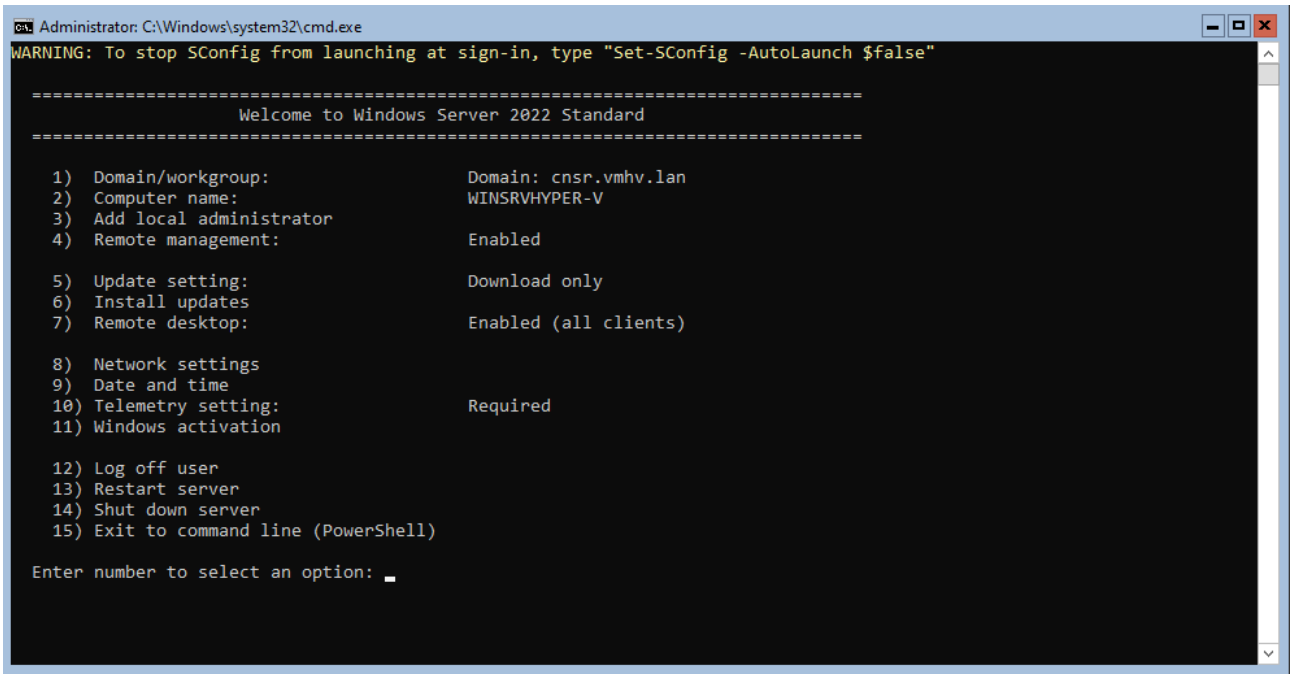

Рисунок 2.2 – Інструмент конфігурації SConfig

SConfig - це інструмент командного рядка, який дозволяє адміністраторам швидко налаштовувати основні параметри та опції сервера. Він дозволяє виконувати базові завдання конфігурації та управління сервером без необхідності виходити з командного рядка.

Сервісна програма SConfig включає в себе ряд опцій, таких як зміна імені комп'ютера, налаштування мережі, оновлення операційної системи та інші базові налаштування сервера. Це корисний інструмент для швидкого налаштування системи, зокрема у випадках, коли інші засоби або інтерфейси не є доступними або зручними для використання.

На рисунку 2.3 показано мережеві налаштування Windows Server 2022 Core в сервісній програмі SConfig.

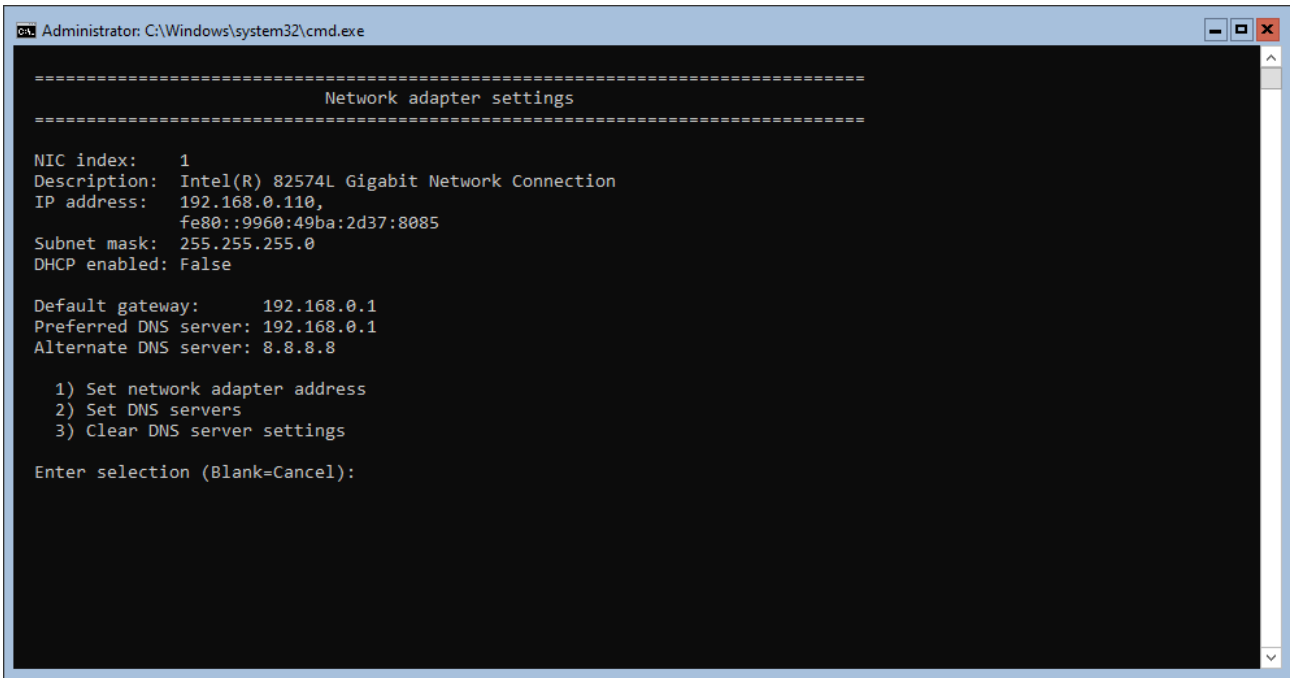

Рисунок 2.3 – Мережеві налаштування Windows Server 2022 Core

На рисунку 2.4 показано принцип взаємодії Windows Server 2022 Core та фізичного обладнання до встановлення гіпервізора Hyper-V.

Рисунок 2.4 – Windows Server 2022 встановлений безпосередньо на фізичному обладнанні

Оскільки Windows Server 2022 Core встановлено безпосередньо на фізичному обладнанні без будь-яких віртуалізаційних шарів операційна система взаємодіє безпосередньо з апаратним забезпеченням сервера, що забезпечує максимальну продуктивність та контроль над ресурсами але з втратою ефективності використання ресурсів фізичного обладнання.

Windows Server 2022 Core буде використано для встановлення та налаштування гіпервізора Hyper-V. Він є основою для налаштування віртуалізованої IT-інфраструктури.

2.3 Встановлення та налаштування Hyper-V

Для створення та запуску віртуальних машин необхідно додати роль Hyper-V в операційну систему Windows Server 2022 Core. Це можна зробити через інтерфейс Server Manager або використовуючи командлет Install-WindowsFeature в середовищі Windows PowerShell [7].

На рисунку 2.5 показано встановленням Hyper-V за допомогою команди Install-WindowsFeature в PowerShell.

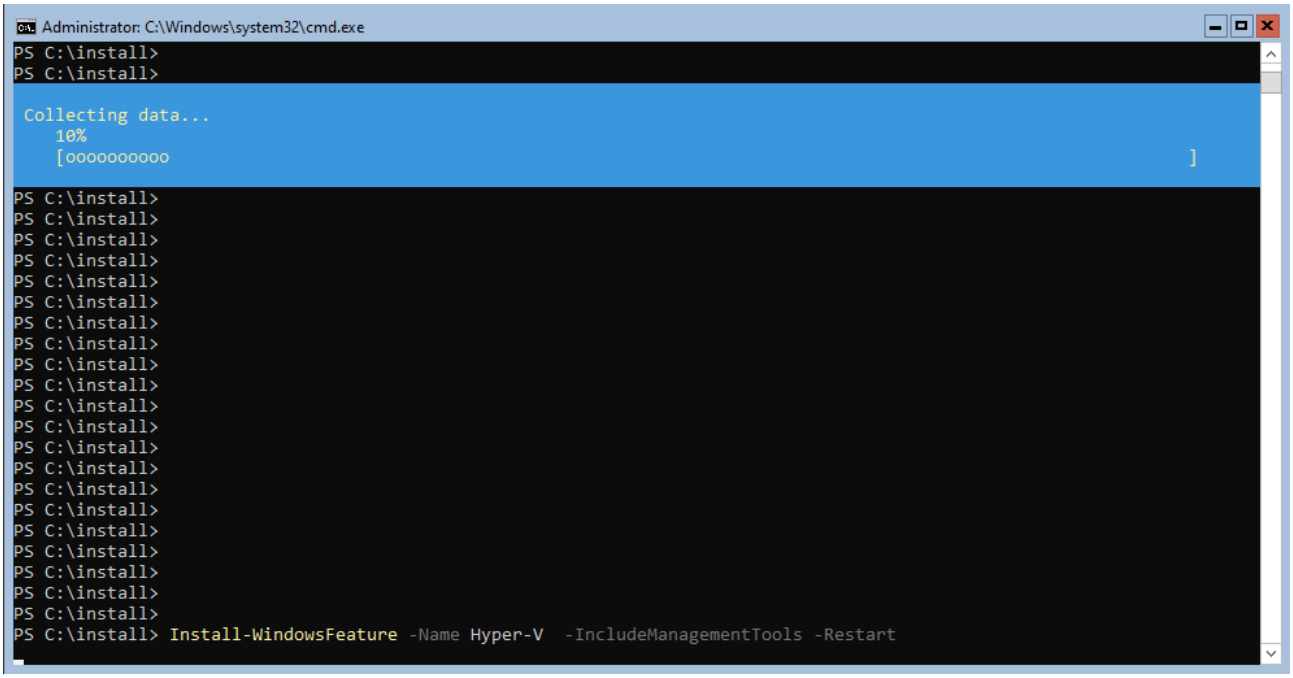

Рисунок 2.5 – Встановленням Hyper-V в Windows Server 2022 Core

Ця команда дозволяє швидко встановити та налаштувати роль Hyper-V на сервері, включаючи необхідні інструменти для його ефективного управління. Команда PowerShell Get-WindowsOptionalFeature використовується для отримання інформації про стан та наявність додаткових функцій в операційній

системі Windows. На рисунку 2.6 показано вивід даної команди при перевірці статусу сервісу Hyper-V.

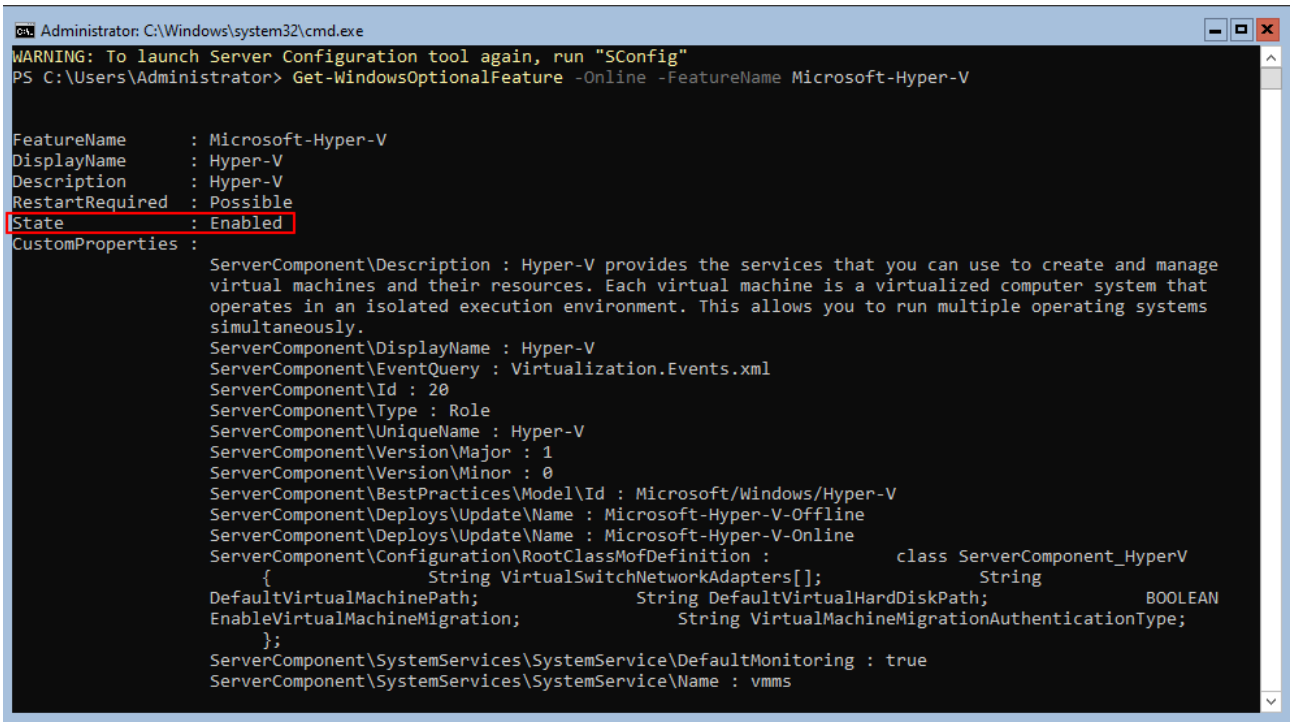

Рисунок 2.6 – Перевірка статусу сервісу Hyper-V в Windows Server 2022 Core

Ця команда надає інформацію щодо статусу функції Hyper-V в операційній системі, таку як її поточний стан.

Після встановлення роль Hyper-V і перезавантаження хоста попередня операційна система (див.рисунок 2.4) працюватиме на віртуальній машині (див.рисунок 2.7).

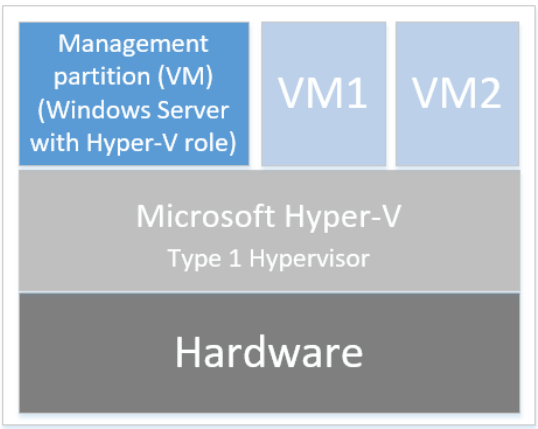

Рисунок 2.7 – Windows Server з роллю гіпервізора тип 1 Hyper-V

Windows Server 2022 Core вже працює не безпосередньо на апаратному забезпеченні, а всередині віртуальної машини - management partition

Мережа у віртуальному середовищі схожа на свою фізичну аналогію. Віртуальна машина management partition, так само як будь-яка віртуальна машина, може використовувати віртуальний мережевий адаптер, який підключається до віртуальної підмережі. Hyper-V прагне спростити взаємодію в мережі. Між віртуальною машиною та фізичним висхідним каналом існують два логічних рівні: віртуальний мережевий адаптер і віртуальний комутатор. Не існує складного інтерфейсу управління. Це більше схоже на логічний рівень абстракції, який фоново забезпечує мережеве підключення до віртуальних машин. Hyper-V надає три типи віртуальних комутаторів: External, Internal та Private. Вони майже ідентичні, основна різниця між ними полягає в можливості або відсутності доступу до розділу керування (host OS) та доступу до зовнішніх мереж.

Віртуальний комутатор External надає доступ до зовнішніх мереж через фізичні висхідні канали, як об’єднані, так і окремі мережеві карти (див.рисунок 2.8).

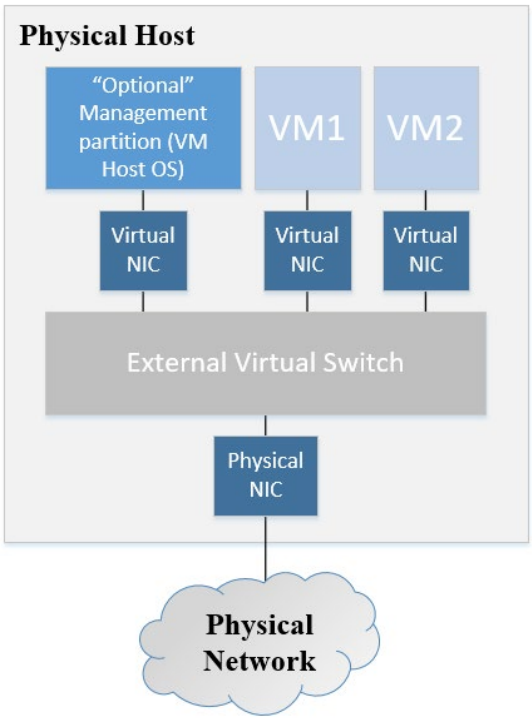

Рисунок 2.8 – Віртуальний комутатор External в гіпервізорі Hyper-V

Можна дозволити доступ до цього комутатора з управлінської операційної системи (Host OS). У цьому випадку Hyper-V автоматично створює новий віртуальний мережевий адаптер і підключає його до віртуального комутатора. Host-OS є ще однією віртуальною машиною, навіть якщо зовні вона виглядає як звичайна фізична інсталяція.

Віртуальний комутатор Internal забезпечує доступ між віртуальними машинами та Host OS (див.рисунок 2.9). Віртуальний комутатор Internal надає доступ до зовнішніх мереж через NAT.

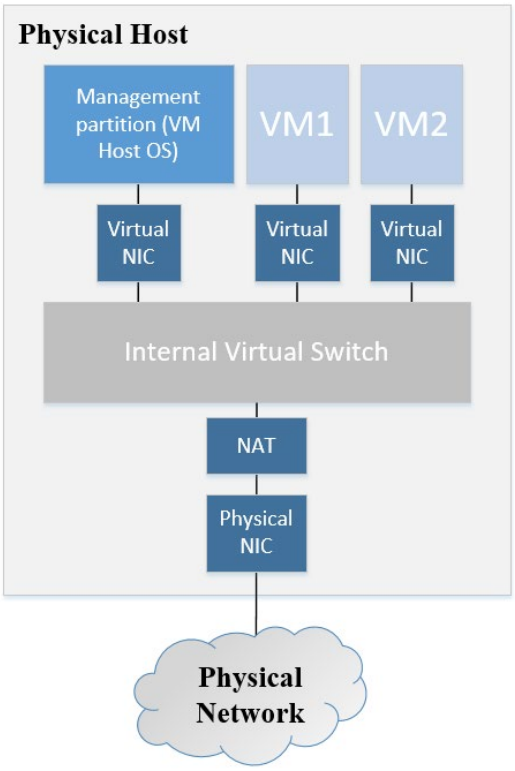

Рисунок 2.9 – Віртуальний комутатор Internal в гіпервізорі Hyper-V

Віртуальний комутатор Private ідентичний внутрішньому комутатору, але без доступу до Host OS (див.рисунок 2.10).

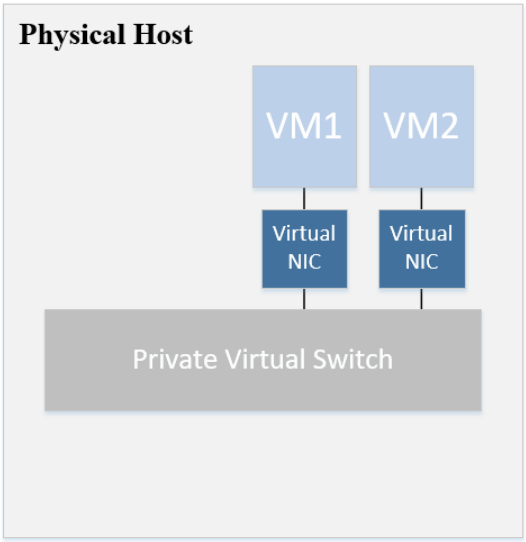

Рисунок 2.10 – Віртуальний комутатор Private в гіпервізорі Hyper-V

Створимо та налаштуємо віртуальні комутатори за допомогою PowerShell. Перед створенням віртуального комутатора потрібно знайти існуючі мережеві адаптери, запустивши командлет Get-NetAdapter. Визначити назву мережевого адаптера, який буде використовуватися для зовнішнього віртуального комутатора та комутатора для локальної мережі. Внутрішній комутатор не використовує фізичних мережевих адаптерів (див.рисунок 2.11).

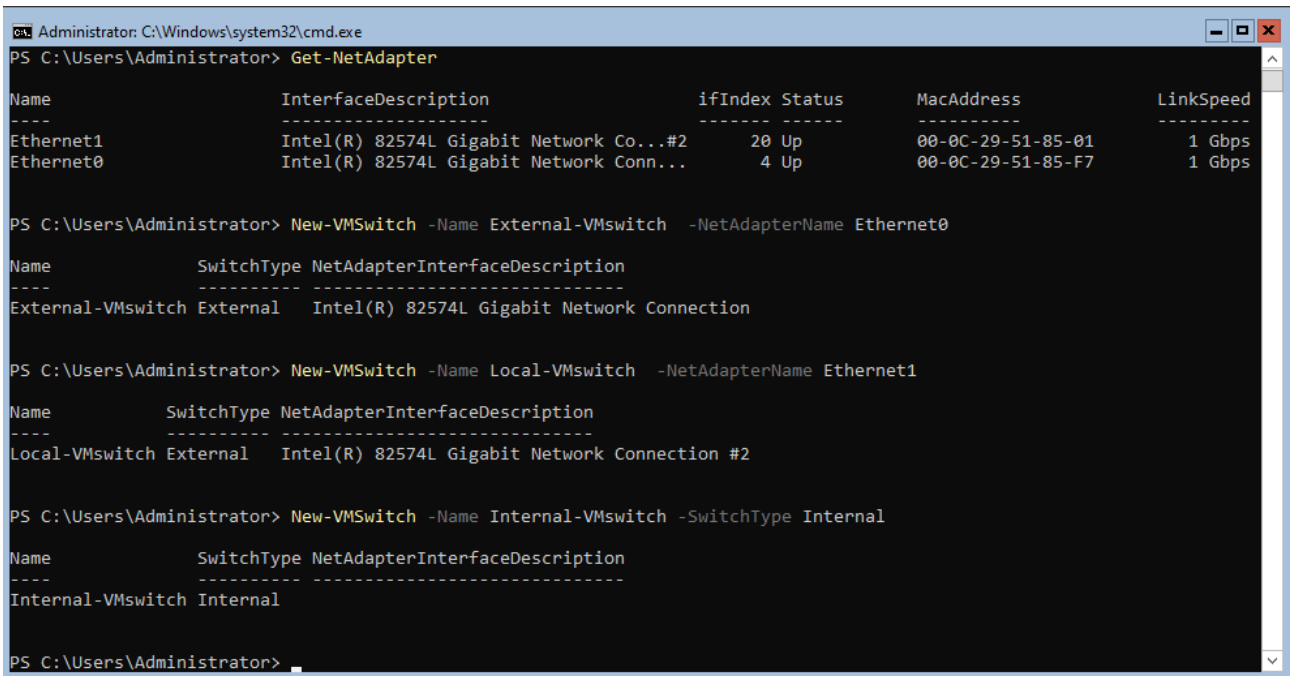

Рисунок 2.11 – Створення віртуальних комутаторів в Hyper-V

Віртуальний комутатор з назвою External-vSwitch, пов'язаний з фізичним адаптером Ethernet0 та зовнішньою мережею. Віртуальний комутатор Local-vSwitch, пов'язаний з фізичним адаптером Ethernet1 та локальною мережею. Неможливо призначити той самий фізичний мережевий адаптер для використання в кількох віртуальних комутаторах.

Віртуальний комутатор Internal-vSwitch з типом Internal не пов'язаний з жодним фізичним адаптером і використовується для внутрішньої комунікації між віртуальними машинами в межах гіпервізора Hyper-V.

При повторному виконанні команди Get-NetAdapter можна побачити що створено віртуальні мережеві адаптери (див.рисунок 2.12).

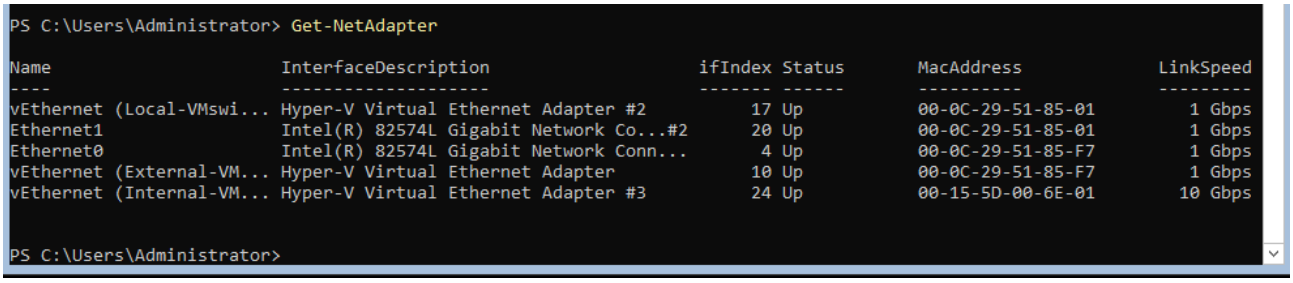

Рисунок 2.12 – Мережеві адаптери в Windows Server 2022 Core

Ці адаптери прив’язані до віртуальних комутаторів через які здійснюється мережева взаємодії віртуальних машин в середовищі Hyper-V.

2.4 Висновки до розділу

У другому розділі було розроблено схему лабораторного тестового середовища для створення віртуалізованої IT-інфраструктури з використанням гіпервізора Hyper-V. Встановлено та налаштовано Windows Server 2022 Core. Показано принцип взаємодії Windows Server 2022 Core та фізичного обладнання до та після встановлення гіпервізора Hyper-V. Встановлено та налаштовано гіпервізор Hyper-V. Проведено огляд мережі в віртуальному середовищі гіпервізора. Створено та налаштовано віртуальні комутатори за допомогою PowerShell.

РОЗДІЛ 3 РОЗГОРТАННЯ ТА ТЕСТУВАННЯ ВІРТУАЛІЗОВАНОЇ ІТ-ІНФРАСТРУКТУРИ

Здійснимо налаштування та тестування віртуалізованої ІТ-інфраструктури згідно схеми розробленої в пункті 2.1.

3.1 Встановлення та налаштування брандмауера IPFire

IPFire - це спеціалізований брандмауер, який можна встановити у будь-якій мережі включно з віртуалізованою [8]. Крім функцій брандмауера із перевіркою стану, він може виступати у ролі шлюзу VPN, аналізувати пакети даних за допомогою системи запобігання вторгненням (IPS). IPFire представляє собою повноцінну операційну систему, яка побудована на основі Linux і оптимізована для використання в якості брандмауера. Кожен компонент та програмний пакет, які використовуються, обираються розробниками і розробляються з їхніх власних джерел. Вони адаптовані для покращення безпеки системи та зменшення ризику атак. З метою забезпечення гнучкості IPFire не ґрунтується на інших дистрибутивах Linux.

Маршрутизатор IPFire використовує стандартні компоненти та пакети Linux, які були адаптовані для забезпечення безпеки. Налаштування цих модулів здійснюється через їхні конфігураційні файли. IPFire можна налаштовувати за допомогою веб-інтерфейсу користувача (WebUI), який реалізований кількома програмами у форматі cgi. Ці програми зберігають свій стан і конфігурацію у внутрішніх файлах, які переважно розташовані в каталозі /var/ipfire. Програми WebUI перевіряють правильність налаштувань та зберігають лише дійсні конфігурації. Вони також перетворюють ці внутрішні налаштування у стандартні файли conf.

Внутрішню конфігурацію IPFire перевіряє на узгодженість лише WebUI, і ручне редагування цих файлів може призвести до виходу системи з ладу.

IPFire надає ряд функцій для ефективної роботи в різноманітних мережевих середовищах з різними вимогами. Починаючи як простий маршрутизатор, він має глибокий аналіз пакетів, надає корисні звіти для керування мережею та виконує різноманітні мережеві послуги. Брандмауер IPFire, який є простим у використанні, але потужним, дозволяє створювати групи мереж, хостів та служб для визначення єдиного правила для великих частин мережі одночасно. З функціями обмеження швидкості та журналювання, він ідеально підходить для розміщення в віртуалізованих центрах обробки даних. Якість обслуговування визначає швидкість Інтернет-з'єднання, розподіляючи необхідну пропускну здатність для критичних застосунків, таких як VoIP, і забезпечуючи ефективний контроль користувачів. Система запобігання вторгненням перевіряє пакети, виявляючи відоме шкідливе програмне забезпечення та реагуючи на підозрілу поведінку, що робить мережу більш захищеною. Функціональність вебпроксі надає потужні можливості, такі як перевірка доступу, кешування вмісту та фільтрація URL для контролю доступу до вебресурсів. Функціональність VPN дозволяє створити VPN сервер за допомогою IPsec або OpenVPN, забезпечуючи безпечний доступ до IT-інфраструктури. Для захисту мережі від підроблення DNS, IPFire використовує внутрішній DNS-проксі, який використовує DNSSEC для фільтрації потенційно шкідливих атак та забезпечення безпеки спілкування з DNS-серверами вищого рівня.

Встановлення та налаштування брандмауера IPFire включає кілька кроків, які дозволяють створити віртуальний маршрутизатор в середовищі гіпервізора Hyper-V та забезпечити захист від несанкціонованого доступу.

На першому етапі створимо віртульну машину в гіпервізорі Hype-V з відповідними налаштуваннями мережі (див.рисунок 3.1).

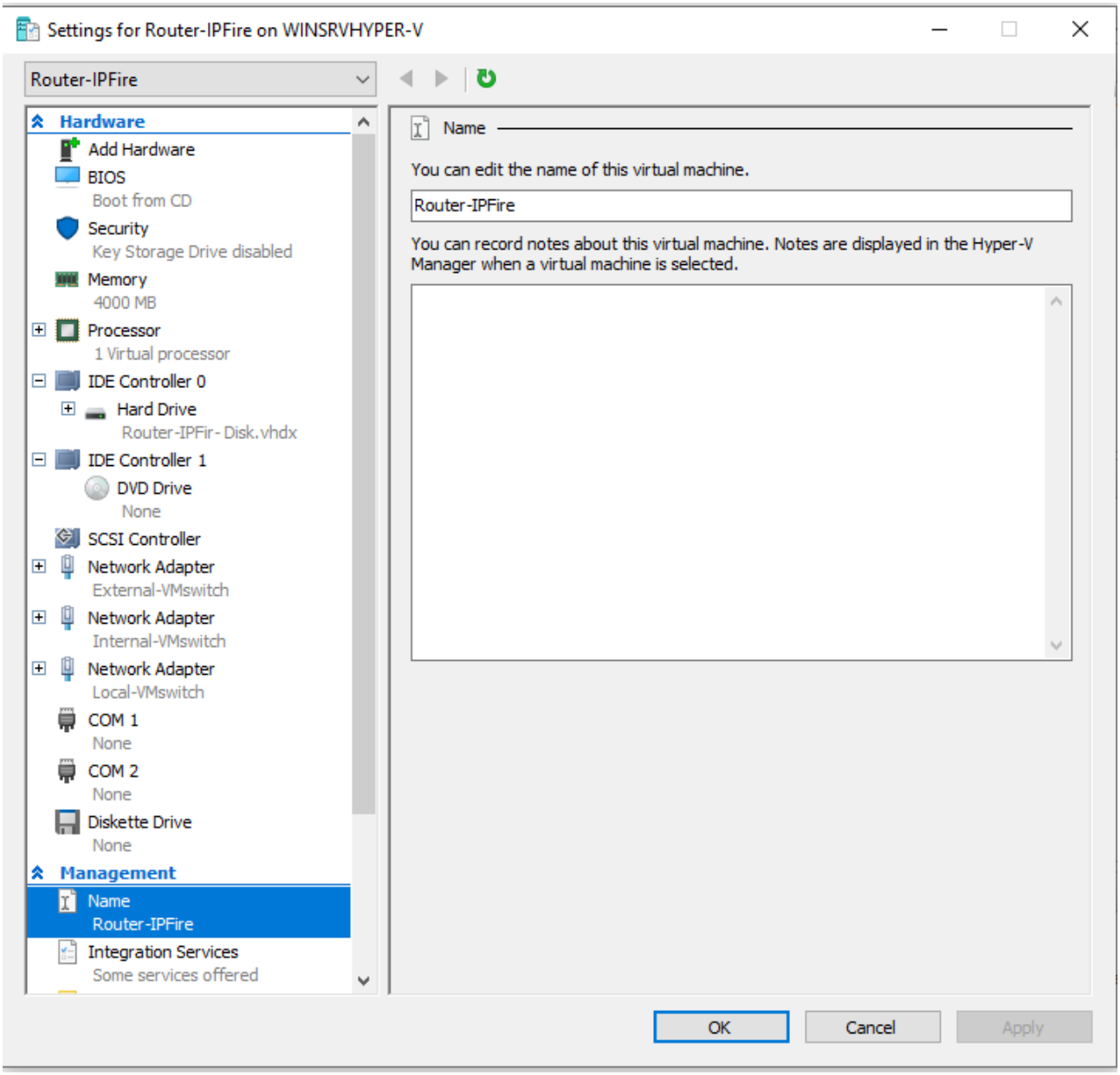

Рисунок 3.1 – Налаштування віртуальної машини Router-IPFire в гіпервізорі Hyper-V

Після встановлення та початкового налаштування зон (див.рисунок 3.2) можна приступати до налаштувань брандмауера, DHCP сервера та система запобігання вторгненням (IPS).

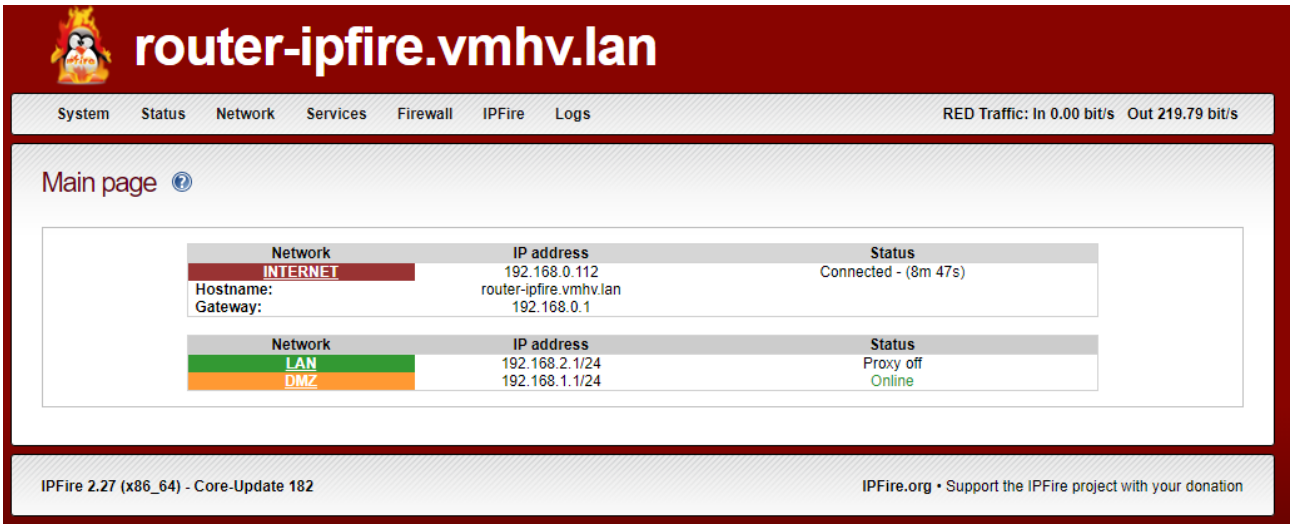

Рисунок 3.2 – Налаштування зон в IPFire

На головній сторінці вебінтерфейсу маршрутизатора IPFire можна побачити що маршрутизатор з іменем хоста router-ipfire.vmhv.lan має зовнішню IP-адресу 192.168.0.112 в зоні RED зі шлюзом за замовчуванням 192.168.0.1.

В параметрі LAN відображається IP-адреса для локальної мережі GREEN - 192.168.2.1/24. В зоні ORANGE відображається IP-адреса для демілітаризованої зони (DMZ) - 192.168.1.1/24.

На рисунку 3.3 показано налаштування NAT в маршрутизаторі IPFire.

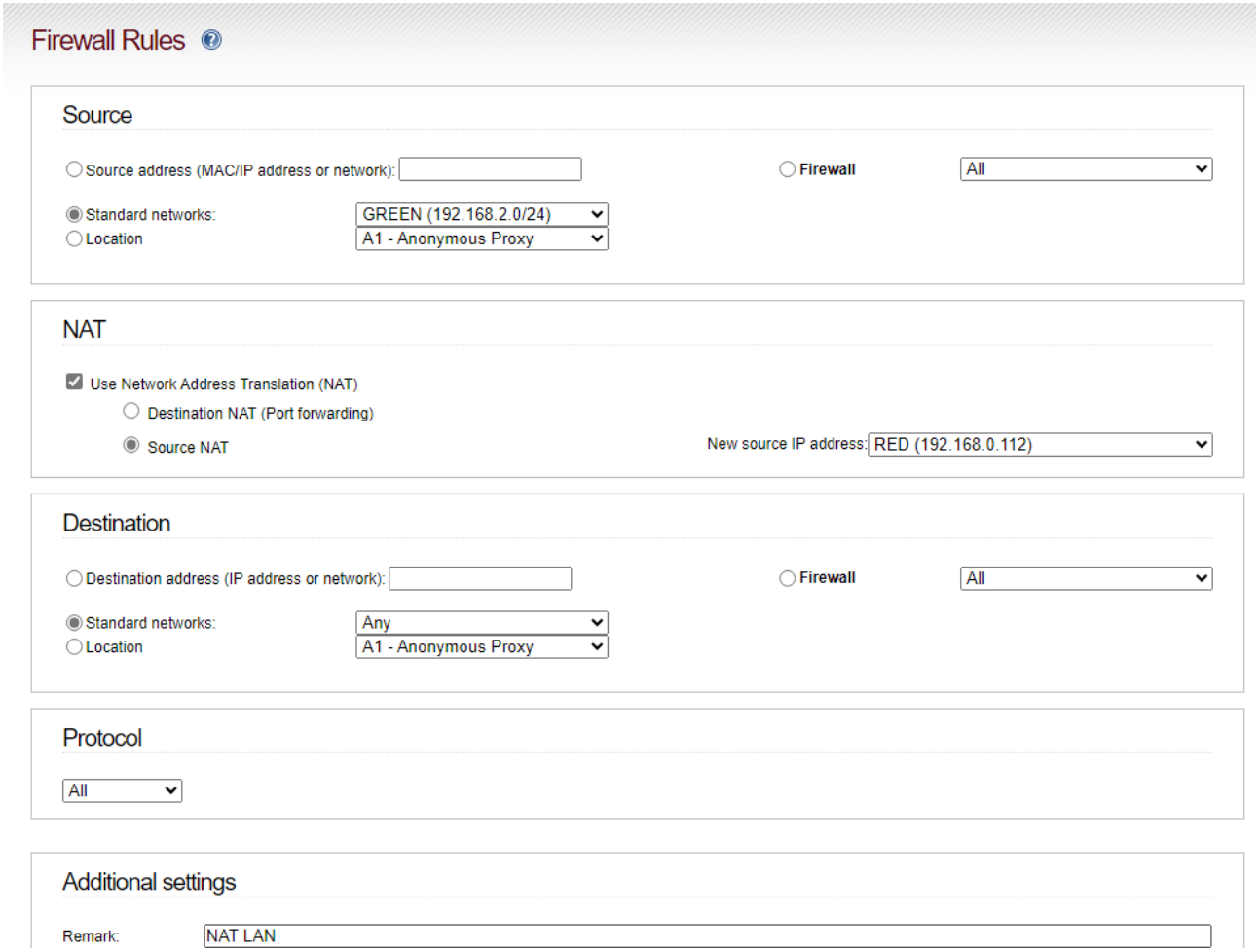

Рисунок 3.3 – Налаштування NAT в IPFire

Правило виконується для зони GREEN (192.168.2.0/24), що означає, що правило застосовується до вихідного трафіку з внутрішньої (зеленої) мережі маршрутизатора. Опція Use Network Address Translation відмічена, що активує використання NAT. Обрано Source NAT, що означає зміну джерела IP-адреси пакетів при проходженні через маршрутизатор. В параметрі New source IP address вказано RED (192.168.0.1.112), це нова IP-адреса, яка буде призначена пакетам, що виходять з мережі. Параметр Destination вибрано Any, що означає, що правило застосовується до трафіку, спрямованого до будь-якої мережі. Protocol встановлено All, що означає, що правило застосовується до всіх мережевих протоколів [9].

Ці налаштування використовуються для того, щоб забезпечити доступ в інтернет для пристроїв у локальній мережі, приховуючи їхні внутрішні IP-адреси за єдиною зовнішньою IP-адресою.

На рисунку 3.4 показано налаштування DHCP сервера в маршрутизаторі IPFire [10].

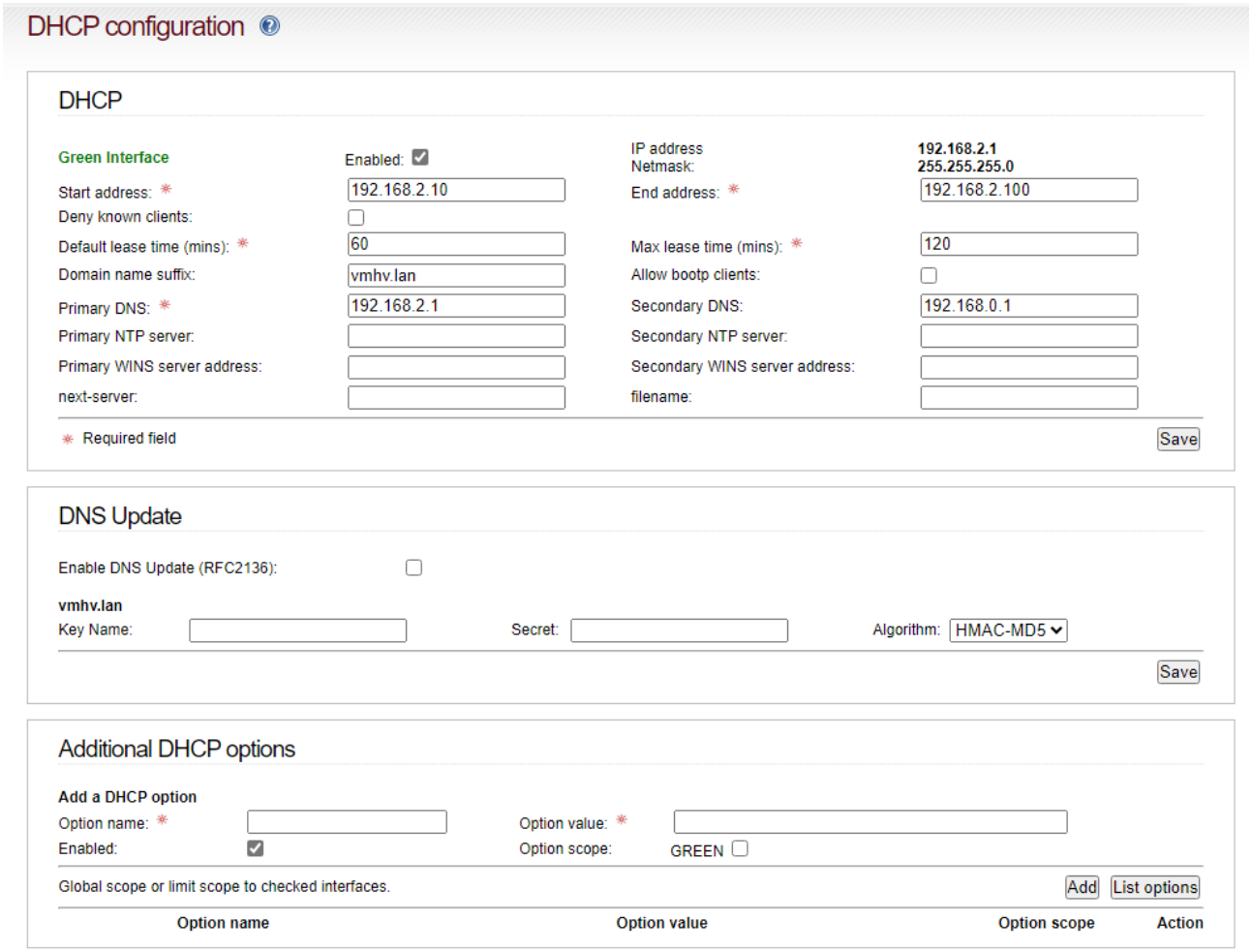

Рисунок 3.4 – Налаштування DHCP сервера в IPFire

Діапазон адрес, який використовується для зеленої (внутрішньої) мережі з 192.168.2.10 до 192.168.2.100 з маскою підмережі - 255.255.255.0. Стандартний час оренди IP-адреси - 60 хвилин. Максимальний час оренди IP-адреси - 120 хвилин. Доменне ім'я, яке додається до імені хоста - vmhv.lan. Основний DNS-сервер - 192.168.2.1 додатковий 192.168.0.1

IPFire використовує Suricata як IPS, що забезпечує ефективний та безпечний аналіз трафіку [11].

IPS може вжити заходів, якщо виявлено спробу вторгнення. Система запобігання вторгненням відстежує мережеву або системну діяльність для виявлення зловмисної активності. Якщо така активність виявляється, IPS

реєструє відповідну інформацію, повідомляє про це та може вживати заходів для блокування чи зупинення зазначеної небезпеки.

IPS у IPFire доповнює функціональність фільтрації пакетів, оскільки він не лише класифікує трафік за IP-адресою, протоколом і портом, але також аналізує самі пакети. Шляхом розшифрування протоколів, таких як DNS, HTTP та інші, IPS може отримати додаткову інформацію про трафік та виявляти непередбачувану поведінку. Пакети проходять через IPS перед тим, як потрапляти до механізму брандмауера.

На рисунку 3.5 показано налаштування IPS в маршрутизаторі IPFire.

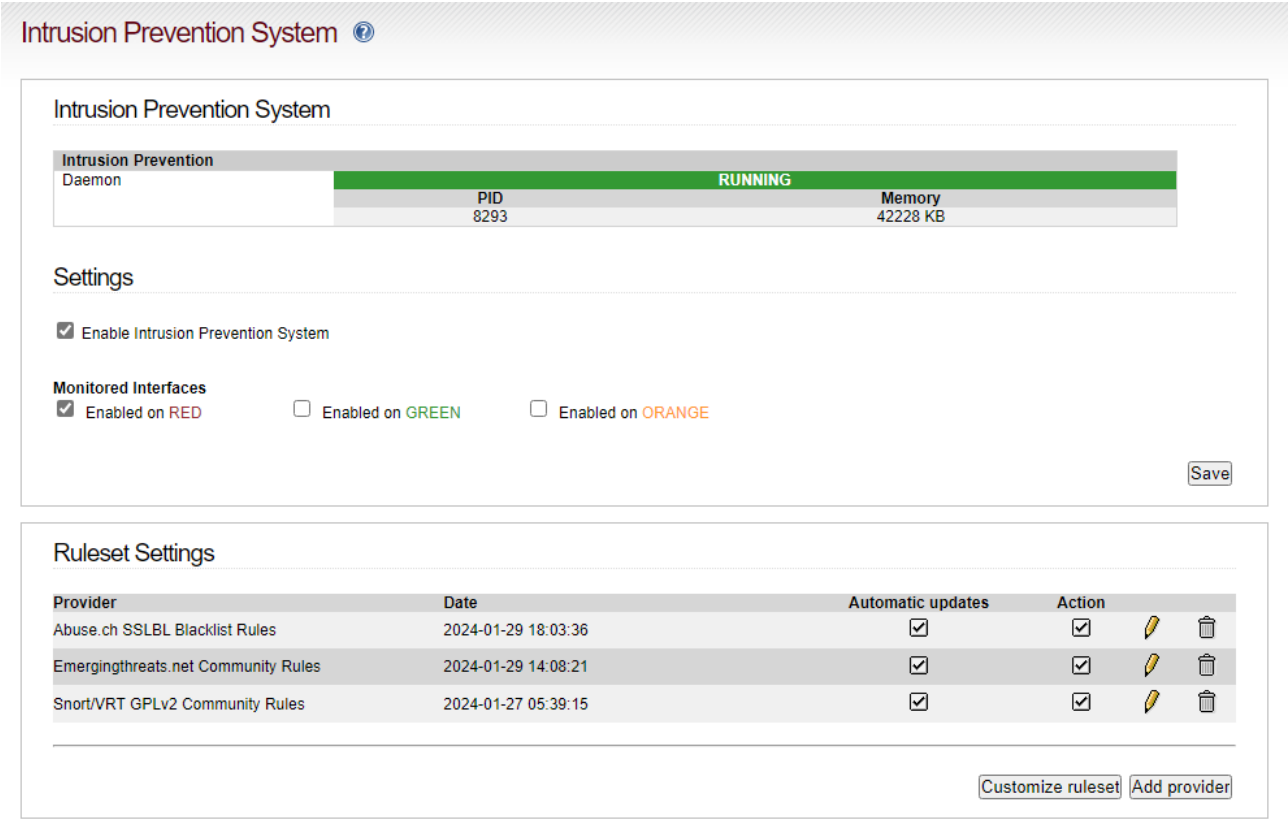

Рисунок 3.5 – Налаштування система запобігання вторгненням в IPFire

Склад правил є ключовим моментом IPS, оскільки він визначає, що піддається аналізу та яку шкідливу активність можна виявити. Ці правила, схожі на сигнатури антивірусних сканерів, вимагають регулярного оновлення для забезпечення ефективного виявлення нових загроз.

3.2 Встановлення та налаштування NAS Openmediavault

Openmediavault - це безкоштовна і відкрита операційна система для мережевого сховища. OMV забезпечує простий та ефективний спосіб налаштовування мережевого пристрою для зберігання даних та надає веб-інтерфейс для управління всією системою [12].

OMV має зручний веб-інтерфейс, який дозволяє користувачам легко налаштовувати та керувати різними аспектами NAS. Підтримує управління різними сховищами даних, RAID-масивами, а також можливість додавання нових жорстких дисків та їх конфігурація. Включає в себе різні мережеві служби, такі як SMB/CIFS (для обміну файлами в середовищі Windows), NFS (для обміну файлами в середовищі Unix або Linux), FTP та інші. OMV дозволяє налаштовувати резервне копіювання та відновлення даних для забезпечення їх безпеки.

На рисунку 3.6 показано етапи створення та запуску процедури встановлення віртуальної машини NAS Openmediavault в гіпервізорі Hype-V за допомогою PowerShell.

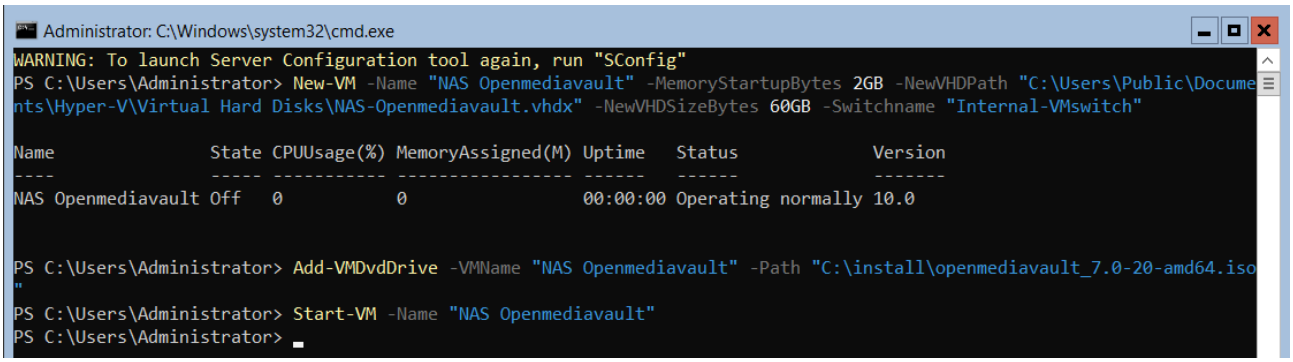

Рисунок 3.6 – Створення віртуальної машини NAS Openmediavault

Після встановлення можна приступати до налаштувань SMB та NFS служ для доступу до ресурсів NAS сервера. Налаштування буде здійснено за допомогою вебінтерфейсу керування NAS сервером (див.рисунок 3.7).

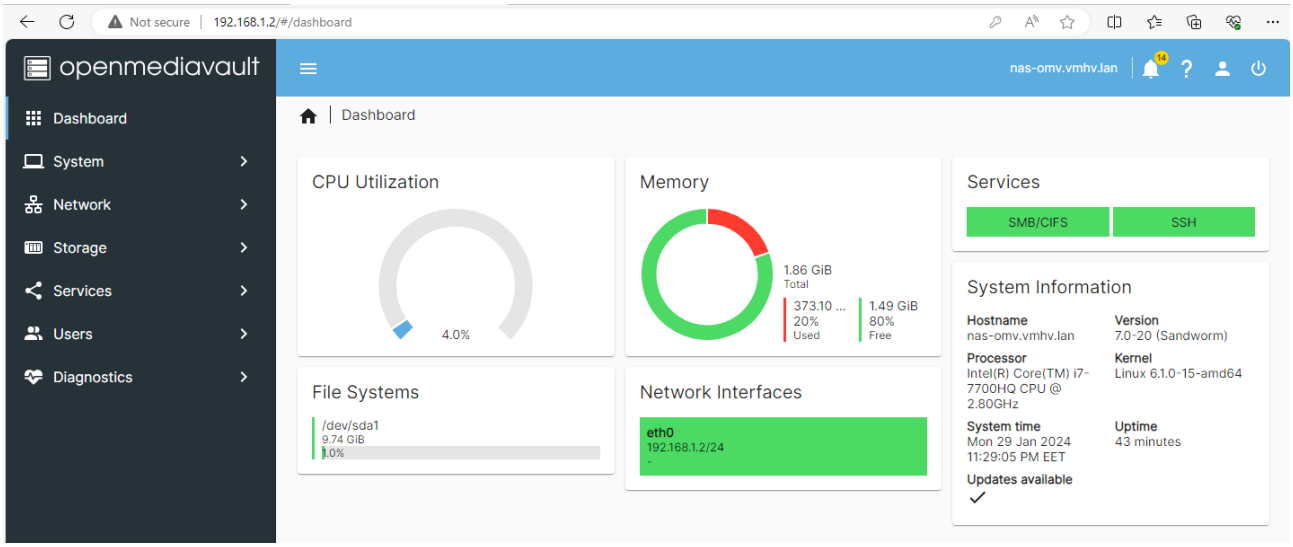

Рисунок 3.7 – Вебінтерфейс керування NAS сервером Openmediavault

На рисунку 3.8 показано налаштування доступу до загального ресурсу зберігання по протоколу SMB.

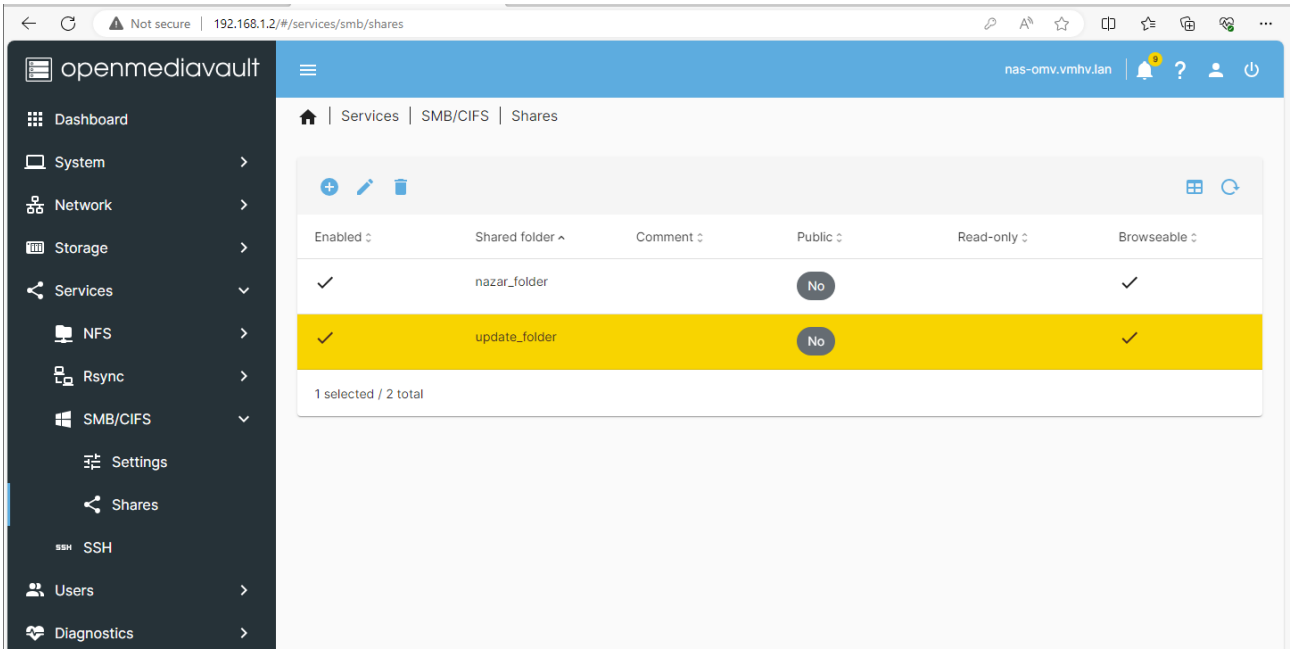

Рисунок 3.8 – Налаштування доступу до ресурсу зберігання по протоколу SMB.

Даний ресурс для обміну файлами буде також доступний по протоколу NFS для можливості підключення з Unix-подібних операційних систем.

3.3 Встановлення та налаштування Windows Server 2022 Desktop

Windows Server 2022 - це остання версія серверної операційної системи від Microsoft, спрямована на забезпечення надійного та ефективного управління серверними середовищами. Вона включає численні інновації та покращення, які роблять її відмінним вибором для корпоративних потреб. Інтеграція з хмарною платформою Azure полегшує взаємодію та управління хмарними ресурсами.

Операційна система має розширену підтримку віртуалізації і контейнеризації, включаючи підтримку Kubernetes. Це сприяє полегшенню розгортання та управління контейнеризованими додатками. Забезпечуючи покращені можливості масштабування та продуктивності, Windows Server 2022 підтримує новітні процесори та оптимізовану роботу з обсягами пам'яті. Інтеграція з Windows Admin Center дозволяє зручно управляти серверною інфраструктурою через вебінтерфейс. Розширені функції моніторингу та звітності допомагають ефективно відслідковувати та реагувати на події. Windows Server 2022 підтримує різні серверні ролі, такі як Active Directory, DNS, DHCP, Hyper-V та інші. Також вона включає підтримку TLS 1.3 для покращення безпеки мережевого зв'язку.

Windows Server 2022 включає вдосконалені функції для управління Active Directory, яка є основним елементом для керування ідентифікацією та доступом в корпоративних мережах. Active Directory є службою каталогів та ідентифікації, яка грає важливу роль в управлінні користувачами, групами, об'єктами та ресурсами в корпоративних мережах на основі Windows. Сервер може бути конфігурований як контролер домену, що використовує службу ADDS. Це дозволяє створювати та управляти доменами, об'єднуючи різні обчислювальні ресурси в єдиний ідентифікаційний простір. Це включає управління обліковим записом користувача, групами, політиками безпеки та іншими об'єктами Active Directory. Windows Server 2022 вдосконалив безпеку служби Active Directory. Active Directory в Windows Server 2022 підтримує різні можливості управління доменними об’єктами, включаючи управління груповою політикою, обліковим записом користувача та іншими параметрами. Сервер надає розширені

можливості моніторингу та журналювання подій для служби Active Directory, щоб ефективно виявляти та реагувати на події безпеки. Також є інструменти для резервного копіювання та відновлення об'єктів Active Directory, щоб забезпечити безпеку даних та відновлення системи в разі збою. Windows Server 2022 підтримує сучасні технології та підходи до роботи з ідентифікацією, включаючи використання мультифакторної аутентифікації та інші інновації.

На рисунку 3.9 показано етапи створення та запуску процедури встановлення віртуальної машини Windows Server 2022 ADDC в гіпервізорі Hype-V допомогою PowerShell [13].

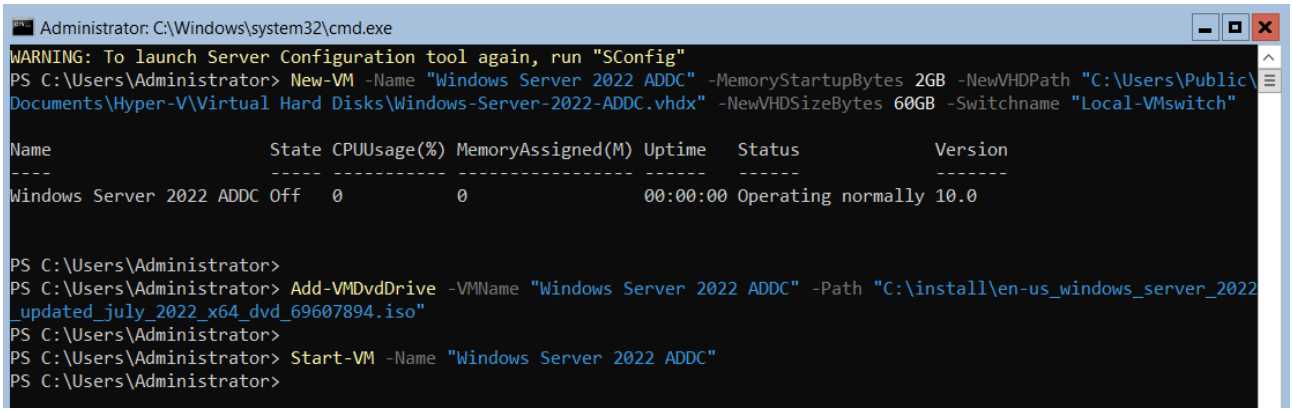

Рисунок 3.9 – Створення віртуальної машини Windows Server 2022 ADDC

Після встановлення Windows Server 2022 Desktop наступний етапом є встановлення доменних служб Active Directory і підвищення рівня сервера до контролера домену. На рисунку 3.10 показано встановлення ролі ADDS за допомогою команди в консолі PowerShell.

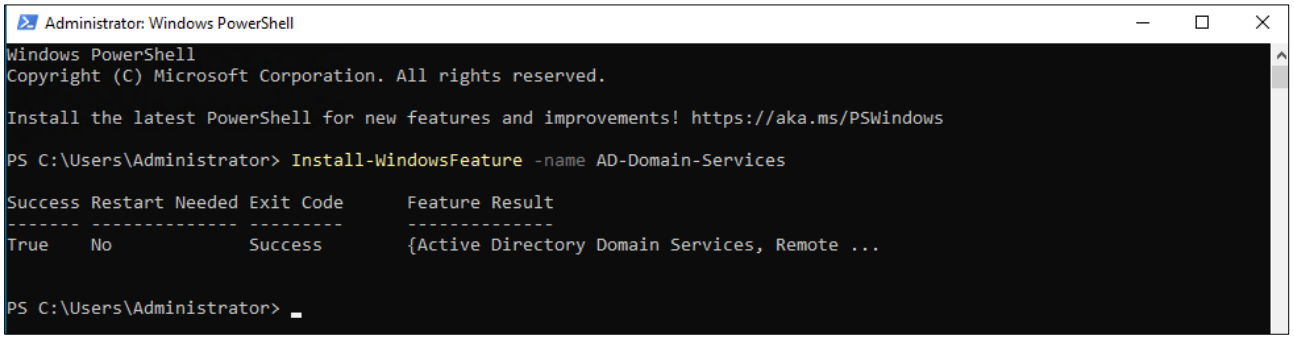

Рисунок 3.10 – Встановлення ролі ADDS в Windows Server 2022

Після встановлення ролі ADDS можна використати командлет PowerShell для розгортання нового домену (див.рисунок 3.11).

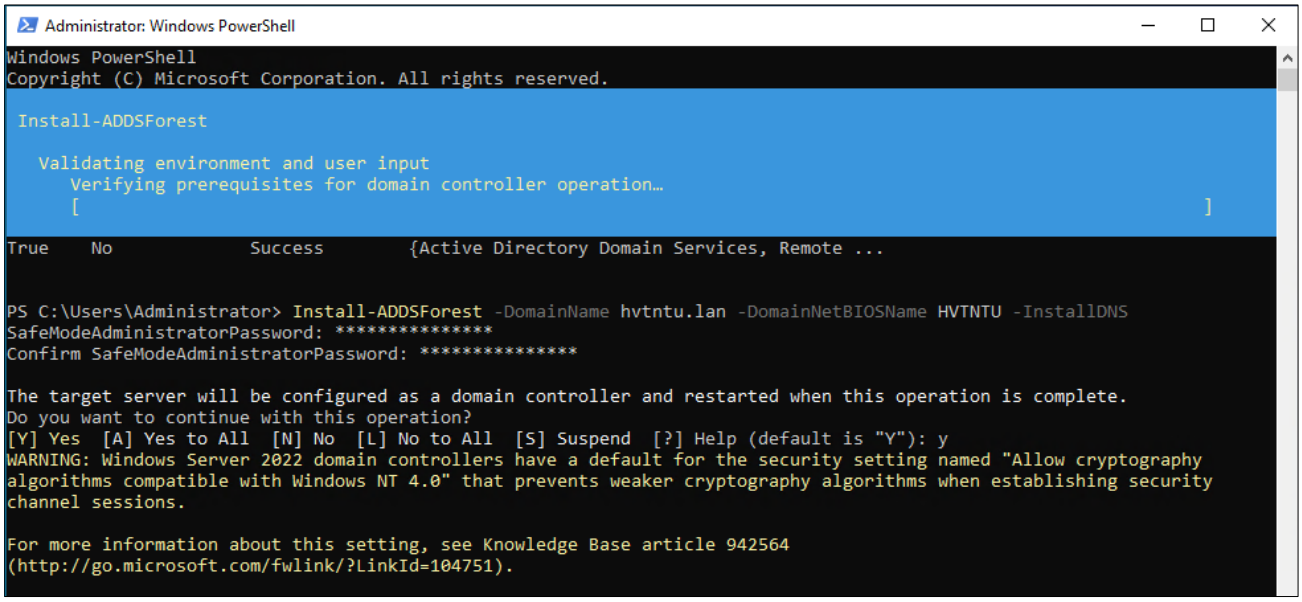

Рисунок 3.11 – Розгортання нового домену в Windows Server 2022

На рисунку 3.12 показано вивід команд, які використовуються для виявлення контролера домену в активному домені та конфігурацію мережі для інтерфейсів.

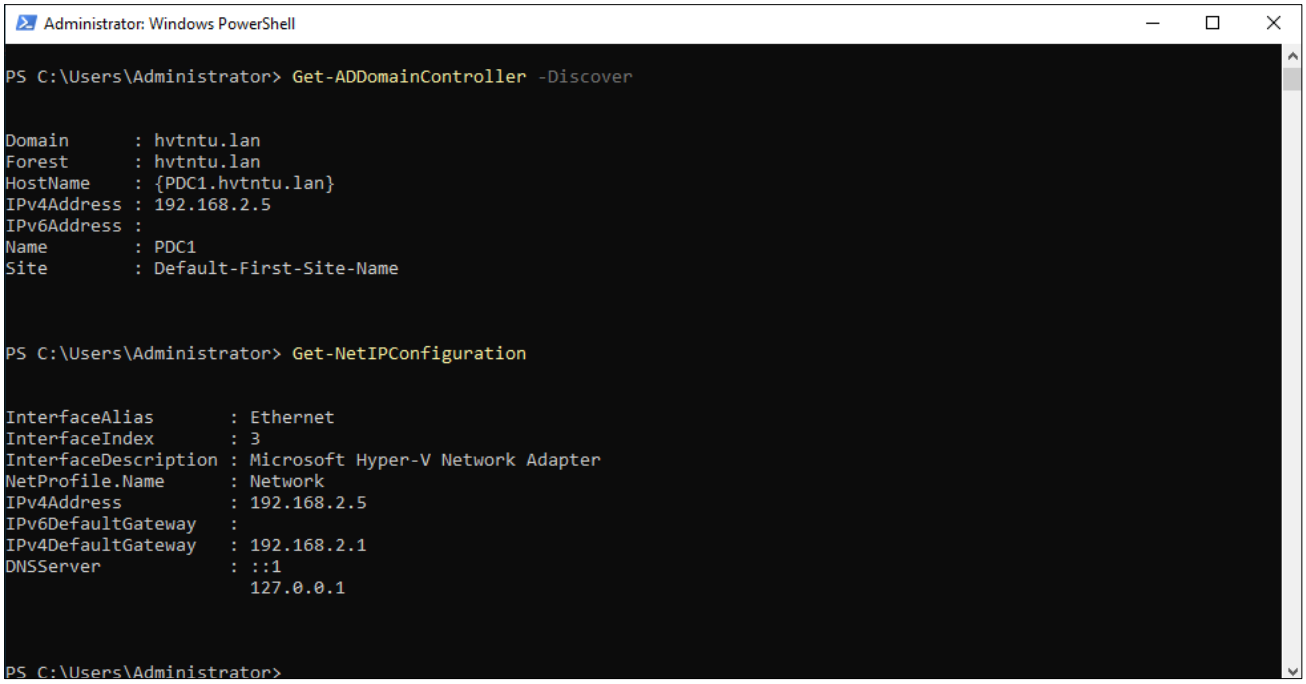

Рисунок 3.12 – Вивід команд Get-ADDomainController та Get-NetIPConfiguration

Вивід першої команди вказує на те, що доступний контролер домену має ім'я PDC1.hvntu.lan та знаходиться в локальній мережі з IP-адресою 192.168.2.5. Вивід другої команди вказує на те, що мережевий адаптер підключений до мережі та має IP-адресу 192.168.2.5 і шлюз 192.168.2.1. DNS сервер налаштований на адресу 127.0.0.1, що є локальною адресою хоста (localhost).

Виконаємо приєднання комп'ютер TestPC з Windows 10 до домену за допомогою PowerShell (див.рисунок 3.13).

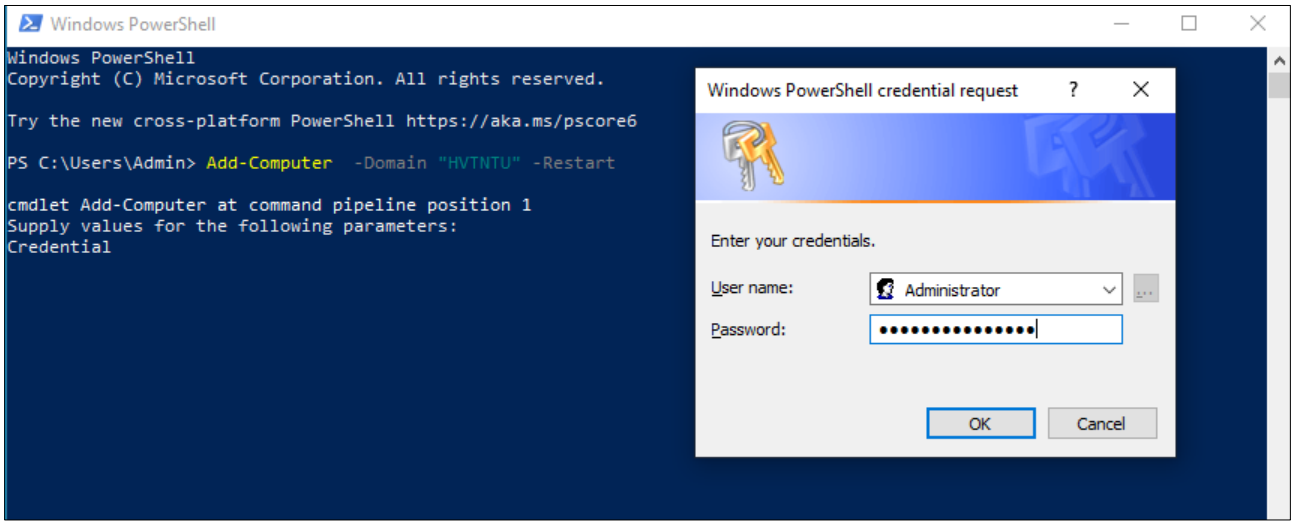

Рисунок 3.13 – Приєднання комп'ютер TestPC з Windows 10 до домену HVTNTU

Приєднання комп'ютера TestPC до домену є завершальним етапом створення віртуалізованої IT-інфраструктури.

3.4 Тестування віртуалізованої інфраструктури

Для тестування віртуалізованого середовища створимо користувача `nazar` в Windows Server 2022 та під'єднаємо каталог, який розміщений на NAS сервері як домашній каталог у вигляді диску Z в налаштуваннях профілю користувача (див рисунок 3.14).

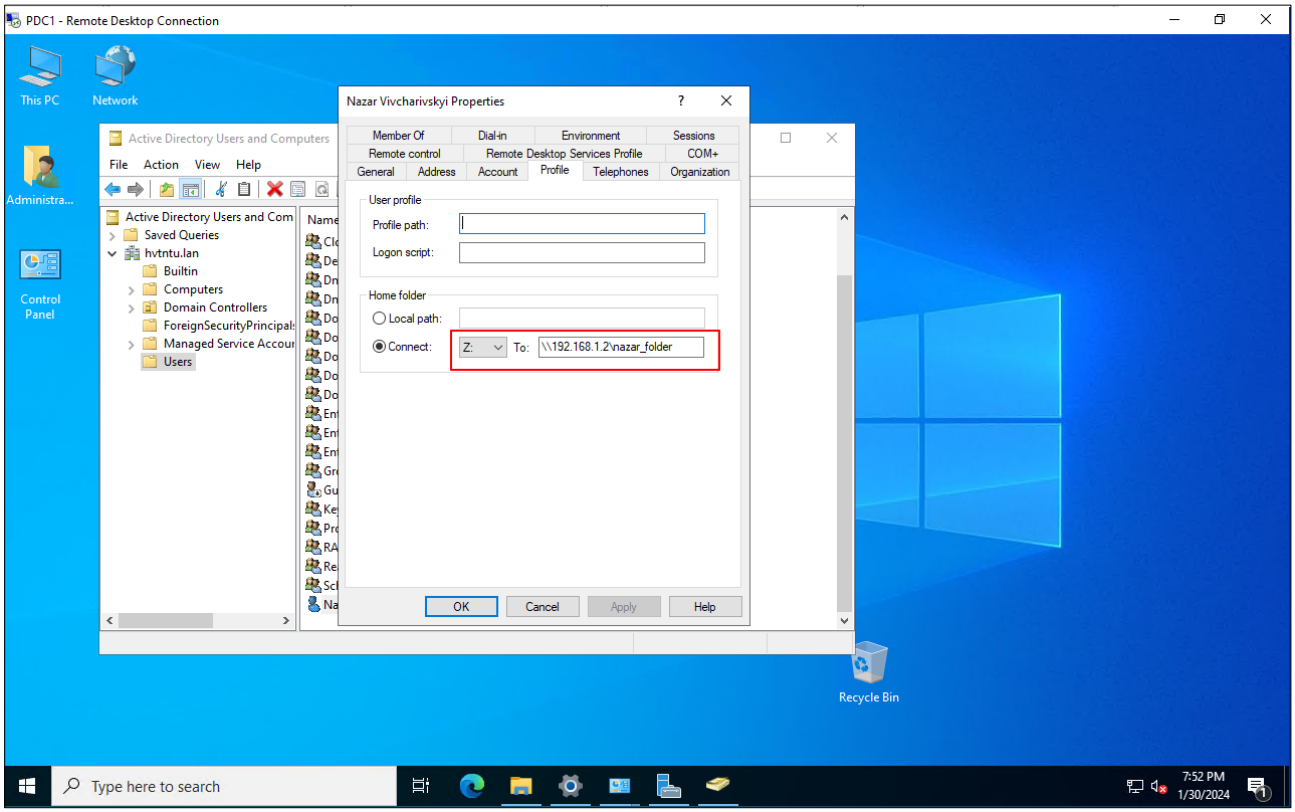

Рисунок 3.14 – Налаштування домашнього каталогу користувача `nazar`

Користувач також буде мати можливість підключення свого домашнього каталогу з Unix-подібних операційних систем по протоколу NFS або SMB.

При вході в операційну систему Windows 10 машини TestPC з логіном `nazar` буде здійснено автоматичне підключення домашнього каталогу у вигляді диску Z (див рисунок 3.15).

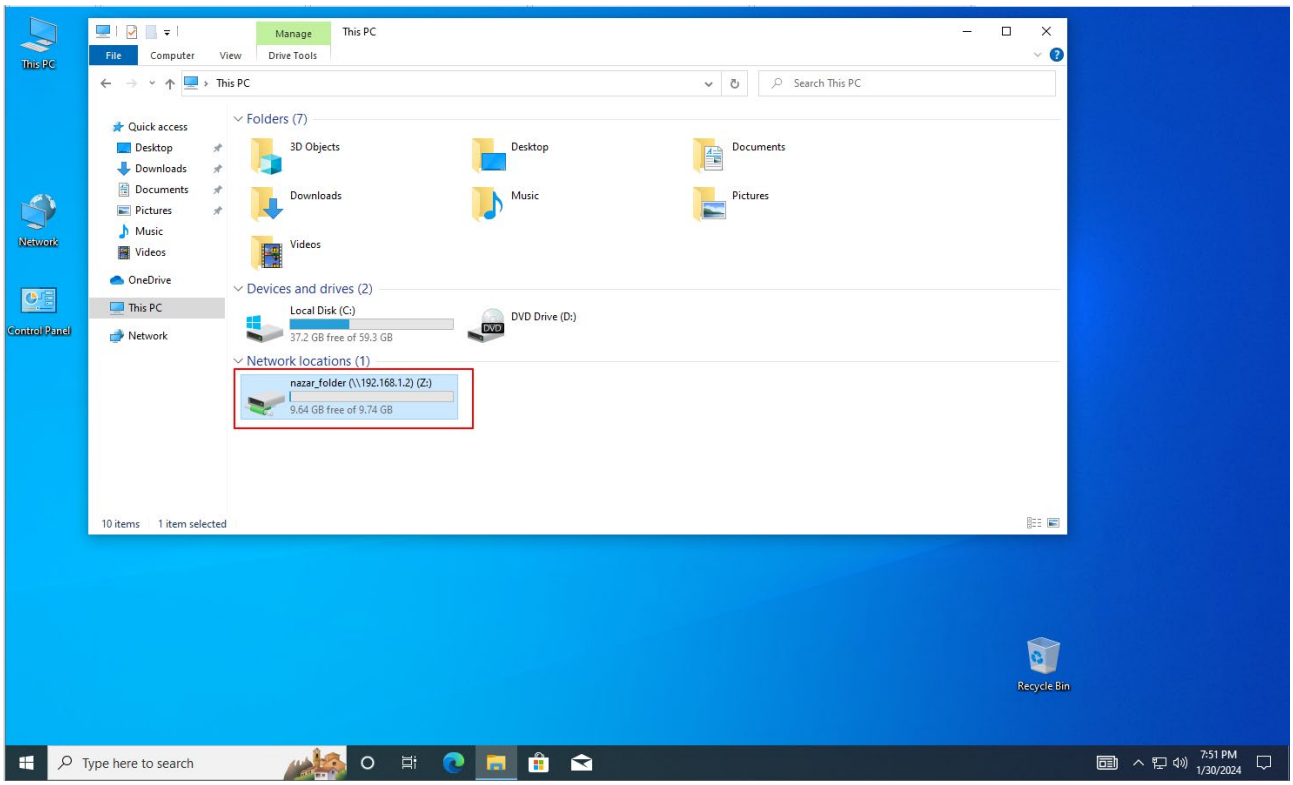

Рисунок 3.15 – Підключення домашнього каталогу користувача `nazar` в Windows 10

На рисунку 3.16 показано вікно командного рядка Windows 10 машини TestPC, де виконано команду ipconfig /all, яка надає детальну інформацію про всі мережеві інтерфейси на комп'ютері.

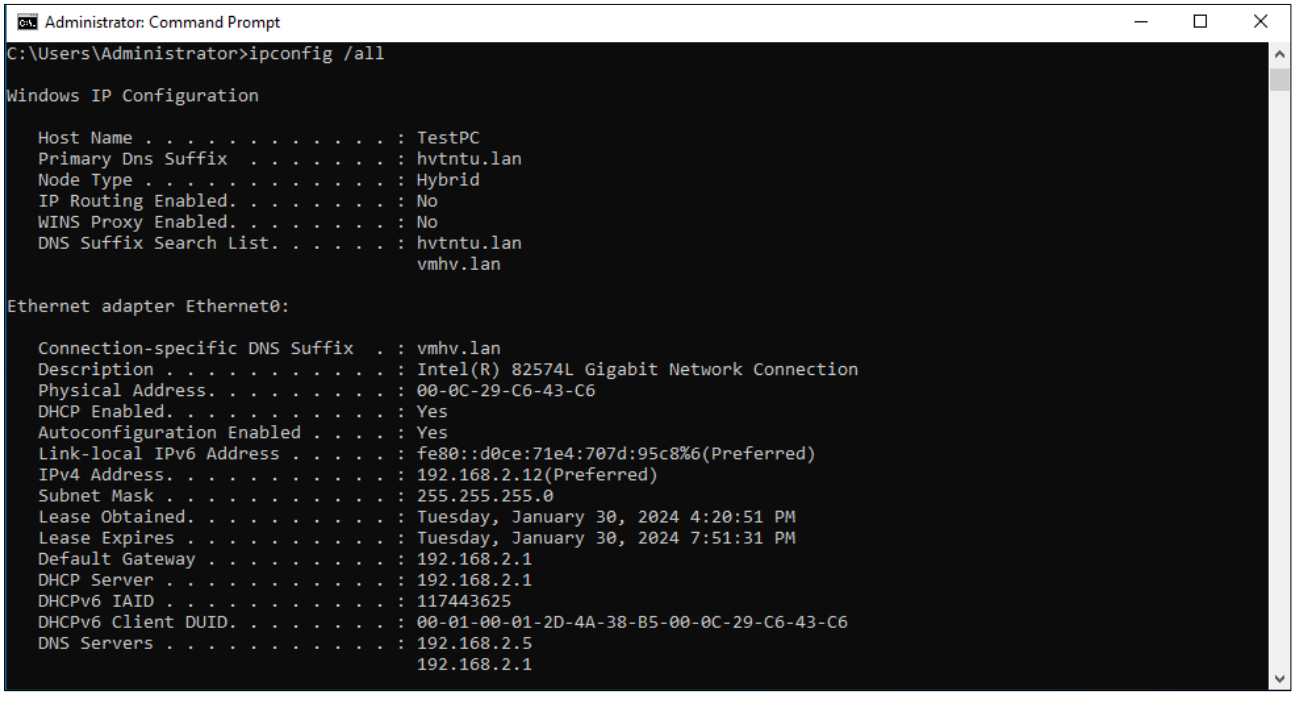

Рисунок 3.16 – Мережеві налаштування Windows 10 машини TestPC

Windows 10 отримав мережеві налаштування по DHCP з маршрутизатора IPFire. Налаштування включають IP-адреса, маску підмережі, шлюз, адресу DHCP та DNS серверів, що використовуються для підключення до мережі та доступу до інтернету. Перевірку доступу до мережі Інтернет здійснимо за допомогою утиліти PingPlotter (див рисунок 3.17).

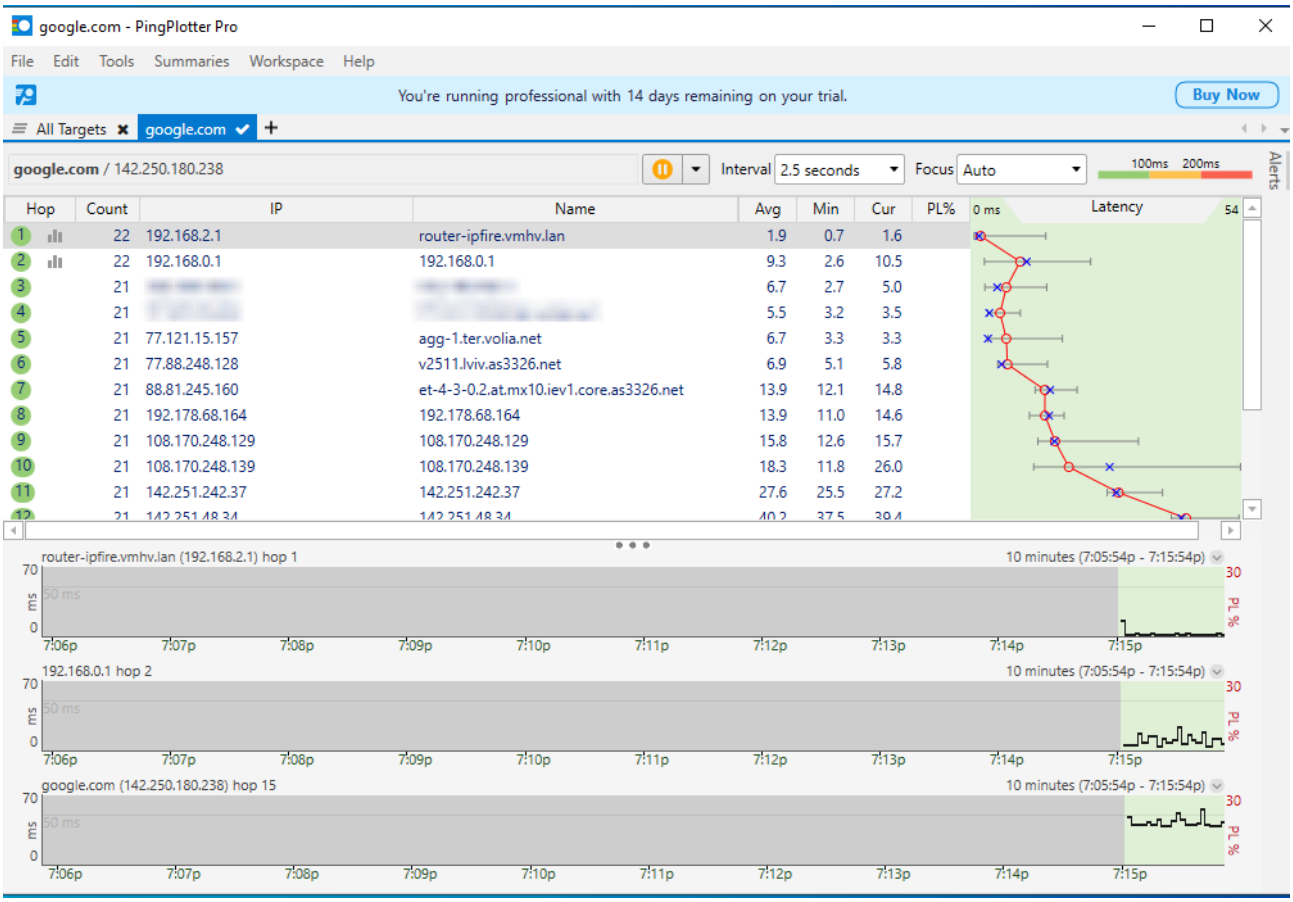

Рисунок 3.17 – Перевірка з’єднання з мережею Інтернет з Windows 10 машини TestPC

PingPlotter - це інструмент для візуалізації та моніторингу мережевого з'єднання, який дозволяє вивчати та відстежувати шлях пакетів у мережі.

Всі проведені тести підтверджують ефективність та коректну роботу віртуалізованої IT-інфраструктури на основі гіпервізора Hyper-V. Це свідчить про те, що обрані операційні системи та налаштовані сервіси працюють узгоджено та задовольняють вимоги щодо безпеки, маршрутизації, захисту та зберігання даних.

3.5 Висновки до розділу

В третьому розділі було виконано налаштування та тестування віртуалізованої IT-інфраструктури згідно розробленої схеми. Проведе встановлення та налаштування брандмауера IPFire. Налаштовано NAT, DHCP, DNS та систему запобігання вторгненням в маршрутизаторі IPFire. У віртуалізованому середовищі встановлено та налаштовано NAS Openmediavault з підтримкою протоколу SMB та NFS для доступу до сховища NAS. Встановлено та налаштовано Windows Server 2022 як контролер домену. Під’єднано до домену тестову машину з операційною Windows 10. Проведено тестування коректності роботи віртуалізованої IT-інфраструктури з тестової машини TestPC. Всі проведені тести підтвердили ефективність та коректну роботу віртуалізованої IT-інфраструктури на основі гіпервізора Hyper-V. Обрані операційні системи, такі як Windows Server 2022, маршрутизатор IPFire, NAS openmediavault, а також налаштовані сервіси NAT, брандмауер, ADDS, DHCP, DNS та SMB, взаємодіють коректно та забезпечують маршрутизацію, безпеку та надійне зберігання даних.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при тепловому ударі

Тепловий удар - це серйозний медичний стан, який виникає внаслідок перегрівання організму, зазвичай внаслідок тривалого перебування на сонці або у дуже спекотному середовищі. Це може призвести до серйозних ушкоджень органів і навіть може привести до смерті потерпілого.

Симптоми теплового удару можуть включати:

- висока температура тіла (понад 40°C);
- запаморочення, слабкість та втома;
- головний біль;
- червона, гаряча суха шкіра;
- швидке та поверхневе дихання;
- слабкість, запаморочення або втрата свідомості.

Долікарська допомога постраждалим при підозрі на тепловий удар є важливою процедурою, яку можуть виконувати особи без медичної освіти.

Наказ Міністерства охорони здоров'я України від 09.03.2022 р. № 441 " Про затвердження порядків надання домедичної допомоги особам при невідкладних станах" встановлює порядки надання домедичної допомоги постраждалим при підозрі на тепловий удар. У цьому порядку термін “тепловий удар” вживаються у такому значенні - невідкладний стан, викликаний дією високої температури навколишнього середовища, що спричиняє системні розлади у постраждалого [14].

Надання домедичної допомоги постраждалим при тепловому ударі передбачає такі кроки:

- переконатися, що немає небезпеки для себе, оточуючих та постраждалого, перед тим, як надавати допомогу;
- заспокоїти постраждалого та пояснити свої дії;
- викликати екстрену медичну допомогу та слухати інструкції диспетчера;

- перемістити постраждалого в прохолодне приміщення, щоб припинити дію тепла на нього;

- виміряти внутрішню температуру тіла постраждалого;

- використовувати методи охолодження, які доступні:

а) повністю занурити постраждалого у холодну воду (18-26 °C), якщо його внутрішня температура тіла перевищує 40°C, та продовжувати занурення, поки температура не знизиться до 39°C;

б) якщо повне занурення неможливе, можна використовувати пакети з льодом, обгорнуті у рушники, і накласти їх на тіло постраждалого. Можна також обдувати постраждалого вентиляторами або накласти вологі серветки на тіло.

- наглядати за постраждалим до прибуття медичної бригади;

- якщо постраждалий залишається свідомим, давати йому пити багато рідини;

- якщо стан постраждалого погіршується, повторно викликати екстрену медичну допомогу;

- зібрати інформацію про обставини виникнення теплового удару і передати її медичним працівникам при прибутті;

- якщо постраждалий втратив свідомість до прибуття медичної бригади, перейти до надання домедичної допомоги при раптовій зупинці кровообігу, відповідно до встановлених протоколів.

Це загальна послідовність дій, яку слід виконати, але завжди важливо дотримуватись інструкцій медичних фахівців та адаптувати допомогу до конкретної ситуації. Виконання цих кроків допоможе забезпечити постраждалому першу необхідну допомогу та зберегти його життя до прибуття медичних фахівців.

4.2 Вплив кольору на покращення умов праці та підвищення продуктивності праці

Кольори можуть впливати на наш настрій, емоційний стан та рівень енергії, що може впливати на продуктивність праці. Дослідження показують, що різні кольори можуть мати різний ефект на працівників залежно від їхньої праці та особистих вподобань.

Синій колір може знижувати агресію та стрес, знижувати пульс, а також підвищувати продуктивність. Він добре підходить для робочих місць, де потрібна концентрація, наприклад, в офісах, де працюють програмісти, адміністратори та інші працівники, що вимагають багато уваги та відповідальності.

Зелений колір є одним з найбільш заспокійливих кольорів, який може знижувати рівень стресу та покращувати настрій. Він добре підходить для робочих місць, де потрібна творчість, наприклад, у мистецьких або дизайнерських студіях.

Червоний колір може збільшувати енергію та стимулювати активність, але водночас може збільшувати рівень стресу та агресії. Він може бути використаний на робочих місцях, де потрібна енергія та активність, наприклад, у спортивних клубах або відділах продажу.

Жовтий колір може підвищувати настрій та енергію, але водночас може викликати відволікання та розсіювання уваги. Він може бути використаний на робочих місцях, де потрібна енергія та веселість, наприклад, у рекламних агентствах або креативних студіях.

Оранжевий колір може підвищувати енергію та стимулювати творчість, але водночас може викликати стрес та роздратування. Він може бути використаний на робочих місцях, де потрібна комунікація та спілкування, наприклад, у відділах клієнтського сервісу або у рекламних агентствах.

Фіолетовий колір може підвищувати концентрацію та творчість, але водночас може викликати меланхолію та депресію. Він може бути використаний

на робочих місцях, де потрібна креативність та концентрація, наприклад, у мистецьких або дизайнерських студіях.

Отже кольори можуть мати різний вплив на різні види діяльності та завдання. Наприклад, для робіт, що вимагають великої уваги та концентрації, можуть бути корисними більш спокійні та нейтральні кольори, такі як блідо-блакитний, блідо-зелений чи блідо-сірий. У той же час, для робіт, пов'язаних з креативністю та інноваціями, можна використовувати яскравіші та барвисті кольори, такі як помаранчевий, червоний чи жовтий, що можуть стимулювати творчий потенціал працівників.

Важливо також звернути увагу на сполучення кольорів на робочому місці. Комбінації кольорів можуть викликати різні емоції та впливати на настрій та продуктивність. Наприклад, сполучення зеленого та синього може знижувати стрес та підвищувати продуктивність, тоді як сполучення червоного та жовтого може викликати напругу та роздратування.

Також важливо зазначити, що вибір кольору для робочого місця повинен відповідати не тільки функціональності та емоційному стану працівників, але й бути відповідним з образом компанії та її бренду. Наприклад, якщо компанія має брендові кольори, то вони можуть бути використані для створення узгодженої атмосфери на робочому місці.

Крім того, важливо не перебільшувати вплив кольору на продуктивність працівників та не забувати про інші аспекти, що впливають на умови праці, такі як комфортне освітлення, правильна організація робочого місця та розміщення обладнання.

Отже, вибір кольору для робочого місця може мати значний вплив на умови праці та продуктивність працівників. Варто враховувати характеристики своєї роботи та особисті вподобання при виборі кольорів для робочого місця.

ВИСНОВКИ

У кваліфікаційній роботі було здійснено аналіз технологій віртуалізації, а також розроблено та налаштовано безпечну IT-інфраструктуру, використовуючи гіпервізор Hyper-V.

У першому розділі було розглянуто основні принципи віртуалізації та вплив цієї технології на управління та використання апаратного забезпечення. Проведено детальний огляд технології Hyper-V, здійснено аналіз та надано опис архітектури гіпервізора Hyper-V. Показано, що гіпервізор типу 1 від компанії Microsoft, Hyper-V, дозволяє ефективно використовувати ресурси фізичного сервера, надаючи можливість одночасно запускати та управляти багатьма віртуальними машинами на одному фізичному обладнанні. Відзначено, що апаратна підтримка віртуалізації (Intel VT-x і AMD-V) зменшує накладні витрати, покращує продуктивність віртуальних машин на платформі Hyper-V та забезпечує ефективну ізоляцію між ними, сприяючи зменшенню взаємовпливу.

У другому розділі була розроблена схема лабораторного тестового середовища для створення віртуалізованої IT-інфраструктури, використовуючи гіпервізор Hyper-V. Здійснено встановлення та налаштування Windows Server 2022 Core, показано принцип взаємодії цієї операційної системи та фізичного обладнання до та після встановлення гіпервізора Hyper-V. Виконано встановлення та конфігурування гіпервізора Hyper-V, проведено огляд мережі в віртуальному середовищі гіпервізора. Створено та налаштовано віртуальні комутатори з використанням PowerShell.

У третьому розділі було проведено налаштування та тестування віртуалізованої IT-інфраструктури відповідно до розробленої схеми. Було встановлено та налаштовано брандмауер IPFire, налаштовано NAT, DHCP, DNS та IPS в маршрутизаторі IPFire. У віртуалізованому середовищі було встановлено та налаштовано NAS Openmediavault з підтримкою протоколів SMB та NFS для доступу до сховища NAS. Також було встановлено та налаштовано Windows Server 2022 Desktop як контролер домену та під'єднано до домену тестову

машину TestPC з операційною системою Windows 10. Тестування коректності роботи віртуалізованої IT-інфраструктури було проведено з машині TestPC.

Результати тестів свідчать про те, що було успішно розроблено та налаштовано безпечну та функціональну віртуальну інфраструктуру, що включає в себе різноманітні сервіси та рішення для оптимального управління ресурсами та забезпечення потреб користувачів. Це може мати важливе практичне значення для подальшого використання в корпоративному середовищі або інших проектах, де важлива стабільність та безпека інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What are hypervisors. URL: https://www.ibm.com/topics/hypervisors (дата звернення: 24.01.2024).

2. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

3. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05.2024; Запоріжжя, Україна), 145-146. https://doi.org/10.62731/mcnd-24.05.2024.001

4. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170. https://doi.org/10.36074/logos-21.06.2024.034

5. Hyper-V architecture. URL: https://learn.microsoft.com/en-us/windows-server/administration/performance-tuning/role/hyper-v-server/architecture (дата звернення: 31.01.2024).

6. What is the Server Core installation option in Windows Server. URL: https://learn.microsoft.com/en-us/windows-server/administration/server-core/what-is-server-core x.html (дата звернення: 31.01.2024).

7. Install the Hyper-V role on Windows Server. URL: https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server (дата звернення: 31.01.2024).

8. IPFire Documentation. URL: https://www.ipfire.org/docs (дата звернення: 31.01.2024).

9. IPFire Firewall Documentation. URL: https://www.ipfire.org/docs/configuration/firewall (дата звернення: 31.01.2024).

10. IPFire DHCP Server. URL: https://www.ipfire.org/docs/configuration/network/dhcp (дата звернення: 31.01.2024).

11. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми Україна), 191-193. https://doi.org/10.62731/mcnd-14.06.2024.004

12. Openmediavault documentation. URL: https://docs.openmediavault.org/en/stable/index.html (дата звернення: 31.01.2024).

13. Nataliya Zagorodna, Iryna Kramar (2020). Economics, Business and Security: Review of Relations. Business Risk in Changing Dynamics of Global Village BRCDGV-2020: Monograph / Edited by Pradeep Kumar, Mahammad Sharif. India, Patna: Novelty & Co., Ashok Rajpath,. 446 p., pp.25-39.

14. Про затвердження порядків надання домедичної допомоги особам при невідкладних станах. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/z0356-22#n769 (дата звернення: 31.01.2024).