

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи моніторингу IT-
інфраструктури організації на базі рішень Icinga 2»

Виконав: студент 4-го курсу групи КБ-22-2

спеціальності 125 «Кібербезпека»

Ілля Берковський
Керівник: Старший викладач кафедри КІ та КБ

Ігор Фальковський

Рецензент: Доцент кафедри КІ та КБ, к.т.н., доцент

Юрій Россінський

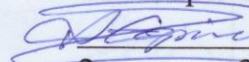
Житомир – 2026

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
2 лютого 2026 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Берковський Ілля Юрійович

Тема роботи: «Проект системи моніторингу IT-інфраструктури організації на базі рішень Icinga 2»

затверджена Наказом університету від 2 лютого 2026 р. № 58/с

Термін здачі студентом закінченої роботи 24 червня 2026 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Корпоративна IT-інфраструктура організації, що включає мережеве обладнання, сервери Windows і Linux, доменні служби, прикладний сервіс Nextcloud, базу даних MariaDB, систему резервного копіювання, pfSense, Suricata та систему моніторингу Icinga 2.

Обладнання та програмне забезпечення:

1. GNS3 2.2.55.
2. pfSense CE 2.8.1-RELEASE (amd64).
3. Cisco IOS image i86bi-linux-l2-adventerprisek9-15.2c.bin.
4. Windows Server 2022 Standard.
5. Ubuntu Server 24.04 LTS.
6. Icinga 2, Icinga Web 2, Icinga Director.
7. MariaDB, Docker, Docker Compose, Nginx, Nextcloud.
8. Suricata IDS/IPS.
9. SNMPv3, Icinga 2 Agent, Monitoring Plugins.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Доцент кафедри КІ та КБ, к.пед.н., доцент Олена ГОЛОВНЯ	02.02.2026	02.02.2026
2	Доцент кафедри КІ та КБ, к.пед.н., доцент Олена ГОЛОВНЯ	02.02.2026	02.02.2026
3	Доцент кафедри КІ та КБ, к.пед.н., доцент Олена ГОЛОВНЯ	02.02.2026	02.02.2026

Студент Ілля Берковський
Керівник Ігор Фальковський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	02.02.2026 08.02.2026	Виконано
2	Аналіз отриманого завдання	09.02.2026 22.02.2026	Виконано
3	Аналіз літературних джерел	23.02.2026 25.02.2026	Виконано
4	Оформлення 1 розділу пояснювальної записки	26.03.2026 29.03.2026	Виконано
5	Проектування архітектури моделі	30.03.2026 12.04.2026	Виконано
6	Вибір технологій та інструментів для реалізації	23.04.2026 26.04.2026	Виконано
7	Оформлення 2 розділу пояснювальної записки	27.04.2026 10.05.2026	Виконано
8	Підготовка необхідних компонентів для мережі	11.05.2026 24.05.2026	Виконано
9	Розгортання середовища та	25.05.2026	

	мережевої інфраструктури	29.05.2026	
10	Проведення базового налаштування мережі	01.06.2026 08.06.2026	Виконано
11	Налагодження засобів моніторингу та механізмів реагування	09.06.2026 15.06.2026	Виконано
12	Оформлення 3 розділу пояснювальної записки	16.06.2026 21.06.2026	Виконано
13	Підготовка доповіді та презентації	22.06.2026 23.06.2026	Виконано
14	Захист	24.06.2026	

Студент Ілля Берковський
Керівник Ігор Фальковський

КАКІДРБ-125-03-113

Дата	Зроблено	Підпис	Примітка
20.06.26	Спеціаліст І. Ю.		
23.06.26	Фальковський І.Г.		
24.06.26	Берковський І.Ю.		
24.06.26	Фальковський І.Г.		
24.06.26	Ілля Берковський		

Дія	Арх	Документ
1	3	15
ФІКТ, Гр. КБ-22-2		

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи на тему «Проект системи моніторингу IT-інфраструктури організації на базі рішень Icinga 2» містить 149 сторінок, 184 рисунки, 8 таблиць, 31 найменувань у списку використаних джерел, розміщених на 2 сторінках.

Метою кваліфікаційної роботи є проектування, реалізація та тестування системи моніторингу IT-інфраструктури організації на базі Icinga 2.

У роботі проаналізовано корпоративну IT-інфраструктуру як об'єкт моніторингу, розглянуто збої, експлуатаційні проблеми та підходи до контролю мережевих, серверних і прикладних компонентів. Виконано порівняльний аналіз систем моніторингу Icinga 2, Zabbix, Nagios та Prometheus і обґрунтовано вибір Icinga 2 для реалізації проекту.

У межах проектування визначено архітектуру IT-інфраструктури організації, VLAN-сегментацію, адресний простір, ролі серверних вузлів, політики доступу, резервне копіювання, захист мережевого периметра та модель моніторингу. Реалізація включає налаштування pfSense, Cisco Core L3 Switch, комутаторів доступу, Windows Server 2022 з ролями Active Directory, DNS і DHCP, Linux-серверів, Nextcloud, MariaDB, Backup-Server, Suricata IDS/IPS та Icinga2-Master-Server.

У системі моніторингу реалізовано контроль Windows Server 2022, Linux-серверів, Cisco-комутаторів, pfSense, Nextcloud, Docker-контейнера, MariaDB, backup-журналу та процесу Suricata. Проведене тестування підтвердило, що Icinga 2 коректно реагує на контрольовані збої та переводить сервіси у стани CRITICAL або DOWN.

Ключові слова: ICINGA 2, ICINGA WEB 2, ICINGA DIRECTOR, МОНІТОРИНГ, IT-ІНФРАСТРУКТУРА, PFSENSE, CISCO, VLAN, ACTIVE DIRECTORY, NEXTCLOUD, MARIADB, РЕЗЕРВНЕ КОПІЮВАННЯ, SURICATA.

					ККІКБ.КР.Б – 125 – 03 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Берковський І. Ю.		23.06.2023	Проект системи моніторингу ІТ-інфраструктури організації на базі рішень Icinga 2	Літ.	Арк.	Аркушів
Керівник		Фальковський І.Г.		23.06.2023			5	156
Реценз.		Росинський Ю.		23.06.2023		ФІКТ, Гр. КБ-22-2		
Н. контр.		Фальковський І.Г.		23.06.2023				
Затверд.		Єфіменко А.А.		23.06.2023				

ANNOTATION

The explanatory note for the bachelor's qualification work on the topic "Project of an Organization IT Infrastructure Monitoring System Based on Icinga 2 Solutions" contains 149 pages, 184 figures, 8 tables, 31 references listed on 2 pages.

The aim of the qualification work is to design, implement and test an IT infrastructure monitoring system for an organization based on Icinga 2.

The work analyzes corporate IT infrastructure as a monitoring object, considers failures, operational issues and approaches to monitoring network, server and application components. A comparative analysis of Icinga 2, Zabbix, Nagios and Prometheus is performed, and the choice of Icinga 2 for the project implementation is justified.

The design part defines the architecture of the organization's IT infrastructure, VLAN segmentation, IP addressing, server roles, access policies, backup, perimeter protection and the monitoring model. The implementation includes configuring pfSense, Cisco Core L3 Switch, access switches, Windows Server 2022 with Active Directory, DNS and DHCP roles, Linux servers, Nextcloud, MariaDB, Backup-Server, Suricata IDS/IPS and Icinga2-Master-Server.

The monitoring system provides control of Windows Server 2022, Linux servers, Cisco switches, pfSense, Nextcloud, Docker container, MariaDB, backup log and the Suricata process. The testing confirmed that Icinga 2 correctly responds to controlled failures and changes service states to CRITICAL or DOWN.

Keywords: ICINGA 2, ICINGA WEB 2, ICINGA DIRECTOR, MONITORING, IT INFRASTRUCTURE, PFSENSE, CISCO, VLAN, ACTIVE DIRECTORY, NEXTCLOUD, MARIADB, BACKUP, SURICATA.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РОЗДІЛ 1. АНАЛІЗ ТА ОБҐРУНТУВАННЯ ПОБУДОВИ СИСТЕМИ	
МОНІТОРИНГУ ІТ-ІНФРАСТРУКТУРИ	11
1.1. Аналіз корпоративної ІТ-інфраструктури як об'єкта моніторингу	11
1.2. Аналіз загроз, збоїв та експлуатаційних проблем ІТ-інфраструктури	13
1.3. Огляд сучасних підходів до моніторингу ІТ-інфраструктури	15
1.4. Порівняльний аналіз систем моніторингу з Icinga 2	17
Висновки до розділу 1	18
РОЗДІЛ 2. ПРОЄКТУВАННЯ ІТ-ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ ТА	
СИСТЕМИ ЇЇ МОНІТОРИНГУ	19
2.1. Проєктування загальної архітектури ІТ-інфраструктури організації	19
2.2. Проєктування мережевої інфраструктури та VLAN-сегментації	22
2.3. Проєктування доменної, серверної та прикладної інфраструктури	23
2.4. Проєктування політик доступу, резервного копіювання та захисту	
мережевого периметра	25
2.5. Проєктування системи моніторингу на базі Icinga 2	27
Висновки до розділу 2	29
РОЗДІЛ 3. РЕАЛІЗАЦІЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ СИСТЕМИ	
МОНІТОРИНГУ ІТ-ІНФРАСТРУКТУРИ	31
3.1. Реалізація мережевої та доменної інфраструктури	31
3.2. Реалізація клієнтських вузлів, адміністративної станції, серверних сервісів і	
резервного копіювання	46
3.3. Реалізація політик доступу, внутрішньої сегментації та захисту мережевого	
периметра	68
3.4. Реалізація системи моніторингу на базі Icinga 2	80
3.5 Реалізація заходів забезпечення кібербезпеки	97
3.6. Тестування та оцінка результатів реалізованої системи моніторингу	99
Висновки до розділу 3	105
ВИСНОВКИ	108
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	110

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ДОДАТКИ.....	112
ДОДАТОК А.....	113
ДОДАТОК Б.....	116
ДОДАТОК В.....	120
ДОДАТОК Г.....	125
ДОДАТОК Д.....	126
ДОДАТОК Е.....	128
ДОДАТОК Ж.....	130
ДОДАТОК К.....	132
ДОДАТОК Л.....	134
ДОДАТОК М.....	136
ДОДАТОК Н.....	140
ДОДАТОК П.....	142
ДОДАТОК Р.....	143
ДОДАТОК С.....	145
ДОДАТОК Т.....	148
ДОДАТОК У.....	151

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL — Access Control List
 AD DS — Active Directory Domain Services
 API — Application Programming Interface
 CPU — Central Processing Unit
 DHCP — Dynamic Host Configuration Protocol
 DNS — Domain Name System
 GNS3 — Graphical Network Simulator-3
 GPO — Group Policy Object
 HTTPS — HyperText Transfer Protocol Secure
 ICMP — Internet Control Message Protocol
 IDS — Intrusion Detection System
 IPS — Intrusion Prevention System
 IP — Internet Protocol
 LAN — Local Area Network
 NAT — Network Address Translation
 OID — Object Identifier
 RDP — Remote Desktop Protocol
 SNMP — Simple Network Management Protocol
 SSH — Secure Shell
 SVI — Switch Virtual Interface
 TCP — Transmission Control Protocol
 UDP — User Datagram Protocol
 VLAN — Virtual Local Area Network
 WAN — Wide Area Network
 ОС — операційна система
 ПЗ — програмне забезпечення
 СУБД — система управління базами даних

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сучасна IT-інфраструктура організації складається з великої кількості взаємопов'язаних компонентів: мережевого обладнання, серверів, доменних служб, баз даних, прикладних сервісів, систем резервного копіювання та засобів захисту периметра. Відмова одного з таких компонентів може вплинути на роботу інших сервісів і призвести до недоступності корпоративних ресурсів для користувачів.

Ручна перевірка стану окремих серверів, служб і мережевих пристроїв є неефективною, оскільки потребує багато часу та не дозволяє швидко визначити джерело проблеми. Особливо це важливо для сегментованої інфраструктури, де працездатність сервісів залежить від VLAN, маршрутизації, ACL, firewall-правил, доменних служб, прикладних компонентів і систем резервного копіювання. [1; 2; 3; 4] Тому актуальним є створення централізованої системи моніторингу, яка дозволяє контролювати стан усіх ключових вузлів і сервісів в одному середовищі.

Метою кваліфікаційної роботи є проєктування, реалізація та тестування системи централізованого моніторингу IT-інфраструктури організації на базі Icinga 2.

Визначена мета обумовлює такі завдання:

- проаналізувати корпоративну IT-інфраструктуру як об'єкт моніторингу;
- розглянути типові збої, експлуатаційні проблеми та підходи до моніторингу IT-інфраструктури;
- виконати порівняльний аналіз Icinga 2, Zabbix, Nagios та Prometheus;
- спроектувати архітектуру IT-інфраструктури організації з урахуванням VLAN-сегментації, серверних ролей, політик доступу, резервного копіювання та захисту периметра;
- реалізувати мережеву, доменну, серверну, прикладну та безпекову частини інфраструктури;
- розгорнути систему моніторингу на базі Icinga 2, Icinga Web 2 та Icinga Director; [5; 8; 9]
- реалізувати агентний моніторинг Windows- і Linux-серверів;

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

- реалізувати SNMP-моніторинг Cisco-комутаторів і pfSense;
- налаштувати перевірки Nextcloud, Docker-контейнера, MariaDB, backup-журналу та Suricata; [16; 24; 25; 26; 27]
- протестувати реакцію системи моніторингу на контрольовані збої.

Об'єктом дослідження є процеси функціонування, адміністрування та супроводу корпоративної IT-інфраструктури організації.

Предметом дослідження є методи, засоби та архітектурні підходи до побудови системи централізованого моніторингу IT-інфраструктури організації на базі Icinga 2.

У процесі виконання кваліфікаційної роботи було розроблено проєкт IT-інфраструктури організації та реалізовано систему її моніторингу на базі Icinga 2. Реалізована система контролює сервери Windows і Linux, мережеве обладнання Cisco, pfSense, Nextcloud, MariaDB, резервне копіювання та Suricata, а також перевіряє реакцію моніторингу на контрольовані збої.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ТА ОБҐРУНТУВАННЯ ПОБУДОВИ СИСТЕМИ МОНІТОРИНГУ ІТ-ІНФРАСТРУКТУРИ

1.1. Аналіз корпоративної ІТ-інфраструктури як об'єкта моніторингу

Сучасна корпоративна ІТ-інфраструктура являє собою сукупність взаємопов'язаних мережевих, серверних, програмних і клієнтських компонентів, які забезпечують роботу інформаційних сервісів організації. До її складу можуть входити маршрутизатори, комутатори, сервери автентифікації, служби DNS і DHCP, бази даних, прикладні сервіси, системи резервного копіювання, робочі станції користувачів та адміністративні вузли. Кожен із цих компонентів виконує окрему функцію, однак у реальних умовах вони працюють не ізольовано, а як єдина система. [1; 2]

Особливістю корпоративної інфраструктури є наявність значної кількості залежностей між її елементами. Наприклад, стабільна робота клієнтських комп'ютерів у доменному середовищі залежить від доступності контролера домену, DNS-служби, DHCP-служби та мережевої зв'язності між сегментами. Прикладні сервіси, своєю чергою, можуть залежати від бази даних, вебсервера, контейнерного середовища, файлової системи та правил міжмережевого доступу. Через це збій одного компонента може впливати на роботу одразу кількох сервісів.

У межах даної кваліфікаційної роботи розглядається інфраструктура, що містить граничний маршрутизатор pfSense, комутатор ядра Cisco Core L3 Switch, VLAN-сегментацію, сервер Windows Server 2022 з ролями Active Directory, DNS і DHCP, Linux-сервери для бази даних, прикладних сервісів і резервного копіювання, а також центральний сервер моніторингу Icinga2-Master-Server-1. Така структура відповідає типовій моделі невеликої або середньої корпоративної мережі, у якій поєднуються мережеві, серверні, доменні та прикладні служби. [14; 18; 20; 21; 22; 26; 27]

З погляду моніторингу така інфраструктура є складним об'єктом, оскільки вона складається з різномірних компонентів. Частина вузлів працює під керуванням Windows Server, частина — під керуванням Linux, окремо функціонує мережеве

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

обладнання Cisco та маршрутизатор pfSense. Для кожного типу вузлів потрібні різні способи контролю. Наприклад, доступність маршрутизатора або комутатора можна перевіряти за допомогою ICMP або мережевих портів, тоді як для серверів важливо контролювати не лише доступність, а й використання процесора, оперативної пам'яті, дискового простору, стан системних служб і прикладних процесів.

Ще однією важливою особливістю корпоративної IT-інфраструктури є її сегментованість. Використання VLAN дає змогу розділити мережу на логічні частини: серверний сегмент, клієнтський сегмент, адміністративну зону, сегмент моніторингу та інші підмережі. Це підвищує рівень безпеки, однак ускладнює контроль роботи системи. Для коректного функціонування інфраструктури необхідно стежити не лише за станом окремих вузлів, а й за доступністю взаємодії між сегментами, правильністю маршрутизації, роботою DHCP Relay, правилами firewall та ACL. [3; 17; 18]

Важливим аспектом є також централізоване адміністрування. У корпоративному середовищі адміністратор повинен мати змогу швидко визначити, який саме компонент спричинив проблему: мережеве обладнання, доменна служба, сервер бази даних, прикладний сервіс або система резервного копіювання. Без централізованого моніторингу така діагностика часто виконується вручну: через підключення до кожного вузла, перегляд журналів, запуск команд перевірки та аналіз стану служб. Це займає багато часу й підвищує ризик несвоєчасного виявлення несправності.

Отже, корпоративна IT-інфраструктура є багаторівневим і взаємозалежним об'єктом моніторингу. Її ефективний контроль потребує системи, яка здатна відстежувати стан мережевого обладнання, серверів, доменних служб, прикладних сервісів, резервного копіювання та ключових каналів доступу. Саме тому в межах роботи доцільним є створення централізованої системи моніторингу, яка об'єднує інформацію про стан усіх основних компонентів інфраструктури в єдиному середовищі.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

1.2. Аналіз загроз, збоїв та експлуатаційних проблем ІТ-інфраструктури

Під час експлуатації корпоративної ІТ-інфраструктури можуть виникати різні типи збоїв. Частина з них пов'язана з повною відмовою обладнання або сервісу, інша частина — з погіршенням продуктивності, неправильними налаштуваннями, нестачею ресурсів або порушенням взаємодії між компонентами. Саме тому моніторинг повинен виявляти не лише факт недоступності вузла, а й ознаки потенційних проблем.

Однією з найпоширеніших проблем є втрата мережевої доступності. Вона може бути спричинена помилками в налаштуванні VLAN, trunk-портів, access-портів, міжвланової маршрутизації, правил firewall або ACL. У сегментованій мережі сервер може залишатися працездатним, але бути недоступним із певного сегмента через некоректне правило доступу. Наприклад, якщо сервер моніторингу не має дозволу на звернення до контрольованих вузлів, система не зможе отримувати їхній стан, навіть якщо самі вузли працюють коректно. [17; 18]

Другою групою проблем є збої доменної інфраструктури. Active Directory, DNS і DHCP є базовими службами для Windows-середовища. У разі відмови DHCP клієнтські станції можуть не отримати IP-адресу, а при збоях DNS користувачі та сервіси можуть втратити можливість звертатися до ресурсів за іменами. Несправність Active Directory може призвести до проблем із входом користувачів у домен, застосуванням групових політик і доступом до корпоративних ресурсів. Тому для Windows Server 2022 необхідно контролювати не лише загальну доступність сервера, а й стан окремих критичних служб. [20; 21; 22]

Третьою важливою категорією є проблеми серверних ресурсів. До них належать перевантаження процесора, нестача оперативної пам'яті, переповнення дисків, збільшення навантаження на файлову систему або зупинка системних сервісів. Такі проблеми можуть не одразу призвести до повної відмови, але поступово погіршують роботу прикладних сервісів. Наприклад, нестача вільного місця на сервері бази даних може вплинути на роботу MariaDB, а проблеми з ресурсами Linux-App-Server-1 можуть призвести до нестабільної роботи Nextcloud.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Окрему увагу слід приділити прикладним сервісам. Для користувача важливо не лише те, що сервер відповідає на ping, а й те, що конкретний сервіс справді працює. Наприклад, Nextcloud може бути недоступним через зупинку Docker-контейнера, помилки Nginx, проблеми з HTTPS, відсутність з'єднання з базою даних або неправильні права доступу до файлів. Тому моніторинг повинен перевіряти не лише доступність сервера, а й стан окремих прикладних компонентів.

Важливою складовою надійності інфраструктури є резервне копіювання. Проблеми в роботі backup-системи часто залишаються непоміченими до моменту, коли виникає потреба у відновленні даних. До таких проблем належать невиконання скриптів резервного копіювання, помилки SSH-доступу, нестача місця на сервері Backup-Server-1, відсутність актуальних копій, пошкодження архівів або некоректне копіювання конфігурацій. Через це система моніторингу має враховувати стан резервного копіювання як один із ключових елементів стабільності всієї інфраструктури. [4]

Ще однією експлуатаційною проблемою є хибні спрацювання. Якщо система моніторингу неправильно оцінює стан служби, адміністратор отримує зайві попередження, що знижує довіру до системи. Наприклад, у Linux використання оперативної пам'яті може відображатися некоректно, якщо не враховувати кешування ядра. У таких випадках доцільно використовувати спеціалізовані плагіни або коректно налаштовувати порогові значення Warning і Critical.

Також значну роль відіграють проблеми прав доступу. Для повноцінного моніторингу агенту або плагіну можуть бути потрібні права на читання стану системних служб, Docker-контейнерів, файлових каталогів або служб Windows. Якщо такі права не налаштовані, перевірка може повертати помилку, хоча сам сервіс працює. Тому моніторинг потребує не лише встановлення програмного забезпечення, а й правильного налаштування дозволів, firewall-правил і політик безпеки. [2; 14; 23]

Отже, експлуатаційні ризики IT-інфраструктури охоплюють мережеві збої, відмови доменних служб, нестачу серверних ресурсів, проблеми прикладних сервісів, збої резервного копіювання, помилки доступу та хибні спрацювання. Для

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

своєчасного виявлення таких проблем необхідна централізована система моніторингу, яка дає змогу швидко отримувати інформацію про стан основних вузлів і сервісів.

1.3. Огляд сучасних підходів до моніторингу ІТ-інфраструктури

Моніторинг ІТ-інфраструктури може здійснюватися різними способами залежно від типу середовища, кількості вузлів, вимог до деталізації та обраної архітектури. Найпоширенішими підходами є безагентний моніторинг, агентний моніторинг, комбінований моніторинг, шаблонний підхід до налаштування перевірок і автоматизація розгортання агентів.

Безагентний моніторинг передбачає перевірку вузлів без встановлення додаткового програмного забезпечення на контрольовану систему. У такому випадку центральний сервер моніторингу виконує перевірки через мережу. Найчастіше використовуються ICMP-запити, TCP-перевірки портів, HTTP/HTTPS-запити або SNMP. Перевагою такого підходу є простота впровадження. Він добре підходить для контролю доступності маршрутизаторів, комутаторів, вебсервісів та інших вузлів, де достатньо перевірити факт доступності. [6; 10; 19]

Недоліком безагентного підходу є обмежена глибина контролю. Якщо сервер відповідає на ping, це ще не означає, що всі його служби працюють коректно. Так само відкритий порт не завжди гарантує правильну роботу прикладного сервісу. Тому безагентний моніторинг доцільно використовувати для перевірки зовнішньої доступності, але його недостатньо для повного контролю серверної інфраструктури.

Агентний моніторинг передбачає встановлення спеціального агента на контрольований вузол. Агент збирає локальну інформацію про стан операційної системи, ресурси, служби, процеси та інші параметри. Такий підхід дає змогу отримати значно більше даних, ніж проста мережева перевірка. Наприклад, для Windows Server 2022 можна контролювати стан служб Active Directory, DNS, DHCP, W32Time, завантаження процесора, використання пам'яті та дисків. Для

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Linux-серверів можна перевіряти системні ресурси, стан процесів, Docker-контейнерів, файлових систем і спеціалізованих сервісів. [5; 6; 7]

Найбільш доцільним для корпоративного середовища є комбінований підхід. Він поєднує зовнішні мережеві перевірки та внутрішній агентний моніторинг. Наприклад, сервер Windows може контролюватися агентом для перевірки системних служб, а доступність RDP може додатково перевірятися з боку центрального сервера моніторингу. Аналогічно Linux-сервер може передавати локальні метрики через агента, а його вебсервіс або контейнеризований застосунок може перевірятися окремо через HTTP або TCP.

Важливим підходом є використання шаблонів. У великих або навіть середніх інфраструктурах недоцільно вручну створювати однакові перевірки для кожного вузла. Натомість створюються шаблони для типових груп систем: Windows-серверів, Linux-серверів, мережевого обладнання, прикладних сервісів. Наприклад, усі Linux-сервери можуть успадковувати базовий набір перевірок CPU, RAM, disk, load average та доступності агента. Для окремих ролей можна додавати спеціалізовані перевірки: для сервера баз даних — MariaDB, для сервера додатків — Docker і Nextcloud, для backup-сервера — стан резервних копій. [6; 9]

Ще одним актуальним підходом є автоматизація розгортання моніторингу. Якщо агент налаштовується вручну на кожному вузлі, зростає ризик помилок. Тому доцільно використовувати сценарії встановлення, шаблони конфігурації, автоматичне створення сертифікатів або ticket-механізм для підключення агентів. У системах на базі Icinga 2 це особливо важливо, оскільки взаємодія між Master-сервером і агентами має бути захищеною.

Також важливою є централізація візуалізації. Система моніторингу повинна не лише виконувати перевірки, а й надавати адміністратору зручний інтерфейс для перегляду станів хостів і сервісів. Вебінтерфейс дає змогу швидко побачити, які вузли перебувають у стані OK, Warning, Critical або Unknown. Це спрощує діагностику та дозволяє швидше реагувати на інциденти. [8]

Таким чином, сучасний моніторинг IT-інфраструктури повинен поєднувати кілька підходів: мережеві перевірки, агентний збір метрик, шаблонне

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

налаштування, централізовану візуалізацію та автоматизацію підключення вузлів. Саме така модель є найбільш придатною для реалізованої інфраструктури, оскільки вона містить Windows- і Linux-сервери, мережеве обладнання, прикладні сервіси та систему резервного копіювання.

1.4. Порівняльний аналіз систем моніторингу з Icinga 2

Для реалізації системи моніторингу IT-інфраструктури необхідно обрати програмну платформу, яка відповідає вимогам проєкту. У межах роботи доцільно розглянути кілька поширених систем: Icinga 2, Zabbix, Nagios та Prometheus. Кожна з них має власну архітектуру, переваги та обмеження.

Nagios є одним із класичних рішень для моніторингу IT-інфраструктури. Його перевагою є велика кількість плагінів і тривала історія використання. Nagios добре підходить для перевірки доступності хостів і сервісів, а також для побудови базової системи сповіщень. Водночас його конфігурація може бути менш зручною для сучасних сценаріїв, де потрібна гнучка робота з шаблонами, агентами, вебінтерфейсом і масштабуванням. [12]

Zabbix є потужною платформою для централізованого моніторингу, яка має розвинений вебінтерфейс, власний агент, шаблони, графіки, тригери та механізми сповіщень. Він добре підходить для інфраструктур, де необхідно збирати багато метрик і будувати детальну аналітику. Недоліком Zabbix у межах даного проєкту може бути його більша комплексність, оскільки для поставленої задачі достатньо гнучкої системи перевірок, агентного моніторингу, вебінтерфейсу та зручного керування об'єктами. [11]

Prometheus орієнтований переважно на збір метрик і часові ряди. Він широко використовується в сучасних середовищах, особливо для контейнеризованих застосунків, Kubernetes та мікросервісної архітектури. Його сильними сторонами є робота з метриками, інтеграція з Grafana та зручність для DevOps-сценаріїв. Водночас Prometheus менш орієнтований на класичну модель моніторингу інфраструктури з хостами, сервісами, агентами Windows/Linux, станами OK/Warning/Critical та традиційними перевітками мережевого обладнання. [13]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Icinga 2 є сучасною системою моніторингу, яка розвинулася з ідей Nagios, але має більш гнучку архітектуру. Вона підтримує моніторинг хостів і сервісів, агентну модель, перевірки через плагіни, шаблони, правила застосування сервісів, вебінтерфейс Icinga Web 2 та керування конфігурацією через Icinga Director. Для даного проєкту важливо, що Icinga 2 дозволяє поєднати моніторинг Windows Server, Linux-серверів, мережевого обладнання, Docker-контейнерів і прикладних сервісів у межах однієї системи. [5; 6; 7; 8; 9]

Висновки до розділу 1

У першому розділі було проаналізовано корпоративну IT-інфраструктуру як об'єкт моніторингу. Встановлено, що така інфраструктура складається з взаємопов'язаних мережевих, серверних, доменних, прикладних і клієнтських компонентів. Через наявність залежностей між вузлами збій одного елемента може впливати на роботу кількох сервісів одночасно, тому ручний контроль стану системи є недостатнім.

Розглянуто основні загрози, збої та експлуатаційні проблеми IT-інфраструктури. До них належать втрата мережевої доступності, помилки VLAN і маршрутизації, відмови DNS, DHCP та Active Directory, нестача серверних ресурсів, збої прикладних сервісів, проблеми резервного копіювання, помилки прав доступу та хибні спрацювання моніторингу. Це підтверджує необхідність централізованого контролю не лише доступності вузлів, а й стану окремих служб, ресурсів і прикладних компонентів.

Проаналізовано сучасні підходи до моніторингу IT-інфраструктури: безагентний, агентний, комбінований, шаблонний підхід і автоматизацію підключення вузлів. Для спроектованого середовища найбільш доцільною є комбінована модель, у якій сервери Windows і Linux контролюються через агент, а мережеве обладнання та окремі сервіси — за допомогою мережевих перевірок і SNMP.

У межах порівняльного аналізу розглянуто Icinga 2, Zabbix, Nagios та Prometheus. Визначено, що Icinga 2 найкраще відповідає вимогам цієї роботи,

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

оскільки підтримує агентний і безагентний моніторинг, роботу з плагінами, шаблонами, правилами призначення сервісів, Icinga Web 2 та Icinga Director. Це дозволяє контролювати Windows Server, Linux-сервери, Cisco-комутатори, pfSense, Nextcloud, MariaDB, Docker-контейнер і систему резервного копіювання в межах однієї платформи.

Отже, у першому розділі обґрунтовано потребу в побудові централізованої системи моніторингу IT-інфраструктури та вибір Icinga 2 як основного інструменту реалізації. Результати аналізу стали основою для подальшого проектування архітектури інфраструктури, мережевої сегментації, серверних служб, політик доступу, резервного копіювання та системи моніторингу.

РОЗДІЛ 2. ПРОЄКТУВАННЯ IT-ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ ТА СИСТЕМИ ЇЇ МОНІТОРИНГУ

Метою цього розділу є формування проектної моделі IT-інфраструктури організації та системи її моніторингу, яка надалі реалізується в лабораторному середовищі. [30] У межах проектування визначаються структура мережі, ролі серверів, логіка сегментації, принципи доступу між вузлами, підхід до резервного копіювання, засоби захисту периметра та модель централізованого моніторингу.

Проектування виконується з урахуванням фактично реалізованої інфраструктури. Основна ідея полягає не лише в побудові мережі з серверами й робочими станціями, а у створенні контрольованого середовища, де кожен компонент має окрему роль, доступ між сегментами обмежується, критичні служби винесені на окремі вузли, а їхній стан контролюється системою моніторингу. Такий підхід відповідає окремим принципам Zero Trust, зокрема сегментації, мінімальним привілеям, обмеженню адміністративного доступу, контролю стану вузлів і зменшенню можливостей горизонтального переміщення в мережі. [3]

2.1. Проектування загальної архітектури IT-інфраструктури організації

Проектування загальної архітектури є початковим етапом побудови корпоративного середовища. На цьому етапі визначається, які функціональні зони

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

має містити інфраструктура, які вузли входять до її складу, яку роль вони виконують і як між собою взаємодіють.

У межах роботи проектується ІТ-інфраструктура невеликої організації, що включає користувацькі робочі станції, адміністративне робоче місце, серверну ферму, граничний маршрутизатор, комутатор ядра, комутатори доступу, систему резервного копіювання та центральний вузол моніторингу. Така модель дозволяє відтворити типове корпоративне середовище, у якому одночасно функціонують доменні служби, прикладний файловий сервіс, база даних, мережеве обладнання, засоби захисту периметра та система контролю стану інфраструктури.

Загальна схема інфраструктури побудована за зональним принципом. У проєкті виділено чотири основні зони: Untrusted / WAN, Security Perimeter, Corporate LAN та Server Farm. Такий поділ потрібний для того, щоб відокремити зовнішнє середовище від внутрішньої мережі, виділити периметр безпеки, розмежувати користувацькі сегменти та розмістити серверні компоненти в окремій контрольованій області. Загальну логічну схему ІТ-інфраструктури наведено в додатку А на рисунку А.1.

Зона Untrusted / WAN імітує зовнішнє недовірене середовище. Вона використовується для підключення граничного маршрутизатора до зовнішньої мережі та перевірки роботи периметрових механізмів. У реальному середовищі цій зоні відповідає мережа провайдера або Інтернет.

Зона Security Perimeter містить граничний маршрутизатор pfSense. Його призначення полягає у централізованому виході корпоративної мережі до зовнішнього середовища, виконанні NAT, фільтрації трафіку та розміщенні засобів захисту периметра. У подальшій реалізації на pfSense також використовується Suricata IDS/IPS, що дає змогу контролювати підозрілу активність на WAN-рівні. [14; 15; 16]

Зона Corporate LAN охоплює внутрішню користувацьку частину інфраструктури. Центральним елементом цієї зони є Cisco Core L3 Switch, який виконує роль внутрішнього маршрутизуючого вузла. До нього підключаються комутатори доступу для окремих підрозділів: Management, Accounting, HR та IT.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Така побудова потрібна для того, щоб розмістити різні групи користувачів у різних VLAN і надалі застосовувати до них окремі правила доступу.

Зона Server Farm призначена для серверних і службових компонентів. У ній передбачено розміщення Windows Server 2022, Linux-App-Server, Database-Server, Backup-Server та Icinga2-Master-Server. Винесення серверів в окрему зону дозволяє обмежити прямий доступ до критичних служб, спростити адміністрування та централізовано контролювати стан серверної інфраструктури.

Windows Server 2022 проєктується як основний доменний і мережевий сервер. На ньому передбачається розміщення Active Directory Domain Services, DNS та DHCP. Ці служби потрібні для централізованої автентифікації користувачів, роботи доменного середовища, видачі IP-адрес клієнтським станціям і підтримки внутрішнього DNS-резолвінгу. [20; 21; 22]

Linux-App-Server проєктується як сервер прикладного сервісу Nextcloud. Nextcloud використовується як внутрішнє корпоративне файлове сховище. Наявність такого сервісу потрібна для моделювання реальної прикладної служби організації, доступність якої залежить не лише від самого Linux-сервера, а й від Docker-контейнера, вебдоступу, HTTPS і бази даних. [24; 25; 26]

Database-Server використовується для розміщення MariaDB, яка зберігає дані Nextcloud. Розділення прикладного сервера і сервера баз даних потрібне для відокремлення рівня застосунку від рівня зберігання даних. Це спрощує адміністрування, резервне копіювання та моніторинг, оскільки стан вебсервісу й бази даних можна контролювати окремо. [27]

Backup-Server проєктується як окремий вузол для централізованого резервного копіювання. Його призначення полягає у збереженні важливих даних, конфігурацій і службових файлів. Окремий backup-вузол потрібний для того, щоб резервне копіювання не залежало від прикладного, доменного або моніторингового сервера. [4]

Icinga2-Master-Server проєктується як центральний вузол моніторингу. Він повинен контролювати сервери, мережеве обладнання, pfSense, прикладні сервіси, базу даних, процес резервного копіювання та Suricata. Завдяки цьому адміністратор

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

отримує єдину точку перегляду стану інфраструктури та може швидко визначати, який саме компонент спричинив проблему.

Адміністративна станція виділяється в окремий ІТ-сегмент. Її призначення полягає у безпечному керуванні серверами, мережевим обладнанням, pfSense та системою моніторингу. Такий вузол не повинен розглядатися як звичайна користувацька станція, оскільки має розширений адміністративний доступ.

Перелік основних компонентів ІТ-інфраструктури та їх призначення наведено в додатку А, таблиця А.1. Основні залежності між компонентами інфраструктури наведено в додатку А, таблиця А.2.

2.2. Проєктування мережевої інфраструктури та VLAN-сегментації

Мережева інфраструктура проєктується з урахуванням потреби в логічному розмежуванні користувачів, серверів, адміністративних вузлів, системи моніторингу та мережевого обладнання. Основою мережевої архітектури є Cisco Core L3 Switch, який виконує роль центрального маршрутизуючого пристрою внутрішньої мережі. Саме на ньому передбачається створення SVI-інтерфейсів для VLAN і маршрутизація між внутрішніми підмережами. [18]

pfSense у цій моделі не виконує внутрішню міжвланову маршрутизацію. Його роль пов'язана з периметром: виходом до зовнішньої мережі, NAT, фільтрацією трафіку та контролем WAN-рівня. Для взаємодії між pfSense і Core-L3-Switch передбачено окремий транзитний сегмент. Такий поділ ролей робить архітектуру зрозумілою: Cisco Core відповідає за внутрішню маршрутизацію, а pfSense — за периметр. [14]

Для розмежування інфраструктури використовується VLAN-сегментація. Кожен функціональний сегмент отримує окрему VLAN і власну IP-підмережу. Користувацькі підрозділи Management, Accounting та HR розміщуються в окремих VLAN, адміністративна станція — у VLAN IT_Dept, сервери — у VLAN Servers, моніторинг — у VLAN Monitoring, мережеве обладнання — у VLAN Net_Mgmt. Такий підхід потрібен для обмеження прямої взаємодії між сегментами та створення основи для подальшого застосування ACL. [17; 18]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Структура VLAN, їх призначення, підмережі та шлюзи наведені в додатку Б, таблиця Б.1. Адресація основних вузлів IT-інфраструктури наведена в додатку Б, таблиця Б.2.

Для клієнтських VLAN передбачається динамічна видача адрес через DHCP. Оскільки DHCP-сервер розміщується на Windows Server 2022 у серверному сегменті, а клієнтські вузли знаходяться в інших VLAN, на SVI-інтерфейсах користувацьких VLAN необхідно передбачити DHCP Relay. Це дозволяє передавати DHCP-запити клієнтів до централізованого DHCP-сервера.

Комутатори доступу проєктуються як пристрої другого рівня. Вони підключають кінцеві вузли до відповідних VLAN, а зв'язок із комутатором ядра здійснюється через trunk-з'єднання. Така схема дозволяє централізувати маршрутизацію на Core-L3-Switch і спростити керування access-рівнем. Прив'язку комутаторів доступу до VLAN, management-адрес і trunk-з'єднань наведено в додатку Б, таблиця Б.3.

У межах мережевого проєктування також передбачається сегмент моніторингу. Icinga2-Master-Server розміщується в окремій VLAN Monitoring і повинен мати контрольований доступ до серверів, мережевого обладнання та pfSense. Це потрібно для виконання агентних перевірок Windows і Linux-серверів, SNMP-перевірок Cisco-комутаторів і pfSense, а також прикладних перевірок Nextcloud, MariaDB, backup-журналу та Suricata. [14; 19]

Таким чином, спроектована мережева інфраструктура забезпечує логічну ізоляцію сегментів, централізовану внутрішню маршрутизацію, контрольований вихід до зовнішньої мережі та основу для подальшого впровадження ACL, GPO, моніторингу й захисту периметра.

2.3. Проєктування доменної, серверної та прикладної інфраструктури

Після визначення мережевої структури проєктується доменна, серверна та прикладна частина інфраструктури. Її основне завдання полягає в тому, щоб забезпечити централізовану автентифікацію користувачів, роботу базових

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

мережевих служб, функціонування корпоративного прикладного сервісу, збереження даних і подальший контроль стану серверів.

Windows Server 2022 проєктується як основний сервер доменної інфраструктури. На ньому передбачається розміщення Active Directory Domain Services, DNS Server та DHCP Server. Active Directory потрібна для централізованого керування користувачами, комп'ютерами й організаційними підрозділами. DNS забезпечує коректну роботу домену та доступ до внутрішніх сервісів за іменами. DHCP забезпечує автоматичну видачу IP-параметрів клієнтським робочим станціям. [20; 21; 22]

Доменне середовище проєктується на базі внутрішнього домену corp.local. У межах домену передбачається створення організаційних підрозділів Management, Accounting, HR_Dept та IT_Dept. Така структура потрібна для впорядкування користувачів і комп'ютерів за підрозділами, а також для подальшого застосування групових політик до відповідних користувачьких станцій. [23]

До домену включаються користувачькі Windows-станції, оскільки вони потребують централізованої автентифікації та застосування політик безпеки. Водночас Linux-сервери, pfSense, Cisco-комутатори та Icinga2-Master-Server не розглядаються як обов'язкові учасники домену. Це зменшує залежність критичних компонентів від одного доменного середовища та дозволяє керувати ними через окремі адміністративні механізми.

Linux-App-Server проєктується як вузол прикладного рівня. На ньому передбачається розміщення Nextcloud у контейнеризованому середовищі Docker. Nextcloud використовується для організації внутрішнього файлового сервісу, який імітує реальну корпоративну потребу в централізованому зберіганні та обміні файлами. Docker застосовується для ізоляції прикладного середовища та спрощення керування сервісом. [24; 25; 26]

Доступ до Nextcloud передбачається через Nginx із використанням HTTPS. Це дозволяє організувати захищене підключення користувачів до сервісу та відокремити зовнішній вебдоступ від внутрішньої логіки контейнера. Така

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

побудова також дає змогу надалі контролювати доступність Nextcloud як окремого прикладного сервісу, а не лише як доступність Linux-сервера. [28]

Database-Server проєктується як окремий сервер баз даних із MariaDB. Його відділення від Linux-App-Server потрібне для розмежування прикладного рівня та рівня зберігання даних. Це спрощує резервне копіювання, моніторинг і діагностику проблем: окремо можна контролювати стан вебсервісу, Docker-контейнера та бази даних. [27]

Backup-Server проєктується як окремий вузол для зберігання резервних копій. До складу даних, що мають резервуватися, входять файли Nextcloud, база даних MariaDB, конфігурації Docker Compose, Nginx, Icinga 2, Icinga Web 2 та Icinga Director. Передавання резервних копій доцільно виконувати через SSH, а результати роботи backup-сценаріїв фіксувати в окремому журналі. Це дозволяє надалі контролювати не лише наявність backup-сервера, а й актуальність виконання резервного копіювання. [4]

Таким чином, доменна, серверна та прикладна інфраструктура проєктується як набір взаємопов'язаних, але логічно розділених компонентів. Windows Server 2022 забезпечує домен, DNS і DHCP; Linux-App-Server забезпечує Nextcloud; Database-Server зберігає дані; Backup-Server відповідає за резервне копіювання; Icinga2-Master-Server надалі контролює стан цих компонентів.

2.4. Проєктування політик доступу, резервного копіювання та захисту мережевого периметра

Політики доступу проєктуються з урахуванням принципу мінімальних привілеїв. Звичайні користувачі повинні мати доступ лише до тих сервісів, які потрібні для роботи: доменної автентифікації, DNS, DHCP, синхронізації часу та корпоративного сервісу Nextcloud. Прямий доступ користувацьких VLAN до сервера баз даних, backup-сервера, системи моніторингу, інтерфейсів керування Cisco та WebGUI pfSense має бути обмежений. [2; 3]

Для користувацьких Windows-станцій передбачається застосування групових політик Active Directory. Corporate Security Policy повинна забезпечувати базовий

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

рівень безпеки: вимоги до паролів, обмеження локальних адміністративних прав, блокування екрана, заборону несанкціонованої зміни системних параметрів і аудит подій входу. Такі політики потрібні для зменшення ризику помилкових або навмисних змін на користувацьких робочих станціях. [23]

Адміністративна станція виділяється в окремий VLAN IT_Dept. Вона використовується для керування Linux-серверами через SSH, Windows Server 2022 через RDP, Cisco-комутаторами, pfSense та Icinga Web 2. Така модель потрібна для того, щоб не відкривати адміністративні інтерфейси для звичайних користувацьких сегментів.

Для обмеження доступу між VLAN на Cisco Core L3 Switch передбачається використання Extended ACL. ACL мають дозволяти користувачам доступ лише до необхідних сервісів і блокувати прямі підключення до критичних серверів та інтерфейсів керування. Це зменшує ризик горизонтального переміщення в мережі в разі компрометації одного з користувацьких вузлів. [17]

На рівні pfSense передбачається контроль доступу до зовнішньої мережі та адміністративних інтерфейсів. pfSense забезпечує NAT і фільтрацію трафіку на межі інфраструктури. Доступ до WebGUI pfSense має бути дозволений лише з адміністративної станції та сервера моніторингу. Також pfSense використовується як платформа для Suricata IDS/IPS, яка контролює WAN-периметр і дозволяє виявляти підозрілу активність. [14; 15; 16]

Резервне копіювання проєктується як окрема функціональна підсистема. Її призначення полягає у збереженні важливих даних і конфігурацій, необхідних для відновлення сервісів після збою. Окремий Backup-Server дозволяє не поєднувати функції резервного копіювання з доменними, прикладними або моніторинговими службами. Для контролю процесу резервного копіювання передбачається ведення журналу виконання backup-сценарію, який надалі перевіряється системою моніторингу. [4]

Таким чином, політики доступу, ACL, GPO, захист pfSense, Suricata та резервне копіювання проєктуються як єдина модель захисту інфраструктури. Її мета — обмежити доступ до критичних компонентів, забезпечити контроль

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

адміністративних дій, знизити ризик поширення інциденту між сегментами та зберегти можливість відновлення сервісів.

2.5. Проектування системи моніторингу на базі Icinga 2

Система моніторингу проектується як центральний інструмент контролю стану IT-інфраструктури. Її завдання полягає не лише у перевірці доступності хостів, а й у контролі конкретних служб, прикладних сервісів, мережевих інтерфейсів, резервного копіювання та засобів захисту периметра. Такий підхід потрібний для того, щоб адміністратор міг швидко визначити, на якому саме рівні виникла проблема: серверному, прикладному, мережевому або безпековому.

Центральним вузлом моніторингу визначено Icinga2-Master-Server, розміщений у VLAN Monitoring. На ньому передбачається розгортання Icinga 2 як основного ядра моніторингу, Icinga Web 2 як вебінтерфейсу для перегляду стану хостів і сервісів, MariaDB/IDO як механізму збереження даних моніторингу та Icinga Director як інструмента централізованого керування конфігурацією. [5; 8; 9]

Icinga Director у проектній моделі використовується для створення хостів, шаблонів, сервісних наборів, правил автоматичного призначення перевірок, змінних полів і команд перевірки. Такий підхід потрібний для того, щоб не створювати кожну перевірку вручну для кожного вузла. Однотипні сервери або пристрої можуть отримувати перевірки через шаблони, Service Sets або Apply Rules. [6; 9]

Для серверів Windows і Linux передбачається агентна модель моніторингу. Вона дає змогу виконувати локальні перевірки безпосередньо на контрольованому вузлі. Для Windows Server 2022 передбачається контроль доступності сервера, використання CPU, оперативної пам'яті, логічних дисків, мережевого інтерфейсу, доступності RDP, а також стану служб AD DS, DNS, DHCP і W32Time. Такі перевірки потрібні, тому що Windows Server 2022 є критичним вузлом доменної інфраструктури. [5; 6; 7]

Для Linux-серверів передбачається базовий набір перевірок: SSH, CPU, оперативна пам'ять, swp, кількість процесів і дисковий простір. Цей набір

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

застосовується до Linux-App-Server, Database-Server і Backup-Server. Він потрібний для контролю доступності серверів, можливості адміністрування через SSH і стабільності їхніх системних ресурсів. [5; 6; 7; 29]

Для Linux-App-Server додатково передбачається контроль прикладного рівня. Система моніторингу має перевіряти доступність Nextcloud через HTTPS і стан Docker-контейнера Nextcloud. Це важливо, оскільки сам Linux-сервер може бути доступним, але прикладний сервіс може не працювати через помилку контейнера, вебдоступу або конфігурації. [24; 25; 26; 28]

Для Database-Server передбачається спеціалізована перевірка MariaDB. Вона потрібна для визначення доступності бази даних, від якої залежить робота Nextcloud. Якщо MariaDB зупиниться або стане недоступною, вебсервіс може перестати працювати коректно навіть за умови доступності Linux-App-Server. [27]

Для Backup-Server передбачається перевірка актуальності журналу резервного копіювання. Її призначення полягає в тому, щоб контролювати не лише доступність самого сервера, а й факт виконання backup-сценарію. Якщо файл журналу тривалий час не оновлюється, це означає, що процес резервного копіювання може не виконуватися, навіть якщо сервер залишається доступним. [4]

Для Cisco-комутаторів передбачається SNMPv3-моніторинг. Він має контролювати час безперервної роботи, завантаження процесора, оперативну пам'ять, VLAN-інтерфейси, trunk-з'єднання та uplink-порти. Для Core-L3-Switch набір перевірок є ширшим, оскільки він виконує роль центрального маршрутизуючого вузла. Для комутаторів доступу достатньо контролю базових параметрів і стану uplink-порту до ядра мережі. [18; 19]

Для pfSense передбачається SNMP-моніторинг часу безперервної роботи, WAN- і LAN-інтерфейсів, завантаження процесора, доступної оперативної пам'яті та процесу Suricata. Перевірка Suricata Status виділяється окремо, оскільки вона контролює працездатність засобу захисту периметра, а не лише стан самого маршрутизатора. [14; 15; 16]

У межах проектування також передбачається використання різних механізмів призначення перевірок. Host Templates потрібні для групування

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

однотипних вузлів. Service Sets використовуються для серверних перевірок Windows і Linux. Apply Rules застосовуються для автоматичного призначення перевірок мережевому обладнанню та pfSense. Data Fields передають змінні значення в команди перевірки, наприклад назву служби Windows, назву Docker-контейнера, шлях до backup-журналу, режим SNMP-перевірки або назву процесу. CheckCommands визначають, який плагін або скрипт буде виконуватися для конкретної перевірки. [6; 9; 10]

Для перевірки працездатності системи моніторингу передбачаються контрольовані сценарії тестування. До них належать зупинка служби W32Time на Windows Server 2022, зупинка SSH-служби на Linux-сервері, блокування HTTPS-доступу до Nextcloud, зупинка MariaDB, зміна дати журналу резервного копіювання, вимкнення trunk/uplink-інтерфейсу Cisco та вимкнення Suricata на pfSense. Такі сценарії потрібні для підтвердження того, що система моніторингу здатна не лише показувати стан ОК, а й правильно реагувати на реальні збої.

Таким чином, система моніторингу проєктується як завершальний елемент інфраструктури, який об'єднує контроль мережевого, серверного, прикладного та безпекового рівнів. Її структура відповідає фактично реалізованій системі в третьому розділі та дозволяє централізовано контролювати стан усіх ключових компонентів.

Висновки до розділу 2

У другому розділі було сформовано проєктну модель IT-інфраструктури організації та системи її моніторингу. Визначено зональну архітектуру, у якій зовнішнє середовище, периметр безпеки, корпоративна локальна мережа, серверна ферма, адміністративний сегмент і сегмент моніторингу розділені логічно та функціонально. Такий підхід створює основу для ізоляції критичних компонентів, обмеження доступу між сегментами та подальшого централізованого контролю стану інфраструктури.

Було спроектовано мережеву інфраструктуру на базі pfSense, Cisco Core L3 Switch і комутаторів доступу. Передбачено VLAN-сегментацію, транзитну

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

взаємодію між pfSense і комутатором ядра, окремі користувацькі, серверні, адміністративні, моніторингові та management-сегменти. Така модель дозволяє відокремити внутрішню маршрутизацію від функцій периметра, централізувати керування трафіком і створити основу для подальшого застосування ACL.

Було визначено ролі основних серверних компонентів. Windows Server 2022 проєктується як вузол Active Directory, DNS і DHCP; Linux-App-Server — як сервер прикладного сервісу Nextcloud; Database-Server — як окремий сервер MariaDB; Backup-Server — як вузол централізованого резервного копіювання; Icinga2-Master-Server — як центральний сервер моніторингу. Такий розподіл ролей дозволяє не змішувати критичні функції на одному вузлі та спрощує подальший контроль їхнього стану.

Окремо було спроектовано модель доступу й захисту інфраструктури. Вона включає групові політики для користувацьких Windows-станцій, виділений адміністративний сегмент, ACL між VLAN, обмеження доступу до критичних серверів та інтерфейсів керування, захист периметра на базі pfSense і Suricata, а також резервне копіювання важливих даних і конфігурацій. Це відповідає принципам сегментації, мінімальних привілеїв і контрольованого адміністрування.

Завершальною частиною розділу стало проєктування системи моніторингу на базі Icinga 2. Було визначено, що для Windows- і Linux-серверів доцільно використовувати агентний моніторинг, а для Cisco-комутаторів і pfSense — SNMP-моніторинг. Також було передбачено контроль Nextcloud через HTTPS, Docker-контейнера, MariaDB, backup-журналу, VLAN/trunk/uplink-з'єднань, ресурсів pfSense і процесу Suricata. Для централізованого керування моніторингом передбачено використання Icinga Web 2 та Icinga Director із шаблонами хостів, сервісними наборами, Apply Rules, Data Fields і CheckCommands.

Таким чином, у другому розділі було не лише описано загальну структуру інфраструктури, а й визначено логіку її подальшої реалізації та контролю. Запропонована проєктна модель відповідає фактично виконаній практичній роботі та створює основу для реалізації мережевої, доменної, серверної, прикладної, безпекової та моніторингової частин у третьому розділі.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 3. РЕАЛІЗАЦІЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ СИСТЕМИ МОНІТОРИНГУ ІТ-ІНФРАСТРУКТУРИ

Метою третього розділу є практична реалізація спроектованої ІТ-інфраструктури та перевірка працездатності системи її моніторингу. У межах розділу послідовно реалізуються мережевий рівень, доменні служби, серверні та прикладні компоненти, клієнтські й адміністративні вузли, політики доступу, механізми захисту периметра, резервне копіювання та система моніторингу на базі Icinga 2. Така послідовність потрібна для того, щоб спочатку створити сам об'єкт моніторингу, а потім підключити до нього засоби контролю та перевірити реакцію системи на контрольовані збої.

3.1. Реалізація мережевої та доменної інфраструктури

Метою підрозділу є створення базового мережевого й доменного фундаменту, без якого неможлива подальша робота серверів, клієнтів, політик безпеки та системи моніторингу. На цьому етапі реалізується граничний маршрутизатор pfSense, комутатор ядра Cisco Core L3 Switch, VLAN-сегментація, DHCP Relay, trunk/access-порти, а також Windows Server 2022 з ролями Active Directory, DNS і DHCP. Це потрібно для забезпечення маршрутизації між сегментами, централізованої автентифікації користувачів, автоматичної видачі мережевих параметрів і стабільної взаємодії між усіма вузлами інфраструктури.

Налаштування pfSense виконується для створення контрольованого мережевого периметра. pfSense забезпечує вихід внутрішньої мережі до зовнішнього середовища, NAT, статичну маршрутизацію до внутрішніх VLAN, фільтрацію трафіку та обмеження доступу до адміністративного інтерфейсу. [14]

Окремі правила для Icinga2-Master-Server потрібні для того, щоб сервер моніторингу міг перевіряти доступність pfSense та отримувати SNMP-дані, але звичайні користувацькі сегменти не мали доступу до керування маршрутизатором.

Налаштування Cisco Core L3 Switch виконується для централізованої маршрутизації між VLAN і формування внутрішнього ядра мережі. Саме на цьому пристрої створюються VLAN, SVI-інтерфейси, шлюзи для підмереж, маршрут за

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

замовчуванням до pfSense і DHCP Relay. Це дозволяє розділити інфраструктуру на логічні сегменти, але зберегти контрольовану взаємодію між ними. [18]

Налаштування комутаторів доступу виконується для фізичного підключення користувацьких, адміністративних і серверних вузлів до відповідних VLAN. Комутатори доступу не виконують маршрутизацію між сегментами, а передають трафік до ядра мережі через trunk-з'єднання. Така модель спрощує керування access-рівнем і дозволяє централізовано контролювати маршрутизацію та політики доступу на Core-L3-Switch. [18]

Розгортання Windows Server 2022 виконується для створення централізованого доменного середовища. Active Directory забезпечує автентифікацію користувачів і керування обліковими записами, DNS — коректну роботу доменних імен і внутрішніх сервісів, а DHCP — автоматичну видачу мережевих параметрів клієнтським вузлам. Перевірка зв'язності та доменних служб потрібна для підтвердження, що мережевий і доменний рівні готові до підключення робочих станцій та серверних сервісів. [20; 21; 22]

Налаштування граничного маршрутизатора pfSense

Граничний маршрутизатор pfSense у реалізованій інфраструктурі виконує роль точки виходу корпоративної мережі до зовнішнього середовища. Він забезпечує трансляцію мережевих адрес, маршрутизацію між внутрішніми підмережами та зовнішньою мережею, а також базовий контроль доступу на межі інфраструктури. [14]

На початковому етапі маршрутизатору було призначено системне ім'я pfSense-Edge-Router, а як доменне ім'я використано corp.local. Для коректної інтеграції з внутрішнім середовищем основним DNS-сервером було визначено Windows Server 2022 з адресою 192.168.50.10. Це дозволяє pfSense працювати в єдиному внутрішньому просторі імен із доменною інфраструктурою.

Внутрішній інтерфейс LAN у цій топології не використовується для безпосереднього підключення користувацьких станцій. Він виконує роль транзитного сегмента між pfSense та комутатором ядра Cisco Core L3 Switch. На стороні pfSense для цього сегмента використовується адреса 192.168.1.1/24.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Для забезпечення зворотної маршрутизації до внутрішніх VLAN на pfSense було створено шлюз CoreSwitch_GW. Як адресу шлюзу вказано 192.168.1.2, що відповідає транзитному SVI-інтерфейсу VLAN 99 на Cisco Core L3 Switch. Налаштування шлюзу CoreSwitch_GW наведено в додатку В на рисунку В.1.

Після створення шлюзу було додано статичний маршрут до сумарного внутрішнього адресного простору 192.168.0.0/16 через CoreSwitch_GW. Завдяки цьому pfSense може передавати зворотний трафік до корпоративних підмереж, які розміщені за комутатором ядра. Налаштування статичного маршруту наведено в додатку В на рисунку В.2.

Для доступу внутрішніх сегментів до зовнішньої мережі було налаштовано Outbound NAT. Ця конфігурація дає змогу корпоративним вузлам із приватного адресного простору 192.168.0.0/16 виходити до зовнішніх ресурсів через WAN-інтерфейс pfSense без прямого розкриття внутрішньої структури мережі.

Окремо було налаштовано правила міжмережевого екрана на LAN-інтерфейсі pfSense. Їхня мета полягає у розмежуванні доступу до адміністративного інтерфейсу pfSense та одночасному збереженні можливості моніторингу маршрутизатора засобами Icinga 2.

Для звичайних внутрішніх підмереж було створено правило блокування доступу до WebGUI pfSense через HTTP. Воно забороняє підключення з адресного простору 192.168.0.0/16 до самого pfSense на TCP-порт 80. Конфігурацію цього правила наведено в додатку В на рисунку В.3.

Для сервера моніторингу Icinga2-Master-Server було створено окреме правило дозволу ICMP-трафіку. Джерелом виступає адреса 192.168.60.10, а призначенням — This Firewall (self). Це правило дозволяє Icinga перевіряти доступність pfSense за допомогою ICMP-запитів. Налаштування правила ICMP наведено в додатку В на рисунку В.4.

Також для Icinga2-Master-Server було створено правило дозволу SNMP-трафіку до pfSense. У цьому правилі джерелом є 192.168.60.10, призначенням — This Firewall (self), протоколом — UDP, а портом призначення — 161. Це потрібно для SNMP-моніторингу pfSense, зокрема контролю доступності, інтерфейсів,

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

завантаження ресурсів та стану окремих служб. Конфігурацію SNMP-правила наведено в додатку В на рисунку В.5.

Для адміністративної станції було створено окреме правило доступу до WebGUI pfSense. Джерелом є адреса 192.168.40.10, призначенням — This Firewall (self), а дозволеним портом — TCP 443. Це забезпечує доступ до вебінтерфейсу керування pfSense лише з довіреного адміністративного вузла, розміщеного в сегменті IT_Dept. Налаштування цього правила наведено в додатку В на рисунку В.6.

Для заборони доступу до WebGUI pfSense зі звичайних внутрішніх підмереж було створено правило блокування HTTPS. Воно блокує TCP-з'єднання з адресного простору 192.168.0.0/16 до This Firewall (self) на порт 443. Це правило не блокує адміністративний доступ із 192.168.40.10, оскільки правило дозволу для адміністративної станції розміщується вище за правило блокування HTTPS. Конфігурацію цього правила наведено в додатку В на рисунку В.7.

Для збереження виходу внутрішніх підмереж до зовнішніх ресурсів було створено загальне правило Allow LAN outbound traffic. Воно дозволяє трафік із внутрішнього адресного простору 192.168.0.0/16 до інших мереж, однак розміщується нижче правил блокування доступу до WebGUI pfSense, тому не скасовує обмеження адміністративного інтерфейсу.

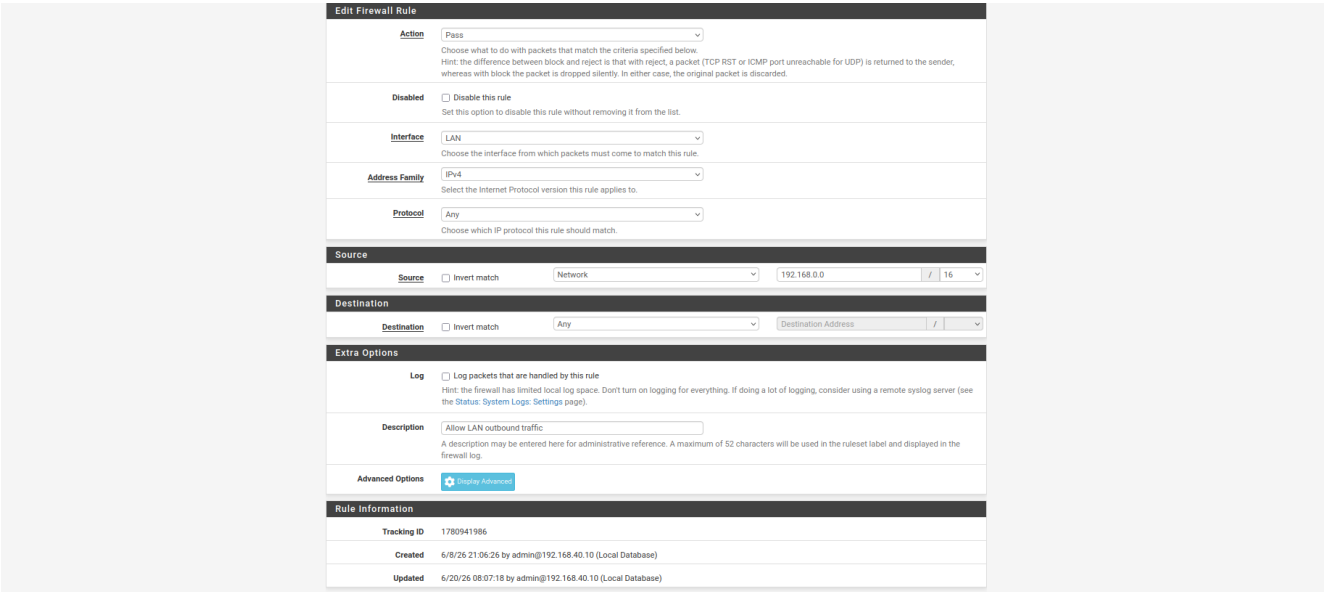


Рисунок 3.1 — Налаштування правила дозволу вихідного трафіку з внутрішньої мережі на pfSense

Підсумкова ієрархія правил на LAN-інтерфейсі pfSense демонструє, що доступ до WebGUI дозволено лише з адміністративної станції, сервер моніторингу має ICMP- і SNMP-доступ до маршрутизатора, а звичайні внутрішні сегменти не можуть відкривати вебінтерфейс керування через HTTP або HTTPS.

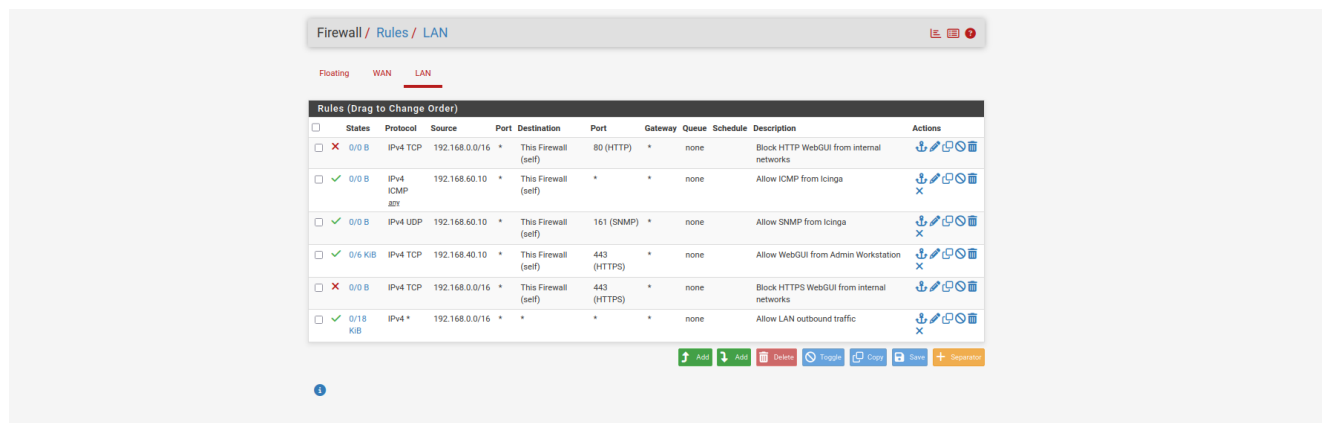


Рисунок 3.2 — Підсумкова ієрархія правил міжмережевого екрана на LAN-інтерфейсі pfSense

Після створення власних правил доступу стандартне правило Anti-Logout Rule було вимкнено через налаштування Admin Access. Це необхідно, оскільки Anti-Logout Rule автоматично дозволяє доступ до WebGUI pfSense з LAN-інтерфейсу та може заважати перевірці власної політики обмеження доступу до адміністративного інтерфейсу.

Таким чином, pfSense було налаштовано як граничний маршрутизатор, який забезпечує статичну маршрутизацію до внутрішніх VLAN, NAT для виходу до зовнішньої мережі, дозвіл моніторингового ICMP/SNMP-доступу для Icinga та обмеження доступу до адміністративного вебінтерфейсу лише з довіреного адміністративного сегмента.

Налаштування комутатора ядра Cisco Core L3 Switch

Наступним етапом було налаштовано комутатор ядра Cisco Core L3 Switch. У цій інфраструктурі він виконує роль центрального маршрутизуючого вузла внутрішньої мережі. Саме на ньому реалізується міжвланова маршрутизація, створюються шлюзи для VLAN, налаштовується транзитне з'єднання з pfSense, DHCP Relay та trunk-з'єднання до комутаторів доступу.

Для роботи комутатора як пристрою третього рівня було активовано маршрутизацію командою `ip routing`. Це дозволяє Cisco Core L3 Switch маршрутизувати трафік між логічними сегментами мережі через SVI-інтерфейси.

```
Core-L3-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#ip routing
Core-L3-Switch(config)#do write
Building configuration...
Compressed configuration from 2370 bytes to 1283 bytes[OK]
Core-L3-Switch(config)#
```

Рисунок 3.3 — Активація маршрутизації третього рівня на Cisco Core L3 Switch

Далі було створено VLAN відповідно до спроектованої структури мережі. У конфігурації передбачено VLAN 10 Management, VLAN 20 Accounting, VLAN 30 HR, VLAN 40 IT_Dept, VLAN 50 Servers, VLAN 60 Monitoring, VLAN 99 Transit і VLAN 100 Net_Mgmt. Для основних VLAN створено SVI-інтерфейси, які виконують роль шлюзів за замовчуванням для відповідних підмереж.

Для користувацьких сегментів шлюзами визначено адреси 192.168.10.254, 192.168.20.254 і 192.168.30.254. Для адміністративного сегмента використовується 192.168.40.254, для серверного сегмента — 192.168.50.254, а для сегмента моніторингу — 192.168.60.254. Налаштування VLAN і SVI-інтерфейсів на комутаторі ядра наведено в додатку В на рисунку В.8.

Для взаємодії з pfSense було створено транзитний сегмент VLAN 99. На стороні Cisco Core L3 Switch для нього використовується адреса 192.168.1.2/24, а на стороні pfSense — 192.168.1.1/24. Фізичний порт Ethernet0/0, який з'єднує комутатор ядра з pfSense, налаштовано як access-порт у VLAN 99. Це важливо, оскільки з'єднання між pfSense і Core-L3-Switch у цій топології є окремим транзитним L3-сегментом, а не trunk-з'єднанням для передавання багатьох VLAN.

Для передавання трафіку до зовнішньої мережі на Cisco Core L3 Switch було додано маршрут за замовчуванням у напрямку pfSense. У ролі next-hop використовується адреса 192.168.1.1. Після цього внутрішні VLAN отримали можливість передавати зовнішній трафік через комутатор ядра до граничного маршрутизатора.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

```

Core-L3-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#interface Ethernet 0/0
Core-L3-Switch(config-if)# no ip address
Core-L3-Switch(config-if)# switchport
Core-L3-Switch(config-if)# exit
Core-L3-Switch(config)#
*Jun  8 00:28:50.772: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Jun  8 00:28:51.777: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Core-L3-Switch(config)#interface Vlan 99
Core-L3-Switch(config-if)# ip address 192.168.1.2 255.255.255.0
Core-L3-Switch(config-if)# no shutdown
Core-L3-Switch(config-if)# exit
Core-L3-Switch(config)#
*Jun  8 00:28:56.289: %LINK-3-UPDOWN: Interface Vlan99, changed state to up
*Jun  8 00:28:57.297: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
Core-L3-Switch(config)#interface Ethernet 0/0
Core-L3-Switch(config-if)# switchport trunk encapsulation dot1q
Core-L3-Switch(config-if)# switchport mode access
Core-L3-Switch(config-if)# switchport access vlan 99
Core-L3-Switch(config-if)# no shutdown
Core-L3-Switch(config-if)# exit
Core-L3-Switch(config)#
Core-L3-Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Core-L3-Switch(config)#do write
Building configuration...
compressed configuration from 2370 bytes to 1281 bytes[OK]
Core-L3-Switch(config)#
Core-L3-Switch(config)#P2Q
Core-L3-Switch(config)#do write

```

Рисунок 3.4 — Налаштування транзитного сегмента VLAN 99 і маршруту за замовчуванням на Cisco Core L3 Switch

Працездатність транзитного з'єднання між Cisco Core L3 Switch і pfSense було перевірено за допомогою ICMP-запитів до адреси 192.168.1.1. Успішне виконання ring підтвердило коректність L3-взаємодії між комутатором ядра та граничним маршрутизатором.

```

Core-L3-Switch#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Core-L3-Switch#
Core-L3-Switch#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Core-L3-Switch#

```

Рисунок 3.5 — Перевірка зв'язності між Cisco Core L3 Switch і pfSense за допомогою ICMP-запитів

Оскільки реалізація виконувалася в лабораторному середовищі GNS3, на комутаторі було вимкнено Cisco Express Forwarding командою no ip cef. Це є специфічною лабораторною адаптацією для стабілізації роботи віртуального образу комутатора та не є типовою вимогою для фізичного production-середовища.

```

Core-L3-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#no ip cef
Core-L3-Switch(config)#do write
Building configuration...
compressed configuration from 2277 bytes to 1239 bytes[OK]
Core-L3-Switch(config)#

```

Рисунок 3.6 — Вимкнення Cisco Express Forwarding у лабораторному середовищі GNS3

Для централізованої видачі IP-адрес клієнтським робочим станціям було налаштовано DHCP Relay. Оскільки DHCP-сервер працює на Windows Server 2022

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

з адресою 192.168.50.10, а клієнтські вузли розміщені в окремих VLAN, широкомовні DHCP-запити необхідно передавати до сервера через комутатор ядра. Для цього на SVI-інтерфейсах користувацьких VLAN було вказано ip helper-address 192.168.50.10.

DHCP Relay застосовується для користувацьких сегментів Management, Accounting та HR. Для адміністративного сегмента IT_Dept використовується статична адресація, тому DHCP-пул для нього не застосовується.

```
Core-L3-Switch#enable
Core-L3-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#hostname Core-L3-Switch
Core-L3-Switch(config)#
Core-L3-Switch(config)#interface vlan 10
Core-L3-Switch(config-if)#ip helper-address 192.168.50.10
Core-L3-Switch(config-if)#exit
Core-L3-Switch(config)#
Core-L3-Switch(config)#interface vlan 20
Core-L3-Switch(config-if)#ip helper-address 192.168.50.10
Core-L3-Switch(config-if)#exit
Core-L3-Switch(config)#
Core-L3-Switch(config)#interface vlan 30
Core-L3-Switch(config-if)#ip helper-address 192.168.50.10
Core-L3-Switch(config-if)#exit
Core-L3-Switch(config)#
Core-L3-Switch(config)#do write
Building configuration...
Compressed configuration from 1605 bytes to 949 bytes[OK]
Core-L3-Switch(config)#
```

Рисунок 3.7 — Налаштування DHCP Relay для користувацьких VLAN на Cisco Core L3 Switch

Для підключення комутаторів доступу до ядра мережі було налаштовано trunk-порти з інкапсуляцією IEEE 802.1Q. Такі з'єднання дозволяють передавати маркований VLAN-трафік між Cisco Core L3 Switch і комутаторами доступу. Конфігурацію trunk-портів до комутаторів доступу наведено в додатку В на рисунку В.9.

Налаштування комутаторів доступу

Комутатори доступу виконують роль пристроїв другого рівня. Вони використовуються для фізичного підключення кінцевих вузлів до відповідних VLAN і передавання трафіку до комутатора ядра через trunk-порт. Маршрутизація між VLAN на access-рівні не виконується, оскільки ця функція покладена на Cisco Core L3 Switch.

На комутаторі SW-Servers було створено VLAN 50 Servers і VLAN 60 Monitoring. VLAN 50 використовується для підключення серверних вузлів, а VLAN 60 — для розміщення центрального вузла моніторингу Icinga2-Master-Server. Порт

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Ethernet0/0 використовується як trunk до комутатора ядра, а інші порти працюють як access-порти відповідних VLAN.

```
SW-Servers#enable
SW-Servers#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-Servers(config)#hostname SW-Servers
SW-Servers(config)#vlan 50
SW-Servers(config-vlan)# name Servers
SW-Servers(config-vlan)# name Monitoring
SW-Servers(config-vlan)#exit
SW-Servers(config)#interface Ethernet 0/0
SW-Servers(config-if)# switchport trunk encapsulation dot1q
SW-Servers(config-if)# switchport mode trunk
SW-Servers(config-if)# no shutdown
SW-Servers(config-if)# exit
SW-Servers(config)#interface range Ethernet 0/1 - 3 , Ethernet 1/0
SW-Servers(config-if-range)# switchport mode access
SW-Servers(config-if-range)# switchport access vlan 50
SW-Servers(config-if-range)# no shutdown
SW-Servers(config-if-range)# exit
SW-Servers(config)#interface Ethernet 1/1
SW-Servers(config-if)# switchport mode access
SW-Servers(config-if)# switchport access vlan 60
SW-Servers(config-if)# no shutdown
SW-Servers(config-if)# exit
SW-Servers(config)#do write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1682 bytes to 966 bytes[OK]
SW-Servers(config)#
```

Рисунок 3.8 — Налаштування VLAN серверного та моніторингового сегментів на комутаторі SW-Servers

На комутаторі SW-Асс-01 налаштовано VLAN 20 Accounting, який використовується для робочих станцій бухгалтерії. Порт підключення до комутатора ядра працює в режимі trunk, а порти кінцевих пристроїв — у режимі access VLAN 20.

```
SW-Acc-01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-Acc-01(config)#vlan 20
SW-Acc-01(config-vlan)# name Accounting
SW-Acc-01(config-vlan)#exit
SW-Acc-01(config)#interface Ethernet 0/0
SW-Acc-01(config-if)# switchport trunk encapsulation dot1q
SW-Acc-01(config-if)# switchport mode trunk
SW-Acc-01(config-if)# no shutdown
SW-Acc-01(config-if)# exit
SW-Acc-01(config)#interface range Ethernet 0/1 - 2
SW-Acc-01(config-if-range)# switchport mode access
SW-Acc-01(config-if-range)# switchport access vlan 20
SW-Acc-01(config-if-range)# no shutdown
SW-Acc-01(config-if-range)# exit
SW-Acc-01(config)#do write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1528 bytes to 909 bytes[OK]
SW-Acc-01(config)#
```

Рисунок 3.9 — Налаштування VLAN 20 Accounting на комутаторі SW-Асс-01

На комутаторі SW-HR-01 реалізовано VLAN 30 HR для робочих станцій відділу кадрів. Як і в інших сегментах, uplink-порт до ядра налаштовано як trunk, а користувацькі порти переведено в режим access VLAN 30.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

```

SW-HR-01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-HR-01(config)#vlan 30
SW-HR-01(config-vlan)# name HR
SW-HR-01(config-vlan)#exit
SW-HR-01(config)#interface Ethernet 0/0
SW-HR-01(config-if)# switchport trunk encapsulation dot1q
SW-HR-01(config-if)# switchport mode trunk
SW-HR-01(config-if)# no shutdown
SW-HR-01(config-if)# exit
SW-HR-01(config)#interface range Ethernet 0/1 - 2
SW-HR-01(config-if-range)# switchport mode access
SW-HR-01(config-if-range)# switchport access vlan 30
SW-HR-01(config-if-range)# no shutdown
SW-HR-01(config-if-range)# exit
SW-HR-01(config)#do write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1527 bytes to 911 bytes[OK]
SW-HR-01(config)#

```

Рисунок 3.10 — Налаштування VLAN 30 HR на комутаторі SW-HR-01

На комутаторі SW-IT-01 налаштовано VLAN 40 IT_Dept, у якому розміщується адміністративна станція. Цей сегмент використовується для керування серверами, мережевим обладнанням, pfSense та системою моніторингу.

```

SW-IT-01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-IT-01(config)#vlan 40
SW-IT-01(config-vlan)# name IT_Dept
SW-IT-01(config-vlan)#exit
SW-IT-01(config)#interface Ethernet 0/0
SW-IT-01(config-if)# switchport trunk encapsulation dot1q
SW-IT-01(config-if)# switchport mode trunk
SW-IT-01(config-if)# no shutdown
SW-IT-01(config-if)# exit
SW-IT-01(config)#interface Ethernet 0/1
SW-IT-01(config-if)# switchport mode access
SW-IT-01(config-if)# switchport access vlan 40
SW-IT-01(config-if)# no shutdown
SW-IT-01(config-if)# exit
SW-IT-01(config)#do write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1476 bytes to 891 bytes[OK]
SW-IT-01(config)#

```

Рисунок 3.11 — Налаштування VLAN 40 IT_Dept на комутаторі SW-IT-01

На комутаторі SW-Mgmt-01 налаштовано VLAN 10 Management для робочої станції відповідного користувацького сегмента. Порт до комутатора ядра працює як trunk, а порт кінцевого пристрою — як access-порт VLAN 10.

```

SW-Mgmt-01#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-Mgmt-01(config)#vlan 10
SW-Mgmt-01(config-vlan)# name Management
SW-Mgmt-01(config-vlan)#exit
SW-Mgmt-01(config)#interface Ethernet 0/0
SW-Mgmt-01(config-if)# switchport trunk encapsulation dot1q
SW-Mgmt-01(config-if)# switchport mode trunk
SW-Mgmt-01(config-if)# no shutdown
SW-Mgmt-01(config-if)# exit
SW-Mgmt-01(config)#
SW-Mgmt-01(config)#interface Ethernet 0/1
SW-Mgmt-01(config-if)# switchport mode access
SW-Mgmt-01(config-if)# switchport access vlan 10
SW-Mgmt-01(config-if)# no shutdown
SW-Mgmt-01(config-if)# exit
SW-Mgmt-01(config)#do write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1478 bytes to 891 bytes[OK]
SW-Mgmt-01(config)#

```

Рисунок 3.12 — Налаштування VLAN 10 Management на комутаторі SW-Mgmt-01

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Розгортання Windows Server 2022 та базових доменних служб

Після налаштування мережевого рівня було виконано розгортання центрального інфраструктурного сервера Windows Server 2022. У межах реалізованої архітектури цей сервер виконує роль контролера домену, DNS-сервера та DHCP-сервера, тому він є одним із ключових вузлів корпоративної інфраструктури.

На початковому етапі серверу було призначено системне ім'я Windows-Server-2022. Мережевий інтерфейс було налаштовано зі статичною IP-адресою 192.168.50.10/24 у серверному сегменті VLAN 50. Як шлюз за замовчуванням використано адресу 192.168.50.254, що відповідає SVI-інтерфейсу серверного VLAN на Cisco Core L3 Switch. Використання статичної адреси для Windows Server 2022 є необхідним, оскільки від нього залежать доменні служби, внутрішній DNS і централізована видача мережевих параметрів клієнтам.

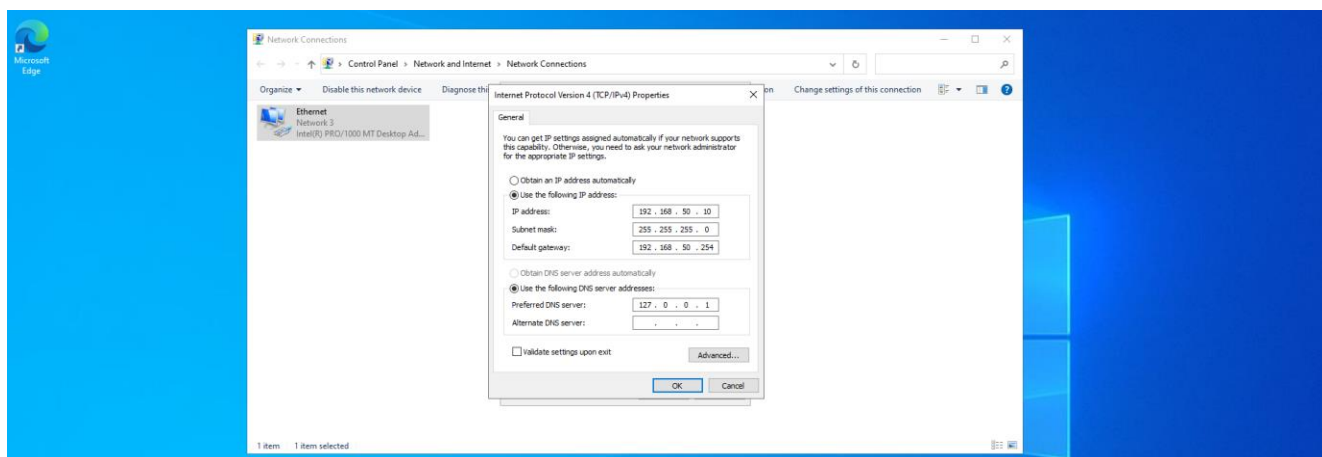


Рисунок 3.13 — Налаштування статичної IP-адресації мережевого інтерфейсу Windows Server 2022

Після базового налаштування мережі було встановлено основні інфраструктурні ролі: Active Directory Domain Services, DNS Server та DHCP Server. Інсталяція виконувалася через Windows PowerShell за допомогою команди Install-WindowsFeature із додаванням інструментів адміністрування. Такий підхід дозволяє швидко та відтворювано встановити всі необхідні компоненти для подальшого розгортання доменного середовища.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

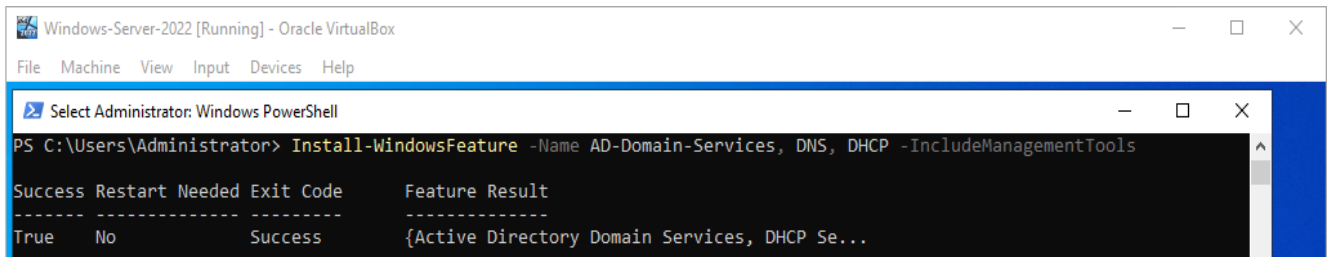


Рисунок 3.14 — Встановлення ролей AD DS, DNS Server та DHCP Server на Windows Server 2022

Наступним етапом було виконано підвищення Windows Server 2022 до контролера домену та створення нового лісу Active Directory. У межах реалізації було створено домен corp.local, який використовується як централізований простір автентифікації користувачів, комп'ютерів і службових об'єктів. Після завершення процесу сервер було перезавантажено, після чого він почав виконувати роль контролера домену.

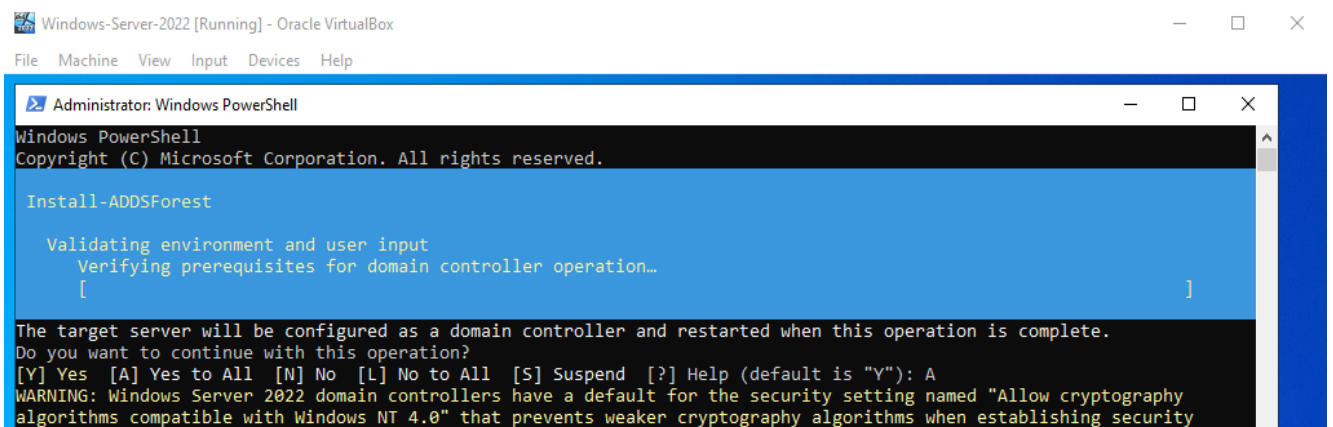


Рисунок 3.15 — Розгортання нового лісу Active Directory з доменом corp.local

Після створення доменного середовища було сформовано логічну структуру Active Directory. Для цього створено організаційні підрозділи Management, Accounting, HR_Dept та IT_Dept. Такий поділ відповідає структурі організації та дозволяє впорядкувати облікові записи користувачів за функціональними групами.

У відповідних організаційних підрозділах було створено тестові доменні облікові записи користувачів. Облікові записи розміщено у відповідних OU, що надалі дає змогу застосовувати політики доступу та безпеки адресно до конкретних підрозділів. Паролі користувачів у звіті не наводяться з міркувань безпеки.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

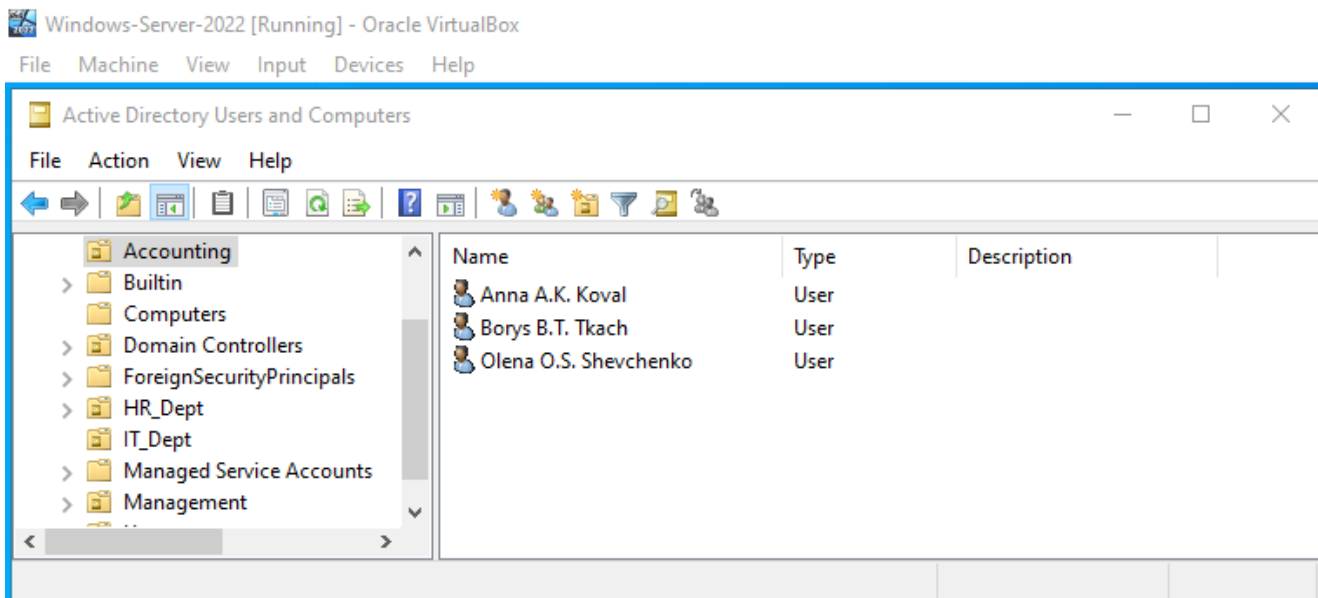


Рисунок 3.16 — Створення організаційних підрозділів і доменних користувачів в Active Directory

Налаштування служби DNS

Оскільки роль DNS Server була встановлена разом з Active Directory Domain Services, подальшим етапом стало налаштування внутрішньої DNS-зони corp.local. DNS-сервер використовується для роботи Active Directory, пошуку контролера домену клієнтськими станціями та доступу до внутрішніх інфраструктурних і прикладних сервісів за доменними іменами. [20; 21]

У зоні corp.local було створено записи типу A для основних серверних вузлів інфраструктури: Linux-App-Server, Database-Server, Backup-Server та Icinga2-Master-Server. Також було створено записи типу CNAME для зручного доступу до прикладних сервісів і службових вузлів. Зокрема, псевдонім nextcloud.corp.local вказує на Linux-App-Server, на якому розгортається корпоративний сервіс Nextcloud.

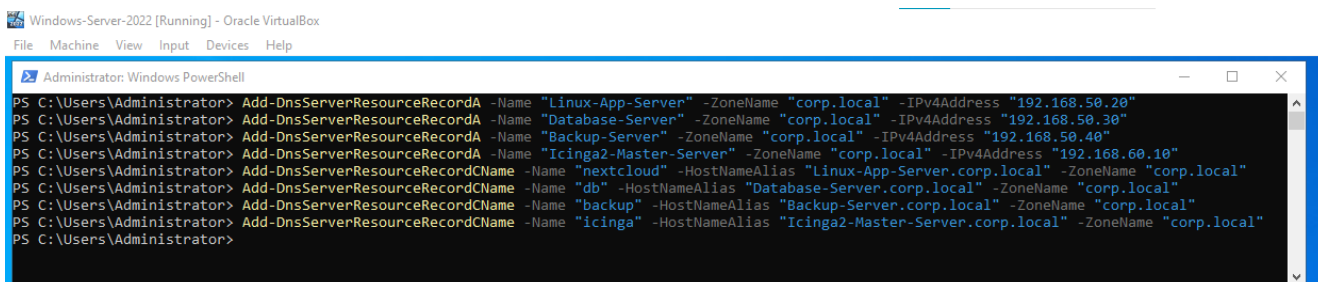


Рисунок 3.17 — Додавання DNS-записів A та CNAME у зоні corp.local

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Для повноцінного функціонування DNS також було створено зворотну зону пошуку. Вона дає змогу виконувати перетворення IP-адрес у доменні імена та використовується для діагностики, журналювання й окремих службових перевірок у корпоративному середовищі.

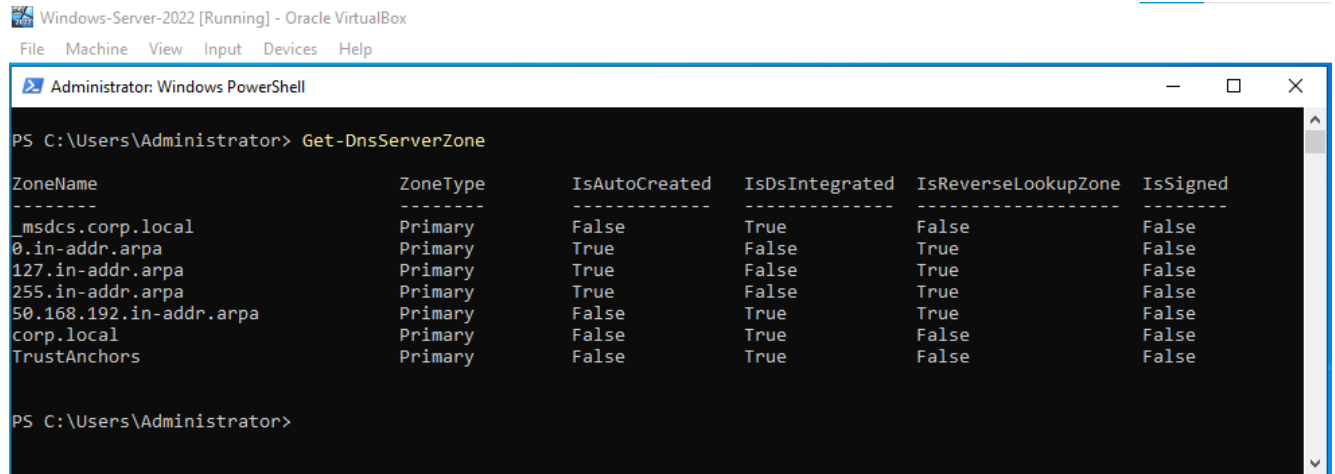


Рисунок 3.18 — Перегляд DNS-зон, створених на Windows Server 2022

Для обробки зовнішніх DNS-запитів було налаштовано DNS Forwarder. У цій конфігурації запити до зовнішніх доменів передаються на граничний маршрутизатор pfSense за адресою 192.168.1.1. Це дозволяє залишити внутрішній DNS-сервер основним для доменної інфраструктури, а зовнішні розв'язання імен спрямовувати через мережевий периметр.

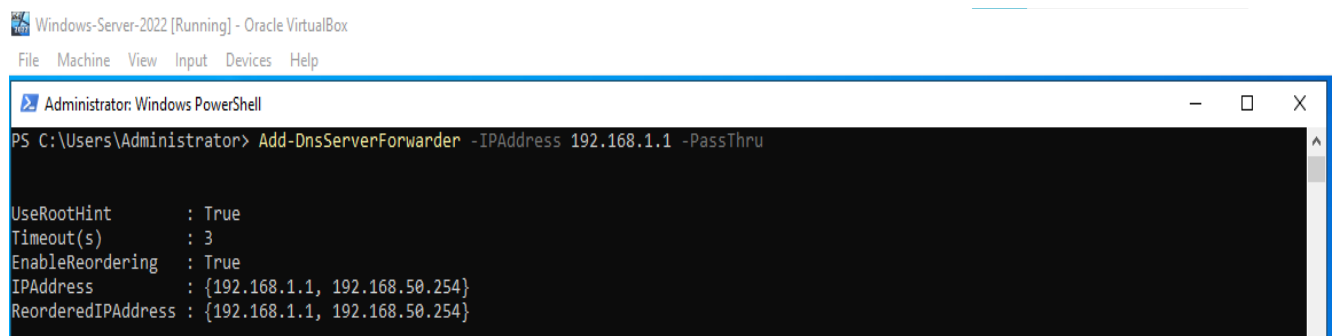


Рисунок 3.19 — Налаштування DNS Forwarder для передавання зовнішніх DNS-запитів на pfSense

Налаштування служби DHCP

Після розгортання ролі DHCP Server було створено області адресації для користувацьких VLAN. У межах реалізованої інфраструктури динамічна адресація використовується для сегментів Management, Accounting та HR. Для кожного

сегмента створено окремий DHCP-пул із власним діапазоном адрес, шлюзом за замовчуванням, DNS-сервером і доменним іменем corp.local. [22]

Для VLAN 10 Management було створено область адресації 192.168.10.0/24 із діапазоном видачі адрес 192.168.10.10–192.168.10.100 та шлюзом 192.168.10.254. Для VLAN 20 Accounting створено область 192.168.20.0/24 із діапазоном 192.168.20.10–192.168.20.100 та шлюзом 192.168.20.254. Для VLAN 30 HR створено область 192.168.30.0/24 із діапазоном 192.168.30.10–192.168.30.100 та шлюзом 192.168.30.254.

Як DNS-сервер для всіх DHCP-областей указано Windows Server 2022 з адресою 192.168.50.10. Також для клієнтів передається доменне ім'я corp.local. Після створення областей DHCP-сервер було авторизовано в Active Directory, що є необхідною умовою для коректної та безпечної роботи DHCP у доменному середовищі

```

Windows-Server-2022 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Add-DhcpServerv4Scope -Name "VLAN10_Management" -StartRange 192.168.10.10 -EndRange 192.168.10.100 -SubnetMask 255.255.255.0 -State Active
PS C:\Users\Administrator> Add-DhcpServerv4Scope -Name "VLAN20_Accounting" -StartRange 192.168.20.10 -EndRange 192.168.20.100 -SubnetMask 255.255.255.0 -State Active
PS C:\Users\Administrator> Add-DhcpServerv4Scope -Name "VLAN30_HR" -StartRange 192.168.30.10 -EndRange 192.168.30.100 -SubnetMask 255.255.255.0 -State Active
PS C:\Users\Administrator> Set-DhcpServerv4OptionValue -ScopeId 192.168.10.0 -DnsDomain "corp.local" -DnsServer 192.168.50.10 -Router 192.168.10.254
PS C:\Users\Administrator> Set-DhcpServerv4OptionValue -ScopeId 192.168.20.0 -DnsDomain "corp.local" -DnsServer 192.168.50.10 -Router 192.168.20.254
PS C:\Users\Administrator> Set-DhcpServerv4OptionValue -ScopeId 192.168.30.0 -DnsDomain "corp.local" -DnsServer 192.168.50.10 -Router 192.168.30.254
PS C:\Users\Administrator> Add-DhcpServerInDC
PS C:\Users\Administrator> Start-Service DHCPService
PS C:\Users\Administrator> Get-DhcpServerv4Scope

ScopeId      SubnetMask    Name          State    StartRange    EndRange      LeaseDuration
-----
192.168.10.0  255.255.255.0 VLAN10_Manag... Active   192.168.10.10 192.168.10.100 8.00:00:00
192.168.20.0  255.255.255.0 VLAN20_Acco... Active   192.168.20.10 192.168.20.100 8.00:00:00
192.168.30.0  255.255.255.0 VLAN30_HR     Active   192.168.30.10 192.168.30.100 8.00:00:00

PS C:\Users\Administrator>
  
```

Рисунок 3.20 — Створення DHCP-областей для користувацьких VLAN та авторизація DHCP-сервера в Active Directory

Оскільки DHCP-сервер розміщений у серверному сегменті VLAN 50, а клієнтські станції знаходяться в окремих VLAN, видача адрес узгоджується з механізмом DHCP Relay на Cisco Core L3 Switch. Саме комутатор ядра приймає

широкомовні DHCP-запити від клієнтів у VLAN 10, VLAN 20 та VLAN 30 і передає їх на Windows Server 2022 за адресою 192.168.50.10. Для адміністративного сегмента VLAN 40 динамічна адресація не використовується, оскільки адміністративна станція має статичну IP-адресу. [18; 22]

Перевірка базової працездатності доменної інфраструктури

Після завершення налаштування Windows Server 2022, Active Directory, DNS та DHCP було виконано базову перевірку працездатності створеної серверної частини інфраструктури. Оскільки встановлення ролей, створення домену, формування структури Active Directory, додавання DNS-записів і створення DHCP-областей уже підтверджено попередніми рисунками, перевірка була зосереджена на ключових функціональних елементах.

У межах перевірки було підтверджено мережеву доступність шлюзу серверного сегмента 192.168.50.254, доступність домену corp.local та коректне розв'язання внутрішніх DNS-імен основних сервісів. Результати базового тестування наведено в додатку Г.

Отримані результати підтверджують, що Windows Server 2022 коректно взаємодіє з мережевою інфраструктурою, домен corp.local доступний, а внутрішній DNS-сервер правильно обробляє запити до службових імен. Фактична перевірка отримання IP-адрес кінцевими клієнтськими вузлами через DHCP Relay виконується на наступному етапі, після введення робочих станцій в експлуатацію.

3.2. Реалізація клієнтських вузлів, адміністративної станції, серверних сервісів і резервного копіювання

Метою підрозділу є введення в роботу кінцевих вузлів і серверних компонентів, які формують практичне навантаження інфраструктури та надалі виступають об'єктами моніторингу. На цьому етапі підключаються клієнтські робочі станції, створюється адміністративна станція, розгортаються Linux-сервери, MariaDB, Nextcloud, Docker, Nginx, HTTPS-доступ і система резервного копіювання. Це потрібно для того, щоб інфраструктура не була лише мережею з

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

доменом, а містила реальні сервіси, користувачів, дані та механізми відновлення. [20; 21; 22; 24; 25; 26; 27; 28; 29]

Введення клієнтських робочих станцій у домен виконується для перевірки роботи DHCP, DNS, Active Directory і майбутнього застосування групових політик. Клієнтські вузли імітують робочі місця різних підрозділів організації та дозволяють перевірити, чи отримують вони правильні мережеві параметри, чи знаходять домен і чи можуть працювати з корпоративними ресурсами. [20; 21; 22; 23]

Адміністративна станція виділяється в окремий сегмент для безпечного керування інфраструктурою. Через неї адміністратор отримує доступ до pfSense, Cisco-комутаторів, Windows Server 2022, Linux-серверів та Icinga Web 2. Її статична адресація потрібна для стабільного застосування правил доступу, ACL і firewall-правил. [2; 3; 17]

Розгортання Database-Server і MariaDB виконується для відокремлення рівня зберігання даних від прикладного сервера. MariaDB використовується як база даних для Nextcloud, тому її працездатність напряду впливає на роботу корпоративного файлового сервісу. Окреме розміщення бази даних спрощує резервне копіювання, моніторинг і діагностику. [27]

Розгортання Linux-App-Server, Docker, Docker Compose, Nextcloud, Nginx і HTTPS виконується для створення прикладного корпоративного сервісу. Nextcloud виступає внутрішнім файловим сховищем організації, Docker ізолює прикладне середовище, Nginx організовує вебдоступ, а HTTPS забезпечує захищене підключення користувачів. Це створює реальний прикладний рівень, доступність якого надалі контролюється в Icinga 2. [24; 25; 26; 28]

Налаштування рольової моделі доступу в Nextcloud виконується для розмежування прав користувачів відповідно до підрозділів. Групи, квоти та спільні каталоги потрібні для того, щоб користувачі отримували доступ лише до необхідних файлів і не могли працювати з даними інших підрозділів без дозволу. [26]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Реалізація Backup-Server виконується для збереження критичних даних і конфігурацій. До резервного копіювання включаються файли Nextcloud, база даних MariaDB, конфігурації Docker, Nginx, SSL-сертифікати, а також конфігурації й бази Icinga. Журнал виконання backup-сценарію потрібний не лише для контролю результату копіювання, а й для подальшої перевірки його актуальності засобами моніторингу. [4]

Введення в експлуатацію клієнтських Windows-станцій

У межах лабораторної інфраструктури було розгорнуто клієнтські робочі станції під керуванням Windows. Вони моделюють робочі місця користувачів різних підрозділів організації, зокрема бухгалтерії, відділу кадрів і керівного сегмента. Кожна станція була підключена до відповідного VLAN через комутатор доступу.

Для клієнтських робочих станцій було використано автоматичне отримання мережевих параметрів через DHCP. Такий підхід відповідає раніше реалізованій моделі, у якій DHCP-сервер розміщується на Windows Server 2022 у серверному сегменті VLAN 50, а DHCP-запити з користувацьких VLAN передаються до нього через механізм DHCP Relay на Cisco Core L3 Switch.

Практичну перевірку отримання мережевих параметрів виконано на прикладі робочої станції WS-ACC-01, що належить до сегмента бухгалтерії VLAN 20. За результатами перевірки станція отримала IP-адресу 192.168.20.11, маску 255.255.255.0, шлюз 192.168.20.254, адресу DHCP-сервера 192.168.50.10 та DNS-сервер 192.168.50.10. Це підтверджує працездатність DHCP-сервера та коректну роботу DHCP Relay між користувацьким і серверним сегментами.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

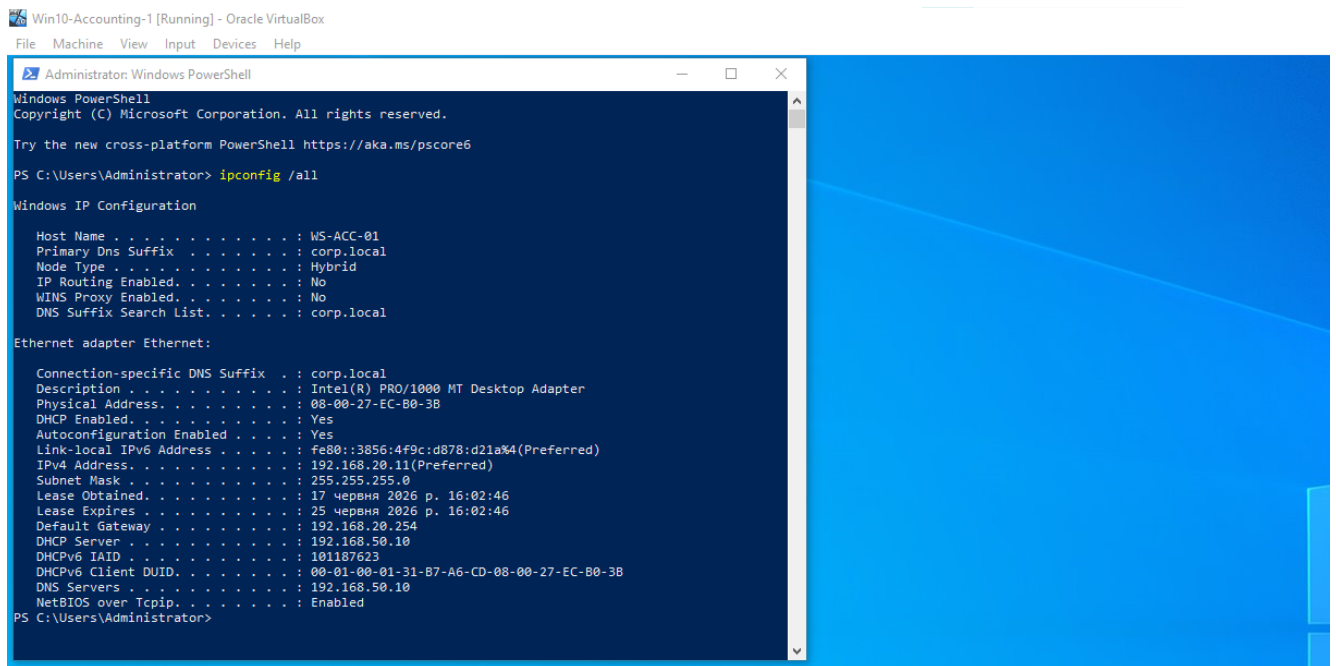


Рисунок 3.21 — Перевірка отримання мережевих параметрів клієнтською станцією WS-ACC-01 через DHCP

Після отримання мережевих параметрів було перевірено роботу внутрішнього DNS-резолвінгу. Для цього на клієнтській станції виконано запит до доменного імені corp.local. У відповіді було отримано адресу Windows Server 2022 — 192.168.50.10, що підтверджує коректну роботу внутрішнього DNS-сервера та правильне передавання DNS-параметрів клієнту через DHCP.



Рисунок 3.22 — Перевірка внутрішнього DNS-резолвінгу домену corp.local на клієнтській станції WS-ACC-01

Після перевірки мережевих параметрів і DNS-резолвінгу клієнтські робочі станції було введено до складу домену corp.local. Для цього кожній станції було призначено стандартизоване ім'я відповідно до її підрозділу. Наприклад, станція бухгалтерського сегмента отримала ім'я WS-ACC-01.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

Після приєднання до домену та перезавантаження системи було виконано перевірку членства робочої станції в домені. На прикладі WS-ACC-01 підтверджено, що комп'ютер належить до домену corp.local. Це означає, що робоча станція успішно інтегрована з Active Directory і може використовувати доменну автентифікацію користувачів.

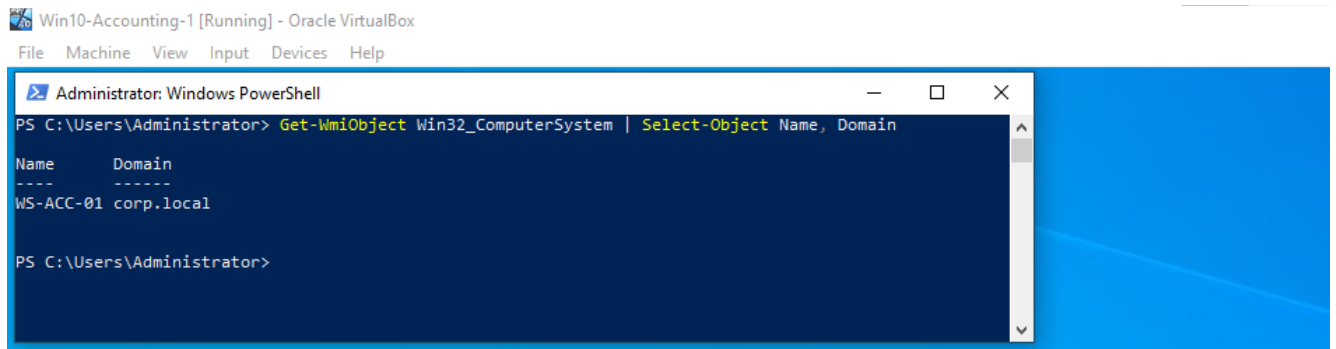


Рисунок 3.23 — Перевірка членства клієнтської робочої станції WS-ACC-01 у домені corp.local

Після введення станцій у домен їхні комп'ютерні облікові записи можуть бути розміщені у відповідних організаційних підрозділах Active Directory. Це створює основу для подальшого застосування групових політик безпеки до робочих станцій різних підрозділів. Детальна перевірка застосування GPO виконується в підрозділі 3.3, оскільки вона належить до реалізації політик доступу та безпеки.

Формування адміністративної площини керування

Після введення клієнтських станцій в експлуатацію було сформовано адміністративну площину керування інфраструктурою. Її завдання полягає в тому, щоб забезпечити централізоване й захищене адміністрування серверів, мережевого обладнання, граничного маршрутизатора pfSense та доменної інфраструктури.

До адміністративної площини входить робоча станція WS-IT-01, з якої виконуються керівні дії, а також серверні й мережеві вузли, які повинні приймати захищені адміністративні підключення. Тому спочатку було налаштовано адміністративну станцію, потім підготовлено Linux-сервери для приймання SSH-з'єднань, після чого організовано SSH- та RDP-доступ до ключових компонентів інфраструктури.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Адміністративну робочу станцію WS-IT-01 було розгорнуто під керуванням Ubuntu Desktop і розміщено в адміністративному сегменті VLAN 40 IT_Dept. Цей вузол використовується як довірене робоче місце для керування серверами, мережевим обладнанням, pfSense та системою моніторингу.

На відміну від звичайних клієнтських станцій, для WS-IT-01 було використано статичну IP-адресацію. Це необхідно для того, щоб адміністративний вузол мав постійну адресу та не залежав від роботи DHCP-служби. Станції було призначено IP-адресу 192.168.40.10/24, шлюз 192.168.40.254 і DNS-сервер 192.168.50.10. Налаштування виконувалося через NetworkManager за допомогою утиліти nmcli, після чого мережеве з'єднання було перезапущено для застосування нових параметрів.

```

Jun 17 12:19
administrator@WS-IT-01: ~/Desktop

administrator@WS-IT-01:~/Desktop$ sudo nmcli con modify "netplan-enp0s3" ipv4.addresses 192.168.40.10/24
[sudo] password for administrator:
administrator@WS-IT-01:~/Desktop$ sudo nmcli con modify "netplan-enp0s3" ipv4.gateway 192.168.40.254
administrator@WS-IT-01:~/Desktop$ sudo nmcli con modify "netplan-enp0s3" ipv4.dns "192.168.50.10"
administrator@WS-IT-01:~/Desktop$ sudo nmcli con modify "netplan-enp0s3" ipv4.method manual
administrator@WS-IT-01:~/Desktop$ sudo nmcli con down "netplan-enp0s3"
Connection 'netplan-enp0s3' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)
administrator@WS-IT-01:~/Desktop$ sudo nmcli con up "netplan-enp0s3"
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
administrator@WS-IT-01:~/Desktop$
administrator@WS-IT-01:~/Desktop$

```

Рисунок 3.24 — Налаштування статичної IP-адресації адміністративної станції WS-IT-01 за допомогою nmcli

Після підготовки адміністративної станції було виконано базове налагодження серверних вузлів, до яких надалі здійснюватиметься віддалене керування. До складу серверної частини входять Linux-App-Server, Database-Server, Backup-Server та Icinga2-Master-Server. Ці вузли розміщуються у серверному та моніторинговому сегментах і повинні мати стабільні мережеві параметри, оскільки на них розгортаються прикладні сервіси, база даних, резервне копіювання та система моніторингу.

На Linux-серверах було застосовано статичну IP-адресацію через підсистему Netplan. Практичний приклад налаштування наведено на сервері Linux-App-Server, для якого було задано адресу 192.168.50.20/24, шлюз 192.168.50.254 та DNS-сервер 192.168.50.10. Також було задано домен пошуку corp.local, що забезпечує узгодженість сервера з внутрішнім простором імен корпоративної інфраструктури.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

Для Database-Server, Backup-Server та Icinga2-Master-Server налаштування виконувалися аналогічно, але з використанням відповідних статичних IP-адрес згідно з адресним планом інфраструктури.

```

GNU nano 7.2 /etc/netplan/50-cloud-init.yaml *
network:
  version: 2
  renderer: networkd
  ethernet:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.50.20/24
      routes:
        - to: default
          via: 192.168.50.254
      nameservers:
        addresses: [192.168.50.10]
        search: [corp.local]
  
```

Рисунок 3.25 — Приклад налаштування статичної IP-адресації Linux-App-Server через Netplan

Після налаштування мережевих параметрів на Linux-серверах було виконано оновлення індексів пакетів. На рисунку 3.26 наведено приклад виконання цієї операції на Linux-App-Server. Таке оновлення потрібне для отримання актуальної інформації про доступні версії програмного забезпечення та підготовки системи до встановлення служб віддаленого керування. На інших Linux-серверах цей етап було виконано за аналогічною процедурою.

```

Linux-App-Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
admin@Linux-App-Server:~$ sudo apt update
[sudo] password for admin:
Hit:1 http://ua.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ua.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ua.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [2,067 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1,763 kB]
Get:7 http://ua.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [363 kB]
Get:8 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [177 kB]
Get:9 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [17,4 kB]
Get:10 http://ua.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,698 kB]
65% [10 Packages 970 kB/1,698 kB 57%] [6 Packages 1,346 kB/1,763 kB 76%]
399 kB/s 9
  
```

Рисунок 3.26 — Приклад оновлення індексів пакетів на Linux-App-Server перед встановленням служб адміністрування

Для забезпечення віддаленого консольного керування на Linux-серверах було встановлено пакет OpenSSH Server. Наявність SSH-служби є необхідною умовою для подальшого адміністрування серверів із виділеної адміністративної станції WS-IT-01. На рисунку 3.27 показано приклад встановлення OpenSSH Server на Linux-App-Server. На Database-Server, Backup-Server та Icinga2-Master-Server встановлення виконувалося аналогічно.

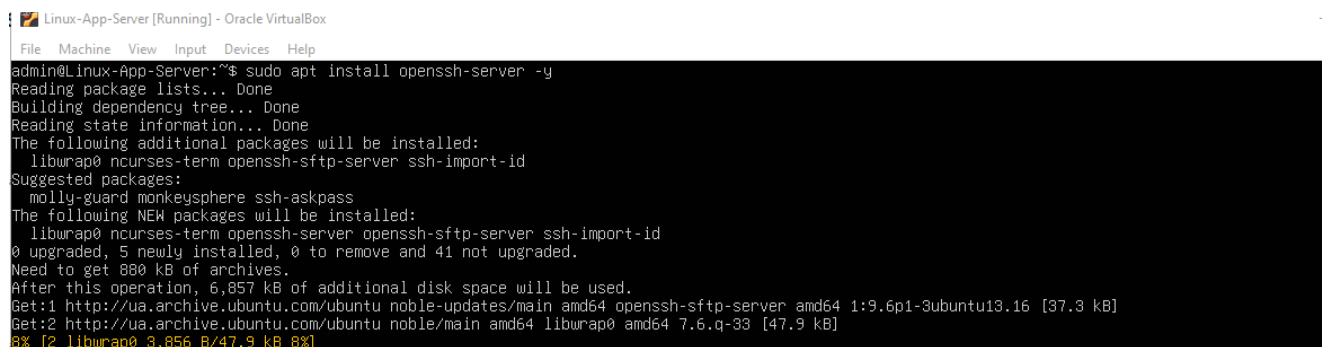


Рисунок 3.27 — Приклад встановлення OpenSSH Server на Linux-App-Server

Після підготовки серверів було налаштовано захищений SSH-доступ з адміністративної станції. На WS-IT-01 використовувалися клієнтські засоби OpenSSH, зокрема ssh-keygen, ssh-agent, ssh-add та ssh-copy-id. OpenSSH Server на адміністративній станції не є обов'язковим, оскільки вона в цій моделі виступає ініціатором підключень, а не сервером для приймання SSH-сесій.

Для підвищення рівня безпеки замість звичайної парольної автентифікації було застосовано автентифікацію за допомогою асиметричних SSH-ключів. На адміністративній станції було згенеровано пару ключів RSA довжиною 4096 біт. Приватний ключ зберігається локально на WS-IT-01, а відкритий ключ використовується для авторизації на віддалених серверах і мережевому обладнанні. Під час створення ключа було використано парольну фразу, що зменшує ризик несанкціонованого використання приватного ключа у випадку компрометації адміністративного робочого місця.

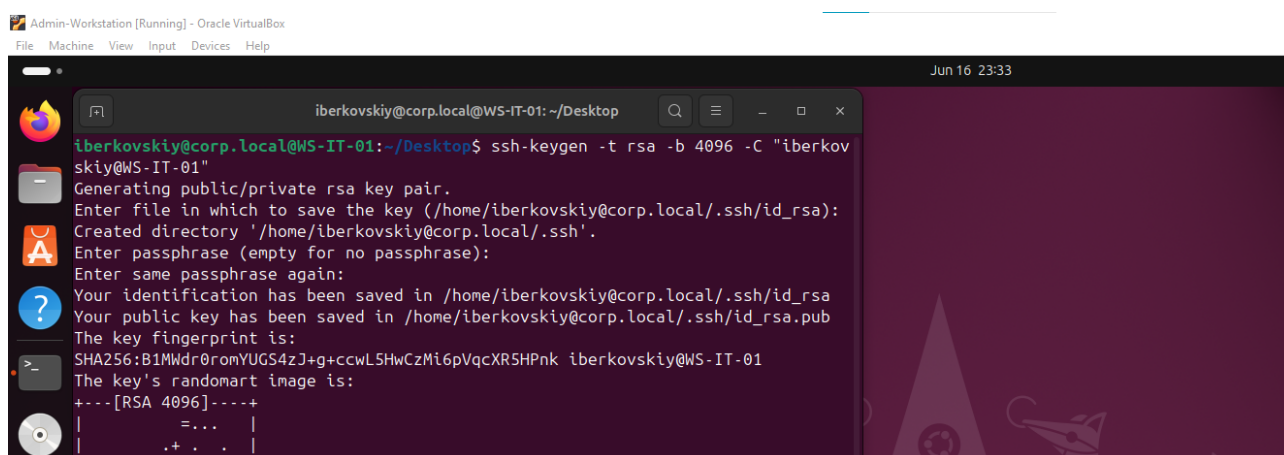


Рисунок 3.28 — Генерація пари SSH-ключів RSA на адміністративній станції WS-IT-01

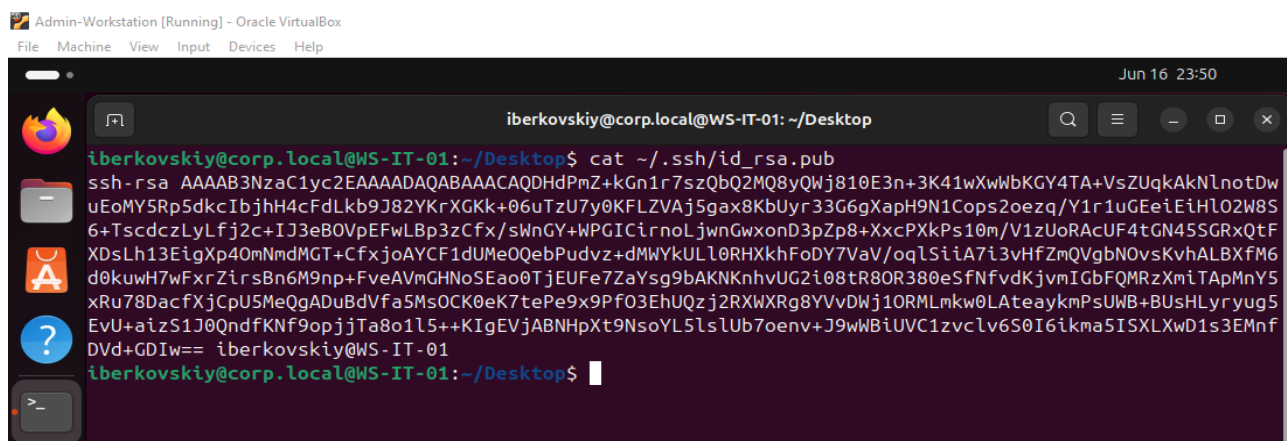
		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Для зручності подальшої роботи було запущено службу ssh-agent і додано до неї приватний SSH-ключ. Це дозволяє адміністратору один раз ввести пароленьку фразу на початку робочої сесії та надалі використовувати ключ для підключень без повторного введення пароля при кожному новому SSH-з'єднанні.

```
iberkovskiy@corp.local@WS-IT-01:~/Desktop$ eval "$(ssh-agent -s)"
ssh-add ~/.ssh/id_rsa
Agent pid 4275
Enter passphrase for /home/iberkovskiy@corp.local/.ssh/id_rsa:
Identity added: /home/iberkovskiy@corp.local/.ssh/id_rsa (iberkovskiy@WS-IT-01)
iberkovskiy@corp.local@WS-IT-01:~/Desktop$
```

Рисунок 3.29 — Ініціалізація ssh-agent і додавання приватного SSH-ключа на WS-IT-01

Перед поширенням ключа було переглянуто вміст відкритого ключа. Відкритий ключ може бути переданий на сервери та мережеве обладнання, тоді як приватний ключ залишається тільки на адміністративній станції.



```
iberkovskiy@corp.local@WS-IT-01: ~/Desktop$ cat ~/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDHDpmZ+kGn1r7szQbQ2MQ8yQWj810E3n+3K41wXwWbKGY4TA+VsZUqkAkNlnotDw
uEoMY5Rp5dkcIbjhH4cFdLkb9J82YKrXGKk+06uTzU7y0KFLZVAj5gax8KbUyr33G6gXapH9N1Cops2oezq/Y1r1uGEeiEiHlO2W8S
6+TscdczLyLfj2c+IJ3eB0VpEFwLBp3zCfx/sWnGY+WPgICirnoLjwnGwxonD3pZp8+XxcPXkPs10m/V1zUoRACUF4tGN45SGRxQtF
XDsLh13EigXp40mNmdMGT+CfxjoAYCF1dUMeOQebPudvz+dMWYkULl0RHxkhFodY7VaV/oqlSiA7i3vHFZmQVgbN0vskvhALBXfM6
d0kuwH7wFxrZirsBn6M9np+FveAVmGHNoSEao0TjEUFe7ZaYsg9bAKNKnhvUG2i08tR80R380eSfNfvdKjvmIGbFQMRzXmiTApMnY5
xRu78DacfxjCpU5MeQgADuBdVfa5Ms0CK0ek7tePe9x9PFO3EhUQzj2RXWXRg8YVvDWj10RMLmkw0LAteaykmpSUWB+BUshLYryug5
EvU+aiZS1J0QndfKNf9opjjTa8o1L5++KIgEVjABNHpXt9NsoYL5lsUub7oenv+J9wWBiUVC1zvcLv6S0I6ikma5ISXLXwD1s3EMnf
DVD+GDIw== iberkovskiy@WS-IT-01
iberkovskiy@corp.local@WS-IT-01:~/Desktop$
```

Рисунок 3.30 — Перегляд відкритого SSH-ключа на адміністративній станції WS-IT-01

Після цього відкритий ключ було передано на всі Linux-сервери інфраструктури, зокрема Linux-App-Server, Database-Server, Backup-Server та Icinga2-Master-Server. Для цього використовувалася утиліта ssh-copy-id, яка автоматично додає відкритий ключ до файлу authorized_keys на віддаленому вузлі. У звіті практичну демонстрацію цього етапу наведено на прикладі Database-Server, оскільки для інших Linux-серверів процедура виконувалася аналогічно. Це дозволило надалі виконувати SSH-підключення з адміністративної станції WS-IT-01 до серверної інфраструктури з використанням ключової автентифікації.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

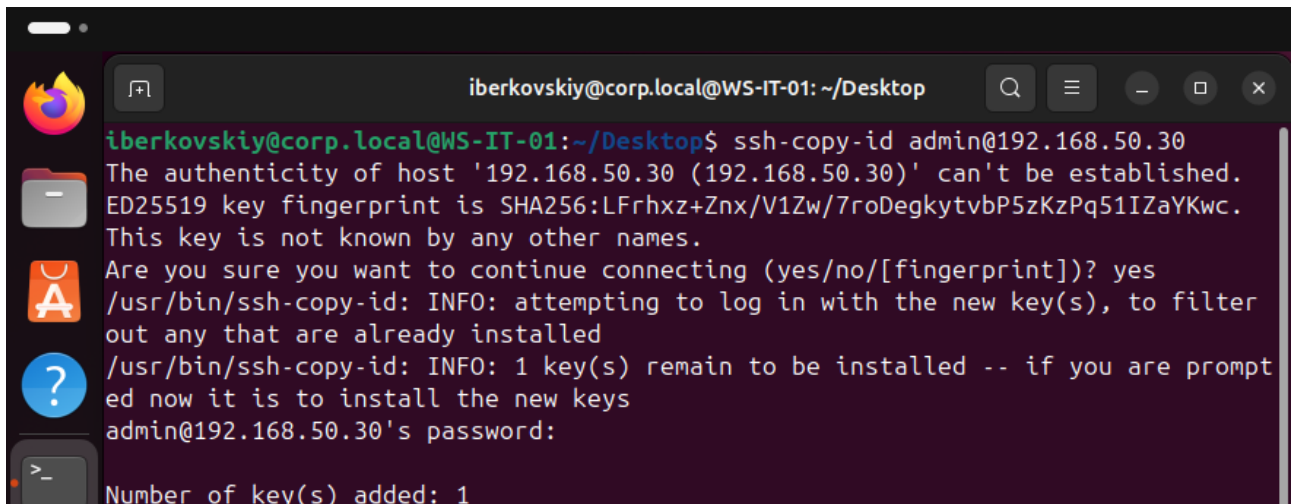


Рисунок 3.31 — Приклад передавання відкритого SSH-ключа на Database-Server за допомогою ssh-copy-id

Окремо було виконано налаштування SSH-доступу до мережевого обладнання Cisco. Як приклад наведено конфігурацію Cisco Core L3 Switch, оскільки саме він є центральним маршрутизуючим вузлом внутрішньої мережі. Для комутатора було задано доменне ім'я corp.local, згенеровано RSA-ключі, увімкнено SSH версії 2, створено локальний адміністративний обліковий запис і дозволено вхід через SSH на лініях vty.

Також було виконано імпорт відкритого SSH-ключа адміністратора в конфігурацію Cisco IOS за допомогою механізму ip ssh pubkey-chain. Це дозволяє використовувати ключову автентифікацію для доступу до мережевого обладнання. Аналогічний підхід може застосовуватися для комутаторів доступу, однак у звіті достатньо показати реалізацію на прикладі комутатора ядра.

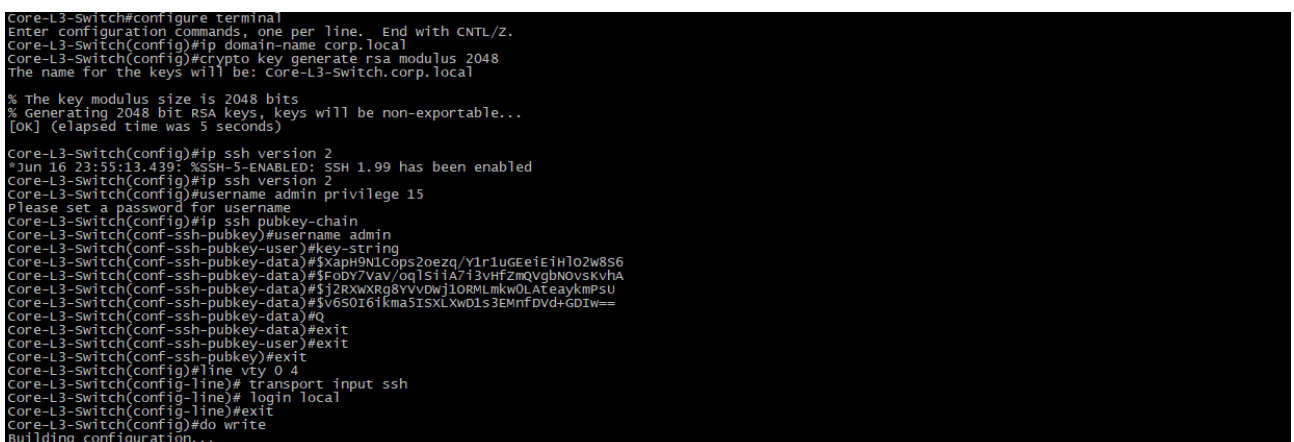


Рисунок 3.32 — Налаштування SSH-доступу та імпорт відкритого ключа на Cisco Core L3 Switch

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Для переходу в привілейований режим керування на Cisco Core L3 Switch було налаштовано enable secret та встановлено privilege level 15 для адміністративного доступу через vty-лінії. Значення секретного пароля у звіті не наводиться і на рисунку має бути приховане з міркувань безпеки.

```
Core-L3-Switch#enable
Core-L3-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#enable secret 5673##3fkjkgA
Core-L3-Switch(config)#line vty 0 4
Core-L3-Switch(config-line)# privilege level 15
Core-L3-Switch(config-line)#exit
Core-L3-Switch(config)#
Core-L3-Switch(config)#do write
Building configuration...
```

Рисунок 3.33 — Налаштування привілейованого адміністративного доступу на Cisco Core L3 Switch

Для спрощення адміністрування на WS-IT-01 було створено файл SSH-профілів ~/.ssh/config. У ньому описано короткі імена для підключення до pfSense, Cisco Core L3 Switch, комутаторів доступу та Linux-серверів. Це дозволяє адміністратору підключатися до вузлів за зручними іменами, не вводячи щоразу повну IP-адресу та додаткові параметри з'єднання.

Для мережевого обладнання Cisco у файлі конфігурації додатково вказано параметри сумісності з алгоритмами SSH, які використовуються лабораторними образами Cisco IOS. Такі винятки застосовуються лише для мережевого обладнання і не поширюються на Linux-сервери. Фрагменти конфігураційного файлу SSH-профілів наведено в додатку Д на рисунках Д.1 та Д.2.

Після створення SSH-профілів було перевірено підключення до Cisco Core L3 Switch. Успішне відкриття SSH-сесії та перехід до режиму конфігурації підтверджує, що адміністративна станція має доступ до мережевого обладнання через захищений канал керування.

Admin-Workstation [Running] - Oracle VirtualBox
File Machine View Input Devices Help

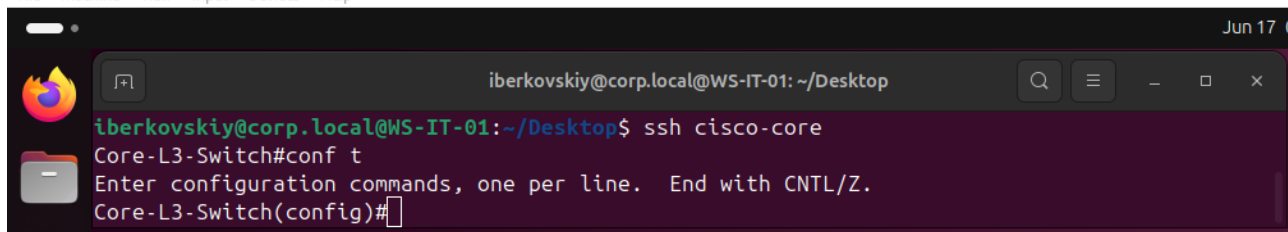


Рисунок 3.34 — Перевірка SSH-доступу з адміністративної станції до Cisco Core L3 Switch

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Окремо було перевірено SSH-доступ до Linux-серверів. Практичну демонстрацію цієї перевірки наведено на прикладі Database-Server, оскільки доступ до Linux-App-Server, Backup-Server та Icinga2-Master-Server організовано за аналогічною схемою. Результат перевірки SSH-підключення до Database-Server наведено в додатку Д на рисунку Д.3.

Для графічного адміністрування Windows Server 2022 з адміністративної станції Ubuntu було встановлено клієнт Remmina з підтримкою протоколу RDP. Це дає змогу виконувати кросплатформене керування доменною інфраструктурою з єдиного адміністративного робочого місця.

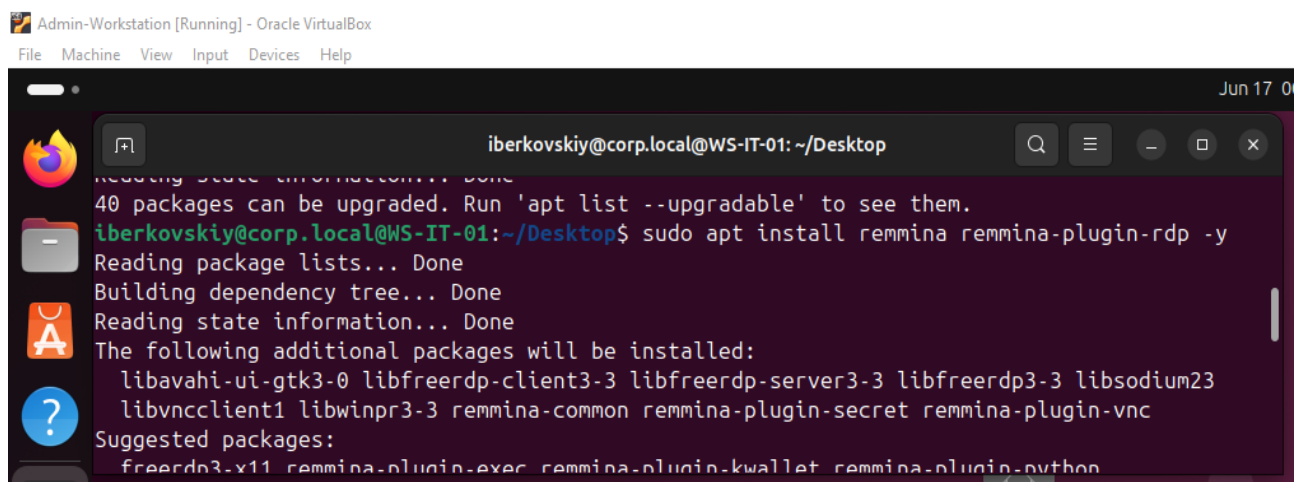


Рисунок 3.35 — Встановлення клієнта Remmina для RDP-доступу на адміністративній станції Ubuntu

У Remmina було створено профіль підключення до Windows Server 2022 за адресою 192.168.50.10. Для автентифікації використовується доменний обліковий запис адміністратора у форматі Administrator@corp.local. Конфігурацію RDP-профілю наведено в додатку Д на рисунку Д.4.

Після створення профілю було виконано підключення до Windows Server 2022. Відображення Server Manager і параметрів локального сервера підтверджує працездатність RDP-доступу з адміністрації

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

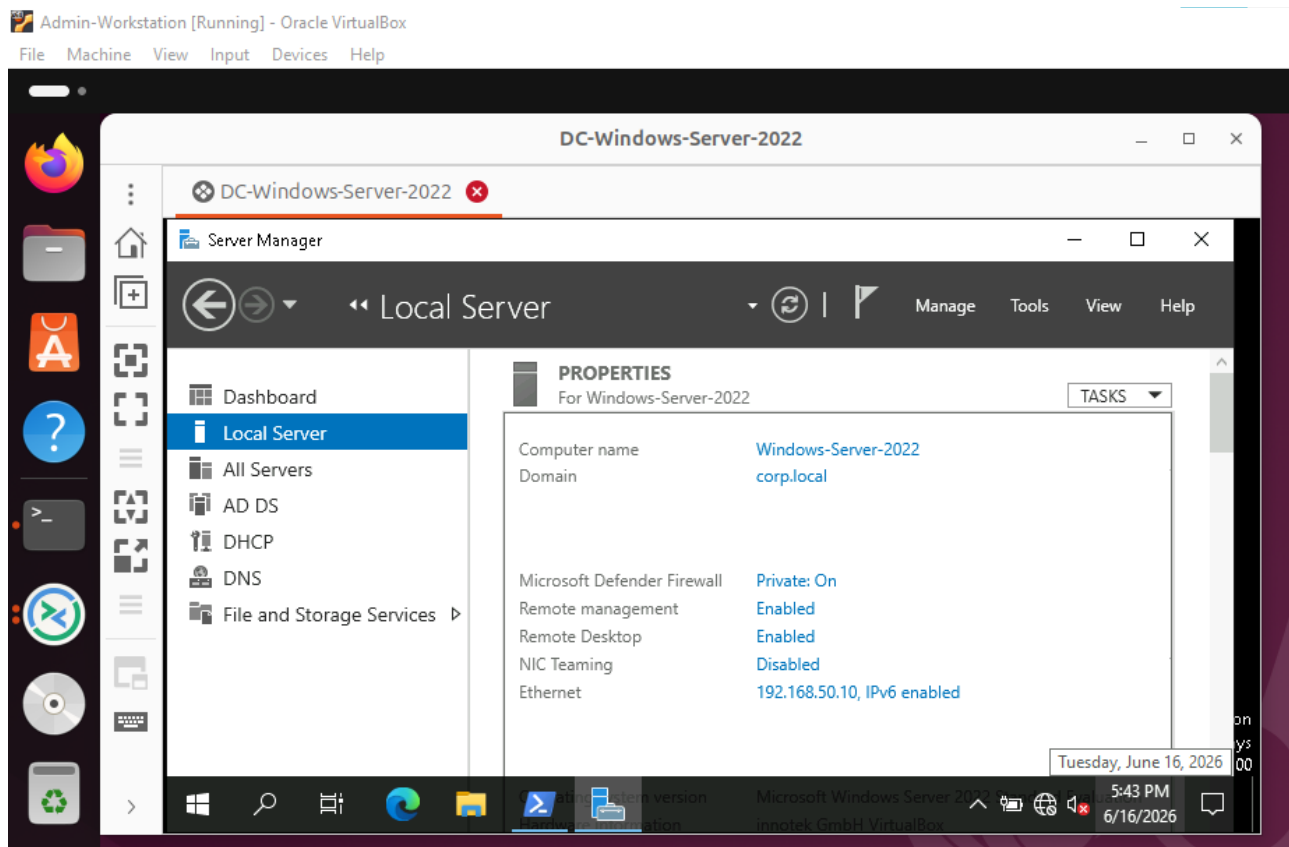


Рисунок 3.36 — Перевірка RDP-доступу до Windows Server 2022 з адміністративної станції WS-IT-01

Налаштування MariaDB на підготовленому Database-Server

Наступним етапом було налаштовано систему керування базами даних MariaDB на сервері Database-Server. На попередньому етапі цей вузол уже було підготовлено до адміністрування: він мав статичну IP-адресу 192.168.50.30 та був доступний через SSH з адміністративної станції WS-IT-01. У цій інфраструктурі Database-Server виконує роль окремого вузла зберігання даних для корпоративного сервісу Nextcloud.

Перед інсталяцією СУБД було оновлено індекси пакетів операційної системи, а потім встановлено пакет mariadb-server разом із необхідними залежностями. Ці дії забезпечили підготовку серверного середовища до подальшої конфігурації MariaDB. Приклади оновлення індексів пакетів і встановлення MariaDB наведено в додатку Е на рисунках Е.1 та Е.2.

Далі було виконано базове гартування MariaDB за допомогою утиліти `mysql_secure_installation`. У межах цього етапу було налаштовано обліковий запис `root`, видалено анонімних користувачів, заборонено віддалений вхід для `root`,

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

видалено тестову базу даних і оновлено таблиці привілеїв. Приклад виконання цієї процедури наведено в додатку Е на рисунку Е.3.

Для роботи корпоративного файлового сервісу Nextcloud у MariaDB було створено окрему базу даних nextcloud_db. Також було створено сервісного користувача nc_user, якому надано права доступу лише до цієї бази даних. Доступ користувача nc_user обмежено IP-адресою Linux-App-Server — 192.168.50.20, що відповідає принципу мінімальних привілеїв і зменшує ризик підключення до СУБД з інших вузлів мережі.

```
admin@Database-Server:~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.11.14-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> CREATE DATABASE nextcloud_db CHARACTER SET utf8mb4 COLLATE utf
8mb4_general_ci;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> CREATE USER 'nc_user'@'192.168.50.20' IDENTIFIED BY 'H3F#GSU02
535K5';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nc_user'@'192.168.5
0.20';
Query OK, 0 rows affected (0.006 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye
admin@Database-Server:~$
```

Рисунок 3.37 — Створення бази даних nextcloud_db та сервісного користувача nc_user для Nextcloud

Оскільки Nextcloud розміщується на окремому сервері Linux-App-Server, сервер баз даних має приймати підключення з прикладного сервера, а не лише з локального інтерфейсу. Для цього у конфігураційному файлі /etc/mysql/mariadb.conf.d/50-server.cnf параметр bind-address було змінено на статичну IP-адресу Database-Server — 192.168.50.30. Завдяки цьому MariaDB прослуховує потрібний внутрішній інтерфейс серверного сегмента та може взаємодіяти з Linux-App-Server.

```

admin@Database-Server: ~
GNU nano 2.2 /etc/mysql/mariadb.conf.d/50-server.cnf
#
# * basic settings
#
user                = mysql
pid-file             = /run/mysqld/mysqld.pid
basedir              = /usr
datadir              = /usr/lib/mysql
tmpdir               = /tmp

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address         = 192.168.50.30

# * Fine Tuning
#
key_buffer_size      = 128M
max_allowed_packet   = 16
thread_stack         = 192K
thread_cache_size    = 8
# This replaces the startup script and checks myisam tables if needed
# the first time they are touched
mysqld_safe_options  = --skip
max_connections      = 100
table_cache          = 64

# * Logging and Replication
#
# Note: The configured log file or its directory need to be created
# and be writable by the mysql user, e.g.:
# $ sudo mkdir -p 2750 /var/log/mysql
# $ sudo chown mysql /var/log/mysql
# Both location gets rotated by the cronjob.
# Be aware that this log type is a performance killer.
# Recommended only changing this at runtime for short testing periods if needed!
general_log_file     = /var/log/mysql/mysql.log
general_log          = 1

# When running under systemd, error logging goes via stdout/stderr to journald
# and when running legacy init, error logging goes to syslog due to
# /etc/mysql/conf.d/mariadb.conf.d/50-mysqld_safe.cnf
# Enable this if you want to have error logging into a separate file
error_log = /var/log/mysql/error.log
# Enable the slow query log to see queries with especially long duration
log_slow_query_file  = /var/log/mysql/mariadb-slow.log
log_slow_query_time  = 10
log_slow_verbosity   = query_plan,explain
log_queries_not_using_indexes
log_slow_min_examined_row_limit = 1000

# The following can be used as easy to replay backup logs or for replication.
# Note: If you are setting up a replica, see README.Debian about other
# settings you may need to change.
server-id            = 1
log_bin              = /var/log/mysql/mysql-bin.log
expire_logs_days     = 10
max_binlog_size      = 100M

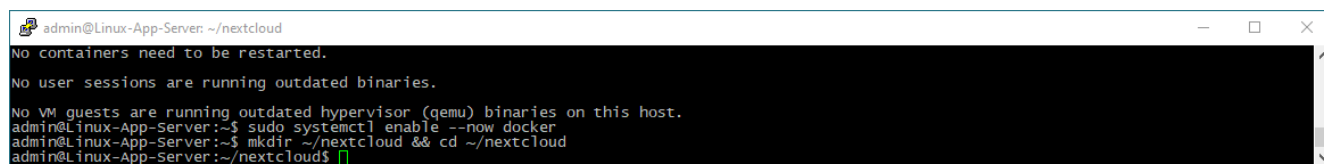
# * SSL/TLS
#
# For documentation, please read
File Name to write: etc/mysql/mariadb.conf.d/50-server.cnf
[Ctrl] [F] [G] [H] [I] [J] [K] [L] [M] [N] [O] [P] [Q] [R] [S] [T] [U] [V] [W] [X] [Y] [Z] [Esc] [F1] [F2] [F3] [F4] [F5] [F6] [F7] [F8] [F9] [F10] [F11] [F12] [F13] [F14] [F15] [F16] [F17] [F18] [F19] [F20] [F21] [F22] [F23] [F24] [F25] [F26] [F27] [F28] [F29] [F30] [F31] [F32] [F33] [F34] [F35] [F36] [F37] [F38] [F39] [F40] [F41] [F42] [F43] [F44] [F45] [F46] [F47] [F48] [F49] [F50] [F51] [F52] [F53] [F54] [F55] [F56] [F57] [F58] [F59] [F60] [F61] [F62] [F63] [F64] [F65] [F66] [F67] [F68] [F69] [F70] [F71] [F72] [F73] [F74] [F75] [F76] [F77] [F78] [F79] [F80] [F81] [F82] [F83] [F84] [F85] [F86] [F87] [F88] [F89] [F90] [F91] [F92] [F93] [F94] [F95] [F96] [F97] [F98] [F99] [F100] [F101] [F102] [F103] [F104] [F105] [F106] [F107] [F108] [F109] [F110] [F111] [F112] [F113] [F114] [F115] [F116] [F117] [F118] [F119] [F120] [F121] [F122] [F123] [F124] [F125] [F126] [F127] [F128] [F129] [F130] [F131] [F132] [F133] [F134] [F135] [F136] [F137] [F138] [F139] [F140] [F141] [F142] [F143] [F144] [F145] [F146] [F147] [F148] [F149] [F150] [F151] [F152] [F153] [F154] [F155] [F156] [F157] [F158] [F159] [F160] [F161] [F162] [F163] [F164] [F165] [F166] [F167] [F168] [F169] [F170] [F171] [F172] [F173] [F174] [F175] [F176] [F177] [F178] [F179] [F180] [F181] [F182] [F183] [F184] [F185] [F186] [F187] [F188] [F189] [F190] [F191] [F192] [F193] [F194] [F195] [F196] [F197] [F198] [F199] [F200] [F201] [F202] [F203] [F204] [F205] [F206] [F207] [F208] [F209] [F210] [F211] [F212] [F213] [F214] [F215] [F216] [F217] [F218] [F219] [F220] [F221] [F222] [F223] [F224] [F225] [F226] [F227] [F228] [F229] [F230] [F231] [F232] [F233] [F234] [F235] [F236] [F237] [F238] [F239] [F240] [F241] [F242] [F243] [F244] [F245] [F246] [F247] [F248] [F249] [F250] [F251] [F252] [F253] [F254] [F255] [F256] [F257] [F258] [F259] [F260] [F261] [F262] [F263] [F264] [F265] [F266] [F267] [F268] [F269] [F270] [F271] [F272] [F273] [F274] [F275] [F276] [F277] [F278] [F279] [F280] [F281] [F282] [F283] [F284] [F285] [F286] [F287] [F288] [F289] [F290] [F291] [F292] [F293] [F294] [F295] [F296] [F297] [F298] [F299] [F300] [F301] [F302] [F303] [F304] [F305] [F306] [F307] [F308] [F309] [F310] [F311] [F312] [F313] [F314] [F315] [F316] [F317] [F318] [F319] [F320] [F321] [F322] [F323] [F324] [F325] [F326] [F327] [F328] [F329] [F330] [F331] [F332] [F333] [F334] [F335] [F336] [F337] [F338] [F339] [F340] [F341] [F342] [F343] [F344] [F345] [F346] [F347] [F348] [F349] [F350] [F351] [F352] [F353] [F354] [F355] [F356] [F357] [F358] [F359] [F360] [F361] [F362] [F363] [F364] [F365] [F366] [F367] [F368] [F369] [F370] [F371] [F372] [F373] [F374] [F375] [F376] [F377] [F378] [F379] [F380] [F381] [F382] [F383] [F384] [F385] [F386] [F387] [F388] [F389] [F390] [F391] [F392] [F393] [F394] [F395] [F396] [F397] [F398] [F399] [F400] [F401] [F402] [F403] [F404] [F405] [F406] [F407] [F408] [F409] [F410] [F411] [F412] [F413] [F414] [F415] [F416] [F417] [F418] [F419] [F420] [F421] [F422] [F423] [F424] [F425] [F426] [F427] [F428] [F429] [F430] [F431] [F432] [F433] [F434] [F435] [F436] [F437] [F438] [F439] [F440] [F441] [F442] [F443] [F444] [F445] [F446] [F447] [F448] [F449] [F450] [F451] [F452] [F453] [F454] [F455] [F456] [F457] [F458] [F459] [F460] [F461] [F462] [F463] [F464] [F465] [F466] [F467] [F468] [F469] [F470] [F471] [F472] [F473] [F474] [F475] [F476] [F477] [F478] [F479] [F480] [F481] [F482] [F483] [F484] [F485] [F486] [F487] [F488] [F489] [F490] [F491] [F492] [F493] [F494] [F495] [F496] [F497] [F498] [F499] [F500] [F501] [F502] [F503] [F504] [F505] [F506] [F507] [F508] [F509] [F510] [F511] [F512] [F513] [F514] [F515] [F516] [F517] [F518] [F519] [F520] [F521] [F522] [F523] [F524] [F525] [F526] [F527] [F528] [F529] [F530] [F531] [F532] [F533] [F534] [F535] [F536] [F537] [F538] [F539] [F540] [F541] [F542] [F543] [F544] [F545] [F546] [F547] [F548] [F549] [F550] [F551] [F552] [F553] [F554] [F555] [F556] [F557] [F558] [F559] [F560] [F561] [F562] [F563] [F564] [F565] [F566] [F567] [F568] [F569] [F570] [F571] [F572] [F573] [F574] [F575] [F576] [F577] [F578] [F579] [F580] [F581] [F582] [F583] [F584] [F585] [F586] [F587] [F588] [F589] [F590] [F591] [F592] [F593] [F594] [F595] [F596] [F597] [F598] [F599] [F600] [F601] [F602] [F603] [F604] [F605] [F606] [F607] [F608] [F609] [F610] [F611] [F612] [F613] [F614] [F615] [F616] [F617] [F618] [F619] [F620] [F621] [F622] [F623] [F624] [F625] [F626] [F627] [F628] [F629] [F630] [F631] [F632] [F633] [F634] [F635] [F636] [F637] [F638] [F639] [F640] [F641] [F642] [F643] [F644] [F645] [F646] [F647] [F648] [F649] [F650] [F651] [F652] [F653] [F654] [F655] [F656] [F657] [F658] [F659] [F660] [F661] [F662] [F663] [F664] [F665] [F666] [F667] [F668] [F669] [F670] [F671] [F672] [F673] [F674] [F675] [F676] [F677] [F678] [F679] [F680] [F681] [F682] [F683] [F684] [F685] [F686] [F687] [F688] [F689] [F690] [F691] [F692] [F693] [F694] [F695] [F696] [F697] [F698] [F699] [F700] [F701] [F702] [F703] [F704] [F705] [F706] [F707] [F708] [F709] [F710] [F711] [F712] [F713] [F714] [F715] [F716] [F717] [F718] [F719] [F720] [F721] [F722] [F723] [F724] [F725] [F726] [F727] [F728] [F729] [F730] [F731] [F732] [F733] [F734] [F735] [F736] [F737] [F738] [F739] [F740] [F741] [F742] [F743] [F744] [F745] [F746] [F747] [F748] [F749] [F750] [F751] [F752] [F753] [F754] [F755] [F756] [F757] [F758] [F759] [F760] [F761] [F762] [F763] [F764] [F765] [F766] [F767] [F768] [F769] [F770] [F771] [F772] [F773] [F774] [F775] [F776] [F777] [F778] [F779] [F780] [F781] [F782] [F783] [F784] [F785] [F786] [F787] [F788] [F789] [F790] [F791] [F792] [F793] [F794] [F795] [F796] [F797] [F798] [F799] [F800] [F801] [F802] [F803] [F804] [F805] [F806] [F807] [F808] [F809] [F810] [F811] [F812] [F813] [F814] [F815] [F816] [F817] [F818] [F819] [F820] [F821] [F822] [F823] [F824] [F825] [F826] [F827] [F828] [F829] [F830] [F831] [F832] [F833] [F834] [F835] [F836] [F837] [F838] [F839] [F840] [F841] [F842] [F843] [F844] [F845] [F846] [F847] [F848] [F849] [F850] [F851] [F852] [F853] [F854] [F855] [F856] [F857] [F858] [F859] [F860] [F861] [F862] [F863] [F864] [F865] [F866] [F867] [F868] [F869] [F870] [F871] [F872] [F873] [F874] [F875] [F876] [F877] [F878] [F879] [F880] [F881] [F882] [F883] [F884] [F885] [F886] [F887] [F888] [F889] [F890] [F891] [F892] [F893] [F894] [F895] [F896] [F897] [F898] [F899] [F900] [F901] [F902] [F903] [F904] [F905] [F906] [F907] [F908] [F909] [F910] [F911] [F912] [F913] [F914] [F915] [F916] [F917] [F918] [F919] [F920] [F921] [F922] [F923] [F924] [F925] [F926] [F927] [F928] [F929] [F930] [F931] [F932] [F933] [F934] [F935] [F936] [F937] [F938] [F939] [F940] [F941] [F942] [F943] [F944] [F945] [F946] [F947] [F948] [F949] [F950] [F951] [F952] [F953] [F954] [F955] [F956] [F957] [F958] [F959] [F960] [F961] [F962] [F963] [F964] [F965] [F966] [F967] [F968] [F969] [F970] [F971] [F972] [F973] [F974] [F975] [F976] [F977] [F978] [F979] [F980] [F981] [F982] [F983] [F984] [F985] [F986] [F987] [F988] [F989] [F990] [F991] [F992] [F993] [F994] [F995] [F996] [F997] [F998] [F999] [F1000] [F1001] [F1002] [F1003] [F1004] [F1005] [F1006] [F1007] [F1008] [F1009] [F1010] [F1011] [F1012] [F1013] [F1014] [F1015] [F1016] [F1017] [F1018] [F1019] [F1020] [F1021] [F1022] [F1023] [F1024] [F1025] [F1026] [F1027] [F1028] [F1029] [F1030] [F1031] [F1032] [F1033] [F1034] [F1035] [F1036] [F1037] [F1038] [F1039] [F1040] [F1041] [F1042] [F1043] [F1044] [F1045] [F1046] [F1047] [F1048] [F1049] [F1050] [F1051] [F1052] [F1053] [F1054] [F1055] [F1056] [F1057] [F1058] [F1059] [F1060] [F1061] [F1062] [F1063] [F1064] [F1065] [F1066] [F1067] [F1068] [F1069] [F1070] [F1071] [F1072] [F1073] [F1074] [F1075] [F1076] [F1077] [F1078] [F1079] [F1080] [F1081] [F1082] [F1083] [F1084] [F1085] [F1086] [F1087] [F1088] [F1089] [F1090] [F1091] [F1092] [F1093] [F1094] [F1095] [F1096] [F1097] [F1098] [F1099] [F1100] [F1101] [F1102] [F1103] [F1104] [F1105] [F1106] [F1107] [F1108] [F1109] [F1110] [F1111] [F1112] [F1113] [F1114] [F1115] [F1116] [F1117] [F1118] [F1119] [F1120] [F1121] [F1122] [F1123] [F1124] [F1125] [F1126] [F1127] [F1128] [F1129] [F1130] [F1131] [F1132] [F1133] [F1134] [F1135] [F1136] [F1137] [F1138] [F1139] [F1140] [F1141] [F1142] [F1143] [F1144] [F1145] [F1146] [F1147] [F1148] [F1149] [F1150] [F1151] [F1152] [F1153] [F1154] [F1155] [F1156] [F1157] [F1158] [F1159] [F1160] [F1161] [F1162] [F1163] [F1164] [F1165] [F1166] [F1167] [F1168] [F1169] [F1170] [F1171] [F1172] [F1173] [F1174] [F1175] [F1176] [F1177] [F1178] [F1179] [F1180] [F1181] [F1182] [F1183] [F1184] [F1185] [F1186] [F1187] [F1188] [F1189] [F1190] [F1191] [F1192] [F1193] [F1194] [F1195] [F1196] [F1197] [F1198] [F1199] [F1200] [F1201] [F1202] [F1203] [F1204] [F1205] [F1206] [F1207] [F1208] [F1209] [F1210] [F1211] [F1212] [F1213] [F1214] [F1215] [F1216] [F1217] [F1218] [F1219] [F1220] [F1221] [F1222] [F1223] [F1224] [F1225] [F1226] [F1227] [F1228] [F1229] [F1230] [F1231] [F1232] [F1233] [F1234] [F1235] [F1236] [F1237] [F1238] [F1239] [F1240] [F1241] [F1242] [F1243] [F1244] [F1245] [F1246] [F1247] [F1248] [F1249] [F1250] [F1251] [F1252] [F1253] [F1254] [F1255] [F1256] [F1257] [F1258] [F1259] [F1260] [F1261] [F1262] [F1263] [F1264] [F1265] [F1266] [F1267] [F1268] [F1269] [F1270] [F1271] [F1272] [F1273] [F1274] [F1275] [F1276] [F1277] [F1278] [F1279] [F1280] [F1281] [F1282] [F1283] [F1284] [F1285] [F1286] [F1287] [F1288] [F1289] [F1290] [F1291] [F1292] [F1293] [F1294] [F1295] [F1296] [F1297] [F1298] [F1299] [F1300] [F1301] [F1302] [F1303] [F1304] [F1305] [F1306] [F1307] [F1308] [F1309] [F1310] [F1311] [F1312] [F1313] [F1314] [F1315] [F1316] [F1317] [F1318] [F1319] [F1320] [F1321] [F1322] [F1323] [F1324] [F1325] [F1326] [F1327] [F1328] [F1329] [F1330] [F1331] [F1332] [F1333] [F1334] [F1335] [F1336] [F1337] [F1338] [F1339] [F1340] [F1341] [F1342] [F1343] [F1344] [F1345] [F1346] [F1347] [F1348] [F1349] [F1350] [F1351] [F1352] [F1353] [F1354] [F1355] [F1356] [F1357] [F1358] [F1359] [F1360] [F1361] [F1362] [F1363] [F1364] [F1365] [F1366] [F1367] [F1368] [F1369] [F1370] [F1371] [F1372] [F1373] [F1374] [F1375] [F1376] [F1377] [F1378] [F1379] [F1380] [F1381] [F1382] [F1383] [F1384] [F1385] [F1386] [F1387] [F1388] [F1389] [F1390] [F1391] [F1392] [F1393] [F1394] [F1395] [F1396] [F1397] [F1398] [F1399] [F1400] [F1401] [F1402] [F1403] [F1404] [F1405] [F1406] [F1407] [F1408] [F1409] [F1410] [F1411] [F1412] [F1413] [F1414] [F1415] [F1416] [F1417] [F1418] [F1419] [F1420] [F1421] [F1422] [F1423] [F1424] [F1425] [F1426] [F1427] [F1428] [F1429] [F1430] [F1431] [F1432] [F1433] [F1434] [F1435] [F1436] [F1437] [F1438] [F1439] [F1440] [F1441] [F1442] [F1443] [F1444] [F1445] [F1446] [F1447] [F1448] [F1449] [F1450] [F1451] [F1452] [F1453] [F1454] [F1455] [F1456] [F1457] [F1458] [F1459] [F1460] [F1461] [F1462] [F1463] [F1464] [F1465] [F1466] [F1467] [F1468] [F1469] [F1470] [F1471] [F1472] [F1473] [F1474] [F1475] [F1476] [F1477] [F1478] [F1479] [F1480] [F1481] [F1482] [F1483] [F1484] [F1485] [F1486] [F1487] [F1488] [F1489] [F1490] [F1491] [F1492] [F1493] [F1494] [F1495] [F1496] [F1497] [F1498] [F1499] [F1500] [F1501] [F1502] [F1503] [F1504] [F1505] [F1506] [F1507] [F1508] [F1509] [F1510] [F1511] [F1512] [F1513] [F1514] [F1515] [F1516] [F1517] [F1518] [F1519] [F1520] [F1521] [F1522] [F1523] [F1524] [F1525] [F1526] [F1527] [F1528] [F1529] [F1530] [F1531] [F1532] [F1533] [F1534] [F1535] [F1536] [F1537] [F1538] [F1539] [F1540] [F1541] [F1542] [F1543] [F1544] [F1545] [F1546] [F1547] [F1548] [F1549] [F1550] [F1551] [F1552] [F1553] [F1554] [F1555] [F1556] [F1557] [F1558] [F1559] [F1560] [F1561] [F1562] [F1563] [F1564] [F1565] [F1566] [F1567] [F1568] [F1569] [F1570] [F1571] [F1572] [F1573] [F1574] [F1575] [F1576] [F1577] [F1578] [F1579] [F1580] [F1581] [F1582] [F1583] [F1584] [F1585] [F1586] [F1587] [F1588] [F1589] [F1590] [F1591] [F1592] [F1593] [F1594] [F1595] [F1596] [F1597] [F1598] [F1599] [F1600] [F1601] [F1602] [F1603] [F1604] [F1605] [F1606] [F1607] [F1608] [F1609] [F1610] [F1611] [F1612] [F1613] [F1614] [F1615] [F1616] [F1617] [F1618] [F1619] [F1620] [F1621] [F1622] [F1623] [F1624] [F1625] [F1626] [F1627] [F1628] [F1629] [F1630] [F1631] [F1632] [F1633] [F1634] [F1635] [F1636] [F1637] [F1638] [F1639] [F1640] [F1641] [F1642] [F1643] [F1644] [F1645] [F1646] [F1647] [F1648] [F1649] [F1650] [F1651] [F1652] [F1653] [F1654] [F1655] [F1656] [F1657] [F1658] [F1659] [F1660] [F1661] [F1662] [F1663] [F1664] [F1665] [F1666] [F1667] [F1668] [F1669] [F1670] [F1671] [F1672] [F1673] [F1674] [F1675] [F1676] [F1677] [F1678] [F1679] [F1680] [F1681] [F1682] [F1683] [F1684] [F1685] [F1686] [F1687] [F1688] [F1689] [F1690] [F1691] [F1692] [F1693] [F1694] [F1695] [F1696] [F1697] [F1698] [F1699] [F1700] [F1701] [F1702] [F1703] [F1704] [F1705] [F1706] [F1707] [F1708] [F1709] [F1710] [F1711] [F1712] [F1713] [F1714] [F1715] [F1716] [F1717] [F1718] [F1719] [F1720] [F1721] [F1722] [F1723] [F1724] [F1725] [F1726] [F1727] [F1728] [F1729] [F1730] [F1731] [F1732] [F1733] [F1734] [F1735] [F1736] [F1737] [F1738] [F1739] [F1740] [F1741] [F1742] [F1743] [F1744] [F1745] [F1746] [F1747] [F1748] [F1749] [F1750] [F1751] [F1752] [F1753] [F1754] [F1755] [F1756] [F1757] [F1758] [F1759] [F1760] [F1761] [F1762] [F1763] [F1764] [F1765] [F1766] [F1767] [F1768] [F1769] [F1770] [F1771] [F1772] [F1773] [F1774] [F1775] [F1776] [F1777] [F1778] [F1779] [F1780] [F1781] [F1782] [F1783] [F1784] [F1785] [F1786] [F1787] [F1788] [F1789] [F1790] [F1791] [F1792] [F1793] [F1794] [F1795] [F1796] [F1797] [F1798] [F1799] [F1800] [F1801] [F1802] [F1803] [F1804] [F1805] [F1806] [F1807] [F1808] [F1809] [F1810] [F1811] [F1812] [F1813] [F1814] [F1815] [F1816] [F1817] [F1818] [F1819] [F1820
```

Підготовка Linux-App-Server для розгортання Nextcloud

Після налаштування Database-Server було підготовлено Linux-App-Server, на якому розміщується прикладний сервіс Nextcloud. Цей сервер виконує роль вузла прикладного рівня: він запускає контейнер Nextcloud, взаємодіє з MariaDB на Database-Server та приймає користувацькі HTTPS-запити через вебсервер Nginx.

Перед встановленням прикладних компонентів на Linux-App-Server було оновлено індекси пакетів операційної системи. Після цього було встановлено платформу контейнеризації Docker та інструмент Docker Compose. Відповідні службові дії наведено в додатку Ж на рисунках Ж.1 та Ж.2.

Після встановлення Docker службу було активовано та додано до автозавантаження. Також було створено окрему робочу директорію ~/nextcloud, у якій надалі розміщувався файл конфігурації docker-compose.yml для запуску сервісу Nextcloud.



```
admin@Linux-App-Server: ~/nextcloud
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
admin@Linux-App-Server:~$ sudo systemctl enable --now docker
admin@Linux-App-Server:~$ mkdir ~/nextcloud && cd ~/nextcloud
admin@Linux-App-Server:~/nextcloud$
```

Рисунок 3.40 — Увімкнення Docker та створення робочої директорії Nextcloud на Linux-App-Server

Розгортання контейнера Nextcloud

Архітектуру сервісу Nextcloud було описано у файлі docker-compose.yml. У цьому файлі вказано офіційний образ Nextcloud, назву контейнера nextcloud_app, параметри автоматичного перезапуску, підключення до зовнішньої бази MariaDB на Database-Server та постійний том nextcloud_data для збереження даних сервісу.

Вебінтерфейс контейнера було прив'язано лише до локального інтерфейсу Linux-App-Server за адресою 127.0.0.1:8080. Це означає, що прямий доступ до контейнера з інших вузлів мережі не використовується, а зовнішні HTTPS-запити надалі обробляються через Nginx як зворотний проксі-сервер.

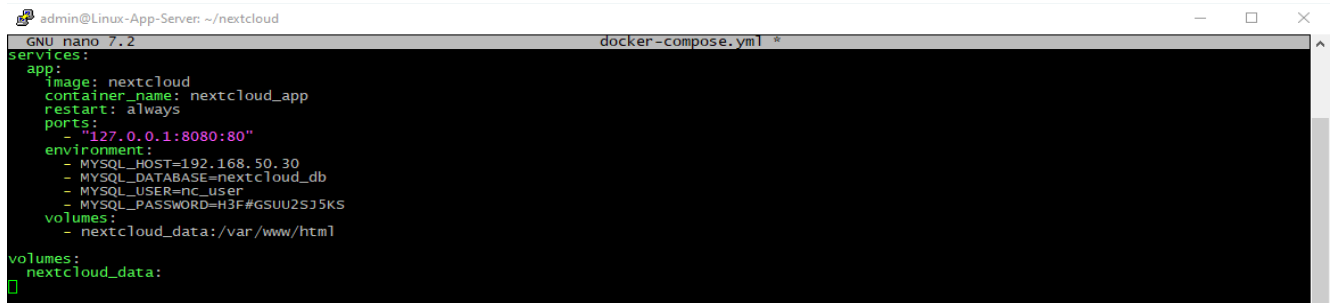


Рисунок 3.41 — Конфігурація docker-compose.yml для запуску контейнера Nextcloud

Після створення docker-compose.yml було виконано запуск контейнеризованого середовища Nextcloud за допомогою команди `docker compose up -d`. У результаті було створено ізольовану мережу Docker, постійний том `nextcloud_data` та запущено контейнер `nextcloud_app`.



Рисунок 3.42 — Ініціалізація та запуск контейнеризованого середовища Nextcloud

Налаштування Nginx та HTTPS-доступу до Nextcloud

Для організації доступу користувачів до Nextcloud було використано вебсервер Nginx, який виконує роль зворотного проксі-сервера. У такій моделі користувацькі запити надходять до Nginx через доменне ім'я `nextcloud.corp.local`, а далі передаються до контейнера Nextcloud, який працює локально на Linux-App-Server за адресою `127.0.0.1:8080`.

Перед налаштуванням зворотного проксі на Linux-App-Server було встановлено пакети `nginx` та `openssl`. Приклад встановлення цих компонентів наведено в додатку Ж на рисунку Ж.3.

Для забезпечення HTTPS-доступу до внутрішнього сервісу було створено самопідписаний SSL-сертифікат для доменного імені `nextcloud.corp.local`. Сертифікат використовується вебсервером Nginx для шифрування трафіку між клієнтськими робочими станціями та сервісом Nextcloud.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

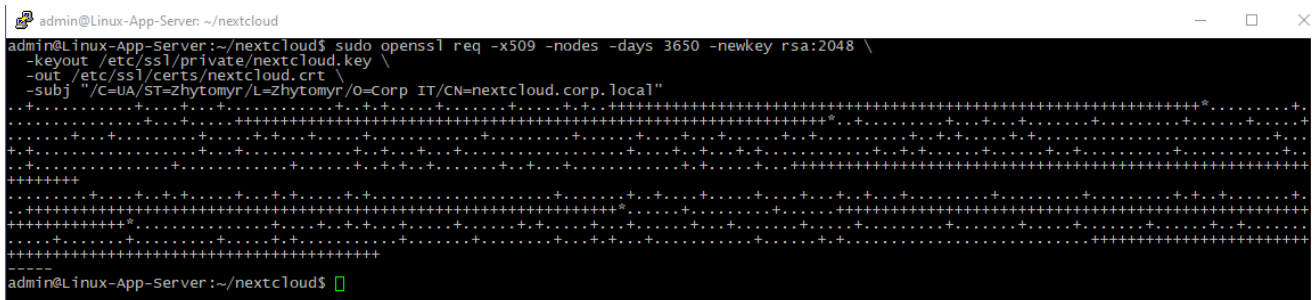


Рисунок 3.43 — Генерація самопідписаного SSL-сертифіката для домену nextcloud.corp.local

Після генерації сертифіката було створено конфігурацію віртуального хоста Nginx для домену nextcloud.corp.local. У ній налаштовано перенаправлення HTTP-запитів на HTTPS, підключення SSL-сертифіката та передавання запитів до локального контейнера Nextcloud. Також було додано службові заголовки проксі-сервера, необхідні для коректної роботи Nextcloud за Nginx.

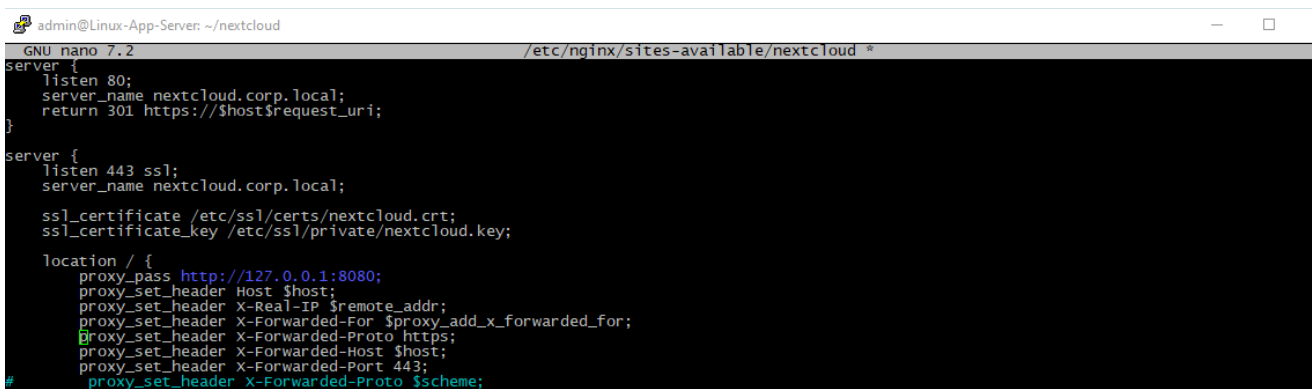


Рисунок 3.44 — Конфігурація віртуального хоста Nginx для проксування HTTPS-запитів до Nextcloud

Після створення конфігурації її було активовано через каталог sites-enabled, стандартну конфігурацію Nginx було відключено, а службу вебсервера перезапущено. Додатково через консольну утиліту oss, яка виконувалася всередині контейнера Nextcloud, було задано параметри роботи сервісу за зворотним проксі-сервером.

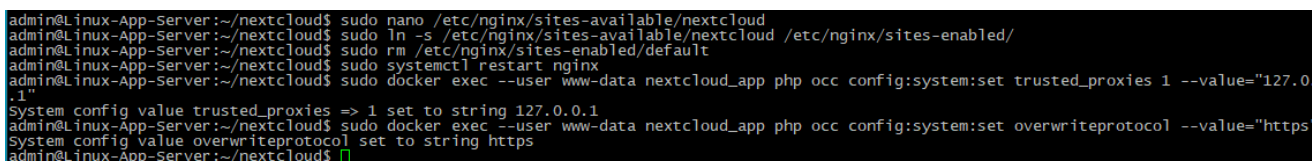


Рисунок 3.45 — Активація конфігурації Nginx та початкове налаштування параметрів Nextcloud через oss

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Для коректної роботи сервісу за внутрішнім DNS-іменем домен nextcloud.corp.local було додано до списку довірених доменів Nextcloud. Також було налаштовано параметри `overwritehost` та `overwrite.cli.url`, які забезпечують правильне формування посилань із використанням HTTPS і доменного імені nextcloud.corp.local. Відповідні службові команди наведено в додатку Ж на рисунках Ж.4 та Ж.5.

Перевірка роботи Nextcloud і налаштування рольової моделі доступу

Після завершення налаштування Nginx і параметрів Nextcloud було перевірено доступ до файлової підсистеми через доменне ім'я nextcloud.corp.local. Успішне відкриття вебінтерфейсу підтверджує працездатність контейнера Nextcloud, зворотного проксі-сервера Nginx, внутрішнього DNS-імені та HTTPS-доступу.

Після завершення налаштування Nginx і параметрів Nextcloud було перевірено доступ до файлової підсистеми через доменне ім'я nextcloud.corp.local. Вебінтерфейс відкрився коректно, що підтвердило працездатність контейнера Nextcloud, зворотного проксі-сервера Nginx, внутрішнього DNS-імені та HTTPS-доступу.

Для імітації організаційної структури підприємства у Nextcloud було створено групи користувачів відповідно до підрозділів: Accounting, HR_Dept, Management та IT_Dept. Для користувачів було задано дискові квоти, що дозволяє обмежити використання сховища окремими обліковими записами та запобігти неконтрольованому заповненню дискового простору.

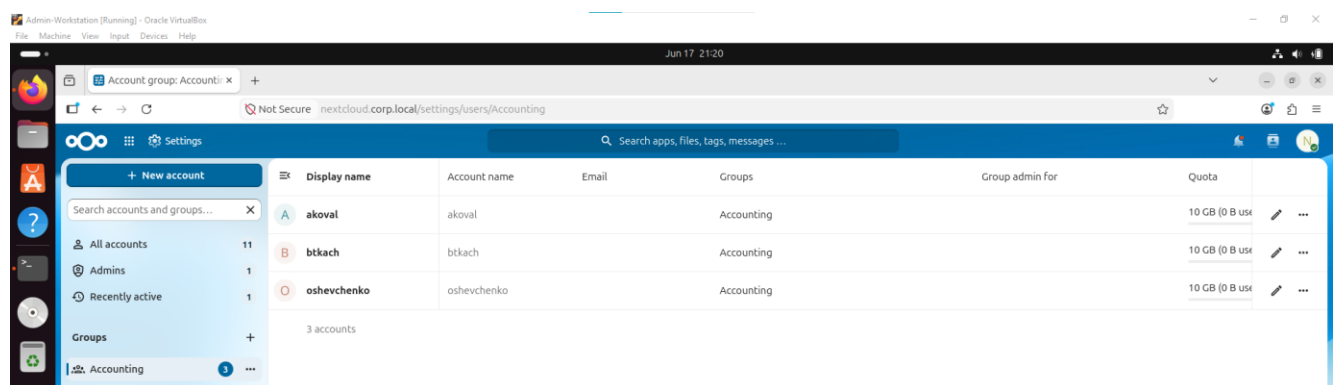


Рисунок 3.47 — Налаштування груп користувачів і дискових квот у Nextcloud

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Для перевірки механізму спільного доступу було створено директорию Financial_Reports. Внутрішній доступ до цієї директорії було надано групі Accounting з правами редагування. Також було налаштовано зовнішній доступ за посиланням із правами лише на перегляд, що дає змогу передавати файли стороннім користувачам без надання їм повного доступу до сховища.

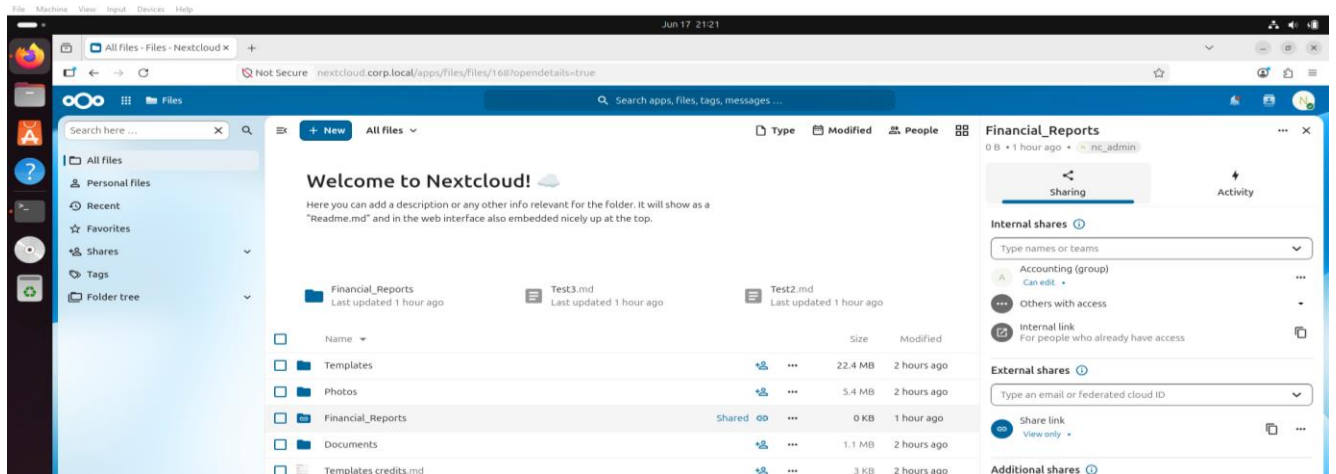


Рисунок 3.48 — Налаштування внутрішнього та зовнішнього спільного доступу до директорії Financial_Reports

Для підтвердження роботи налаштованого спільного доступу було виконано перевірку з клієнтського боку. Користувач отримав доступ до директорії Financial_Reports через вебінтерфейс Nextcloud, де відображалися тестові файли. Це підтвердило, що налаштована рольова модель доступу, спільна директорія та файловий обмін у Nextcloud працюють коректно.

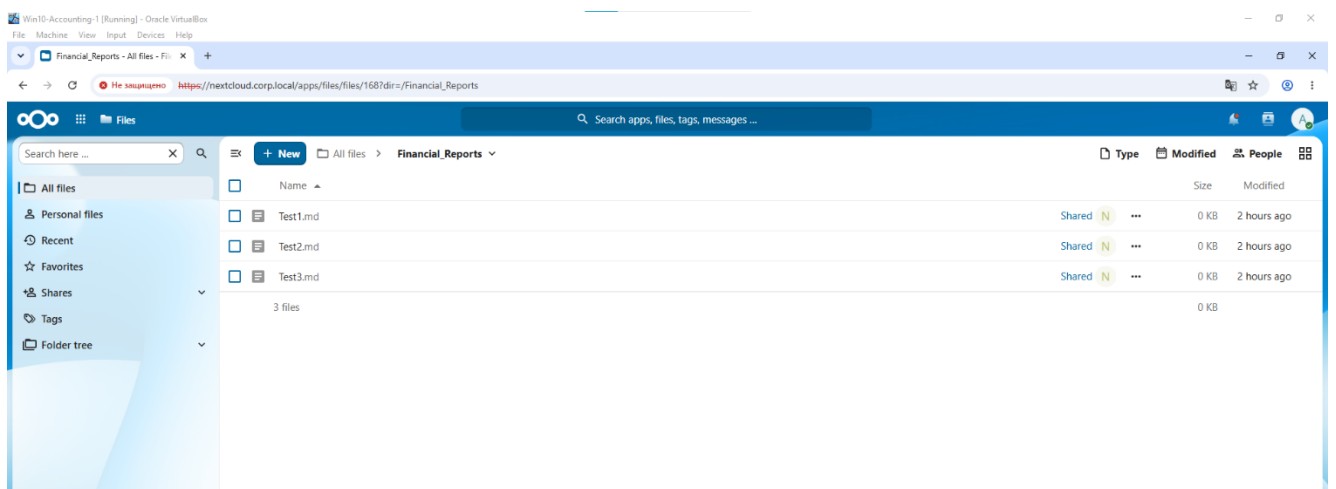


Рисунок 3.49 — Перевірка доступу користувача до спільної директорії Financial_Reports у Nextcloud

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

У результаті було розгорнуто корпоративне хмарне сховище Nextcloud на Linux-App-Server, підключено його до MariaDB на Database-Server, налаштовано HTTPS-доступ через Nginx, додано параметри роботи за зворотним проксі-сервером, створено базову рольову модель доступу користувачів і перевірено роботу файлового обміну.

Реалізація централізованого резервного копіювання

Після розгортання корпоративного сервісу Nextcloud було реалізовано централізоване резервне копіювання. Для цього використовується окремий Backup-Server, який ініціює збирання даних із Database-Server, Linux-App-Server та Icinga2-Master-Server через SSH.

На Backup-Server було встановлено базові утиліти tar та rsync, необхідні для архівації та передавання даних. Приклад встановлення цих утиліт наведено в додатку К на рисунку К.1.

Для автоматизованого доступу Backup-Server до цільових вузлів було згенеровано SSH-ключі та передано відкритий ключ на сервери інфраструктури. Це дозволяє виконувати резервне копіювання без ручного введення облікових даних під час кожного запуску скрипта.

```
admin@Backup-Server:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair:
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/admin/.ssh/id_rsa
Your public key has been saved in /home/admin/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:kDwhLlUUVfAYyQmSmun7zFwtvnaeSpghndCrtp1ou admin@Backup-Server
The key's randomart image is:
[+-----+
|          |
|    o.o.. |
|      .   |
|    + + o  |
|     . o.  |
|      ..o  |
|     . . . |
|    + . .  |
|     . . . |
|    + . .  |
|          |
|----=[SHA256]-----+]
admin@Backup-Server:~$ ssh-copy-id admin@192.168.50.30
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.50.30 (192.168.50.30)' can't be established.
D23519 key fingerprint is SHA256:fRhzazZmVdZw7r2ewqkytDe3zxspIizavc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- If you are prompted now it is to install the new keys
admin@192.168.50.30:~$ password:
Number of key(s) added: 1

How try logging into the machine, with: "ssh 'admin@192.168.50.30'"
and check to make sure that only the key(s) you wanted were added.

admin@Backup-Server:~$ ssh-copy-id admin@192.168.50.20
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.50.20 (192.168.50.20)' can't be established.
E02519 key fingerprint is SHA256:y4QZrVMA30G24Y54ZF9esSwraiglWz+gkvGVZVG.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- If you are prompted now it is to install the new keys
admin@192.168.50.20:~$ password:
Number of key(s) added: 1

How try logging into the machine, with: "ssh 'admin@192.168.50.20'"
and check to make sure that only the key(s) you wanted were added.

admin@Backup-Server:~$ ssh-copy-id admin@192.168.60.10
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.60.10 (192.168.60.10)' can't be established.
E02519 key fingerprint is SHA256:Cq4toezgrnm9GDmO27zhn7FFtkam4/domyucMRd4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- If you are prompted now it is to install the new keys
admin@192.168.60.10:~$ password:
Number of key(s) added: 1

How try logging into the machine, with: "ssh 'admin@192.168.60.10'"
and check to make sure that only the key(s) you wanted were added.

admin@Backup-Server:~$ ll
```

Рисунок 3.50 — Налаштування SSH-доступу Backup-Server до вузлів інфраструктури

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

Основним інструментом автоматизації резервного копіювання став bash-скрипт `sync_master.sh`. Він створює структуру каталогів для резервних копій, формує SQL-дампи баз даних, архівує конфігураційні файли та записує результати виконання до журналу. Фрагменти скрипта наведено в додатку 3 на рисунках 3.2 та 3.3.

Для резервного копіювання системних конфігурацій Icinga2-Master-Server було виконано точкове делегування прав на запуск архіватора `tar` через `sudoers`. Це дозволяє Backup-Server отримувати потрібні конфігураційні файли без надання повного адміністративного доступу до цільового вузла.

```
admin@Icinga2-Master-Server: ~
admin@Icinga2-Master-Server:~$ echo "admin ALL=(ALL) NOPASSWD: /usr/bin/tar" | s
udo tee /etc/sudoers.d/backup_tar
[sudo] password for admin:
admin ALL=(ALL) NOPASSWD: /usr/bin/tar
admin@Icinga2-Master-Server:~$
```

Рисунок 3.51 — Делегування прав на виконання архіватора `tar` для резервного копіювання конфігурацій Icinga 2

Для коректного створення дампа бази даних Nextcloud було додатково налаштовано локальні дозволи сервісного користувача `nc_user` на Database-Server. Відповідні команди наведено в додатку 3 на рисунках 3.4 та 3.5.

Після завершення підготовки було виконано ручний запуск скрипта `sync_master.sh`. Журнал виконання підтвердив успішне створення резервних копій бази даних Nextcloud, баз даних Icinga 2 та конфігураційних файлів.

```
admin@Backup-Server: ~
admin@Backup-Server:~$ ~/backups/sync_master.sh
[11:09:26] Завантаження дампа бази даних nextcloud (192.168.50.30)...
-> [УСПІХ] База даних скопійована.
[11:09:30] Архівування файлів додатку (192.168.50.20)...
-> [УСПІХ] Файли додатку скопійовані.
[11:09:31] Архівування конфігурації моніторингу rki (192.168.60.10)...
-> [УСПІХ] Конфігурація моніторингу (rki) скопійована.
[11:09:33] Завантаження БД Icinga Core (192.168.60.10)...
-> [УСПІХ] База даних core скопійована.
[11:09:34] Завантаження БД Icinga Web 2 (192.168.60.10)...
-> [УСПІХ] База даних web2 скопійована.
[11:09:35] Завантаження БД Icinga Director (192.168.60.10)...
-> [УСПІХ] База даних Director скопійована.
[2026-06-18 11:09:37] ФІНІШ: копіювання завершено успішно.

--- Структура збережених файлів (останні створення) ---
total 1.5M
-rw-rw-r-- 1 admin admin 1.5M Jun 18 11:09 db_nextcloud_2026-06-18_11-09.sql
total 4.0K
-rw-rw-r-- 1 admin admin 373 Jun 18 11:09 app_nextcloud_2026-06-18_11-09.tar.gz
total 2.8M
-rw-rw-r-- 1 admin admin 2.1M Jun 18 11:09 db_director_2026-06-18_11-09.sql
-rw-rw-r-- 1 admin admin 703K Jun 18 11:09 db_icinga_core_2026-06-18_11-09.sql
-rw-rw-r-- 1 admin admin 8.2K Jun 18 11:09 db_icinga_web2_2026-06-18_11-09.sql
-rw-rw-r-- 1 admin admin 9.2K Jun 18 11:09 icinga_master_conf_2026-06-18_11-09.t
ar.gz
admin@Backup-Server:~$
```

Рисунок 3.52 — Журнал успішного виконання централізованого резервного копіювання

Після тестового запуску було перевірено обсяг створених резервних копій. Результат показує окремі каталоги для прикладних файлів, баз даних, конфігурацій Icinga 2, журналів та самого скрипта резервного копіювання.

```
admin@Backup-Server: ~
admin@Backup-Server:~$ du -sh ~/backups/*
8.0K /home/admin/backups/app
1.5M /home/admin/backups/database
2.8M /home/admin/backups/icinga
8.0K /home/admin/backups/logs
8.0K /home/admin/backups/sync_master.sh
admin@Backup-Server:~$
```

Рисунок 3.53 — Перевірка обсягу каталогів резервного копіювання на Backup-Server

Для автоматизації регулярного виконання резервного копіювання було використано планувальник cron. У розклад було додано запуск скрипта sync_master.sh щоденно о 20:00. Налаштування завдання в редакторі crontab наведено в додатку 3 на рисунку 3.6.

Після збереження розкладу було перевірено список активних завдань cron. Наявність запису запуску sync_master.sh підтверджує, що резервне копіювання виконуватиметься автоматично за заданим розкладом.

```
admin@Backup-Server: ~
admin@Backup-Server:~$ crontab -e
no crontab for admin - using an empty one
crontab: installing new crontab
admin@Backup-Server:~$ crontab -l | tail -n 2
0 20 * * * /bin/bash /home/admin/backups/sync_master.sh
admin@Backup-Server:~$
```

Рисунок 3.54 — Перевірка автоматизованого запуску резервного копіювання через crontab

У результаті було реалізовано централізовану систему резервного копіювання, яка охоплює базу даних Nextcloud, конфігураційні файли прикладного сервісу, бази даних і конфігурації Icinga 2, а також забезпечує журналювання та автоматичний запуск за розкладом. Це завершує налаштування серверних сервісів і системи резервного копіювання в межах підрозділу 3.2.

3.3. Реалізація політик доступу, внутрішньої сегментації та захисту мережевого периметра

Метою підрозділу є обмеження прав користувачів і зменшення ризиків несанкціонованого доступу до критичних компонентів інфраструктури. На цьому етапі реалізуються групові політики Active Directory, ACL на Cisco Core L3 Switch, перевірка міжсегментного доступу та Suricata IDS/IPS на pfSense. Ці налаштування

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

потрібні для того, щоб інфраструктура відповідала принципам мінімальних привілеїв, розмежування ролей і контрольованого доступу між сегментами. [1; 2; 3; 14; 16; 17; 23]

Реалізація Corporate Security Policy виконується для базового захисту користувачьких Windows-станцій. Політика обмежує локальні привілеї, ускладнює несанкціоновану зміну системних параметрів, задає вимоги до паролів, блокує неактивні сесії та вмикає аудит подій входу. Це зменшує ризики, пов'язані з помилками користувачів або навмисними змінами на робочих станціях. [23]

Реалізація внутрішньої сегментації через Extended ACL виконується для контролю доступу між VLAN. Користувачьким сегментам дозволяється доступ лише до необхідних служб, таких як DNS, DHCP, доменна автентифікація, синхронізація часу та Nextcloud. Прямий доступ до Database-Server, Backup-Server, Icinga2-Master-Server, Cisco management і WebGUI pfSense обмежується. Це зменшує можливість горизонтального переміщення в мережі у разі компрометації одного з користувачьких вузлів. [17; 18]

Перевірка ACL виконується для підтвердження того, що правила доступу працюють не лише формально, а й фактично. Звичайні користувачькі сегменти повинні мати доступ до потрібних сервісів, але не повинні відкривати адміністративні інтерфейси або напряду підключатися до критичних серверів. Адміністративний сегмент, навпаки, повинен мати розширені права для керування інфраструктурою. [17]

Реалізація Suricata IDS/IPS на pfSense виконується для посилення захисту WAN-периметра. Suricata дозволяє аналізувати мережевий трафік, використовувати сигнатури виявлення атак і блокувати підозрілу активність. Перевірка Suricata за допомогою тестового сканування потрібна для підтвердження того, що засіб захисту не лише встановлений, а й фактично реагує на потенційно небажану активність. [14; 15; 16]

Реалізація доменних політик безпеки для Windows-клієнтів

Для доменних Windows-робочих станцій було реалізовано групову політику Corporate Security Policy. Вона застосовується до клієнтських комп'ютерів і

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

користувачів, які входять до домену corp.local, та призначена для централізованого налаштування базових параметрів безпеки.

На контролері домену Windows Server 2022 було сформовано організаційну структуру Active Directory відповідно до підрозділів організації. У домені створено окремі організаційні підрозділи Accounting, HR_Dept, Management та IT_Dept. У цих підрозділах розміщено відповідні облікові записи користувачів і робочі станції, що дозволяє адресно застосовувати політики безпеки. [20; 23]

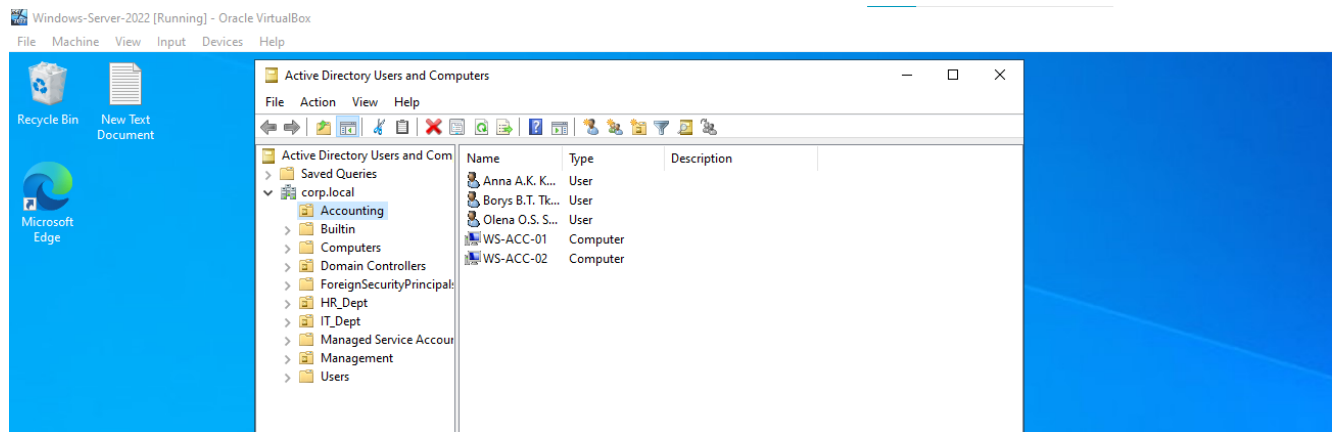


Рисунок 3.55 — Організаційна структура домену corp.local для розміщення користувачів і робочих станцій

Після створення організаційної структури було виконано прив'язку групової політики Corporate Security Policy до користувацьких організаційних підрозділів. Політика застосовується до Accounting, HR_Dept та Management, тобто до підрозділів, у яких розміщені звичайні доменні Windows-клієнти. Адміністративний сегмент IT_Dept не використовується як об'єкт застосування цієї політики для WS-IT-01, оскільки адміністративна станція працює на Ubuntu Desktop і захищається окремими мережевими механізмами. [23]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

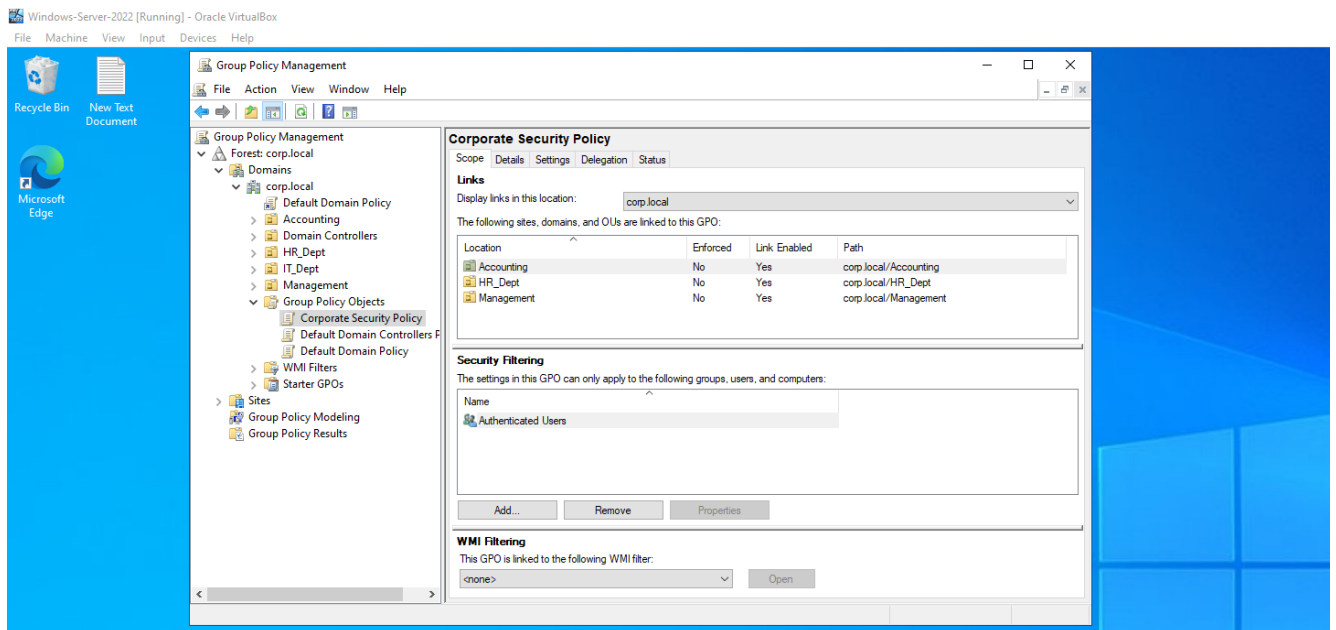


Рисунок 3.56 — Прив’язка групової політики Corporate Security Policy до Windows-клієнтів домену

У межах Corporate Security Policy було налаштовано базові параметри локальної безпеки Windows-станцій. Зокрема, політика вимикає гостьовий обліковий запис, обмежує підвищення привілеїв для стандартних користувачів через UAC, задає автоматичне блокування неактивної сесії та вмикає аудит подій входу, керування обліковими записами й зміни політик. Детальні параметри Corporate Security Policy наведено в додатку Л на рисунках Л.1 та Л.2. [23]

Базові вимоги до паролів доменних облікових записів задаються на рівні стандартної доменної політики Active Directory. У цьому підрозділі Corporate Security Policy використовується саме для керування параметрами безпеки клієнтських Windows-станцій, тоді як доменна парольна політика діє як загальне правило для облікових записів у домені corp.local.

Після застосування політики було виконано перевірку її отримання на робочій станції WS-ACC-01. Для цього використовувалася команда `gpresult /r`, яка показує список групових політик, застосованих до користувача та комп’ютера. Наявність Corporate Security Policy у результатах перевірки підтверджує, що клієнтська Windows-станція отримала потрібну політику з доменного контролера. Результат перевірки наведено в додатку Л на рисунку Л.3.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

Таким чином, у межах доменної частини було реалізовано централізовану політику безпеки для Windows-клієнтів користувацьких підрозділів. Вона забезпечує уніфіковані параметри локальної безпеки робочих станцій, тоді як адміністративна станція WS-IT-01 контролюється через VLAN 40, правила доступу, SSH-ключі та дозволені адміністративні канали керування.

Реалізація політик доступу, внутрішньої сегментації та захисту мережевого периметра

Реалізація внутрішньої сегментації мережі за допомогою Extended ACL

Після налаштування доменних політик безпеки було реалізовано внутрішню сегментацію мережі на рівні Cisco Core L3 Switch. Для цього використано розширені списки контролю доступу Extended ACL, які дозволяють керувати трафіком між VLAN відповідно до ролі користувацького сегмента.

Метою впровадження ACL є реалізація принципу мінімальних привілеїв. Звичайні користувачі повинні мати доступ лише до необхідних служб: DNS, DHCP, доменної автентифікації, синхронізації часу та корпоративного сервісу Nextcloud. Водночас прямий доступ до серверів баз даних, резервного копіювання, системи моніторингу, інтерфейсів керування Cisco та pfSense має бути заблокований.

На комутаторі ядра було створено два основні розширені списки доступу: ACL_MANAGEMENT та ACL_STANDARD_USERS. ACL_MANAGEMENT використовується для сегмента керівництва, а ACL_STANDARD_USERS — для стандартних користувацьких сегментів, зокрема Accounting та HR. У списках доступу спочатку розміщено правила дозволу до необхідних інфраструктурних служб, а після них — заборонні правила для обмеження доступу до критичних сегментів мережі. [17]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

```

Core-L3-Switch - PuTTY
Core-L3-Switch#show ip access-lists
Standard IP access list ACL_ICINGA
10 permit 192.168.60.10 (760 matches)
Extended IP access list ACL_MANAGEMENT
10 permit udp any any eq bootps
20 permit udp any any eq bootpc
30 permit tcp any host 192.168.50.10 eq domain
40 permit udp any host 192.168.50.10 eq domain
50 permit tcp any host 192.168.50.10 eq 88
60 permit udp any host 192.168.50.10 eq 88
70 permit udp any host 192.168.50.10 eq ntp
80 permit tcp any host 192.168.50.10 eq 135
90 permit tcp any host 192.168.50.10 eq 445
100 permit tcp any host 192.168.50.10 eq 389
110 permit tcp any host 192.168.50.10 eq 389
120 permit tcp any host 192.168.50.10 eq 636
130 permit tcp any host 192.168.50.10 eq 3268
140 permit tcp any host 192.168.50.20 eq www
150 permit tcp any host 192.168.50.20 eq 443
160 permit tcp any 192.168.40.0 0.0.0.255 established
170 permit icmp any 192.168.40.0 0.0.0.255 echo-reply
180 deny ip any 192.168.40.0 0.0.0.255
190 deny ip any 192.168.20.0 0.0.0.255
200 deny ip any 192.168.30.0 0.0.0.255
210 deny ip any 192.168.100.0 0.0.0.255
220 deny ip any 192.168.1.0 0.0.0.255
230 deny ip any 192.168.50.0 0.0.0.255
240 deny ip any 192.168.60.0 0.0.0.255
250 permit ip any any
Extended IP access list ACL_STANDARD_USERS
10 permit udp any any eq bootps
20 permit udp any any eq bootpc
30 permit tcp any host 192.168.50.10 eq domain
40 permit udp any host 192.168.50.10 eq domain
50 permit tcp any host 192.168.50.10 eq 88
60 permit udp any host 192.168.50.10 eq 88
70 permit udp any host 192.168.50.10 eq ntp
80 permit tcp any host 192.168.50.10 eq 135
90 permit tcp any host 192.168.50.10 eq 445
100 permit tcp any host 192.168.50.10 eq 389
110 permit udp any host 192.168.50.10 eq 389
120 permit tcp any host 192.168.50.10 eq 636
130 permit tcp any host 192.168.50.10 eq 3268
140 permit tcp any host 192.168.50.20 eq www
150 permit tcp any host 192.168.50.20 eq 443
160 permit tcp any 192.168.40.0 0.0.0.255 established
170 permit icmp any 192.168.40.0 0.0.0.255 echo-reply
180 deny ip any 192.168.10.0 0.0.0.255
190 deny ip any 192.168.40.0 0.0.0.255
200 deny ip any 192.168.100.0 0.0.0.255
210 deny ip any 192.168.1.0 0.0.0.255
220 deny ip any 192.168.50.0 0.0.0.255
230 deny ip any 192.168.60.0 0.0.0.255
240 permit ip any any
Extended IP access list preauth_ipv4_acl (per-user)
10 permit udp any any eq domain
20 permit tcp any any eq domain
30 permit udp any any eq bootps any
40 permit udp any any eq bootpc
50 permit udp any any eq bootpc any
60 deny ip any any

```

Рисунок 3.57 — Перегляд розширених списків контролю доступу на Cisco Core L3 Switch

У списках ACL дозволено звернення до Windows Server 2022 за адресою 192.168.50.10 для роботи DNS, Kerberos, LDAP, SMB та NTP. Також дозволено доступ до Linux-App-Server за адресою 192.168.50.20 через порти HTTP та HTTPS, оскільки саме на цьому сервері працює корпоративний сервіс Nextcloud. Після дозволених правил розміщено заборони доступу до адміністративного сегмента, серверної мережі, сегмента моніторингу, транзитної мережі pfSense та мережі керування.

Окремо в ACL передбачено можливість зворотного трафіку до адміністративного сегмента VLAN 40. Це потрібно для того, щоб адміністративна станція WS-IT-01 могла виконувати діагностику, перевірку доступності та керування вузлами інфраструктури, а відповіді від контрольованих пристроїв могли повертатися назад до адміністратора.

Після створення списків доступу їх було прив'язано до SVI-інтерфейсів Cisco Core L3 Switch. ACL_MANAGEMENT застосовано до інтерфейсу VLAN 10, а ACL_STANDARD_USERS — до інтерфейсу VLAN 20. На користувацьких VLAN

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

також залишено параметр `ip helper-address 192.168.50.10`, який забезпечує передавання DHCP-запитів до Windows Server 2022. [17; 18]

```
Core-L3-Switch#show run | section interface Vlan
interface Vlan1
  no ip address
  shutdown
interface Vlan10
  ip address 192.168.10.254 255.255.255.0
  ip access-group ACL_MANAGEMENT in
  ip helper-address 192.168.50.10
interface Vlan20
  ip address 192.168.20.254 255.255.255.0
  ip access-group ACL_STANDARD_USERS in
  ip helper-address 192.168.50.10
interface Vlan30
  ip address 192.168.30.254 255.255.255.0
  ip access-group ACL_STANDARD_USERS in
  ip helper-address 192.168.50.10
interface Vlan40
  ip address 192.168.40.254 255.255.255.0
interface Vlan50
  ip address 192.168.50.254 255.255.255.0
interface Vlan60
  ip address 192.168.60.254 255.255.255.0
interface Vlan99
  ip address 192.168.1.2 255.255.255.0
interface Vlan100
  ip address 192.168.100.254 255.255.255.0
Core-L3-Switch#
```

Рисунок 3.58 — Застосування ACL до SVI-інтерфейсів Cisco Core L3 Switch

Інтерфейс VLAN 40, у якому розміщена адміністративна станція WS-IT-01, не було обмежено вхідним ACL. Це зроблено свідомо, оскільки адміністративний сегмент призначений для керування серверами, мережевим обладнанням, p fSense та системою моніторингу. Отже, доступ адміністратора контролюється не Windows GPO, а мережевою архітектурою, VLAN-сегментацією та дозволеними адміністративними каналами.

Перевірка роботи внутрішньої сегментації мережі

Після застосування ACL було виконано практичну перевірку доступу з користувацьких і адміністративного сегментів. Метою перевірки було підтвердити, що звичайні користувачі мають доступ до дозволених сервісів, але не можуть напряду звертатися до критичних серверів та інтерфейсів керування.

Спочатку було перевірено доступ до корпоративного сервісу Nextcloud із робочої станції бухгалтерії Win10-Accounting-1, яка розміщена у VLAN 20. Вебінтерфейс Nextcloud успішно відкрився через доменне ім'я nextcloud.corp.local. Це підтверджує, що правила ACL_STANDARD_USERS дозволяють користувачам бухгалтерії доступ до прикладного сервісу на Linux-App-Server через HTTPS.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

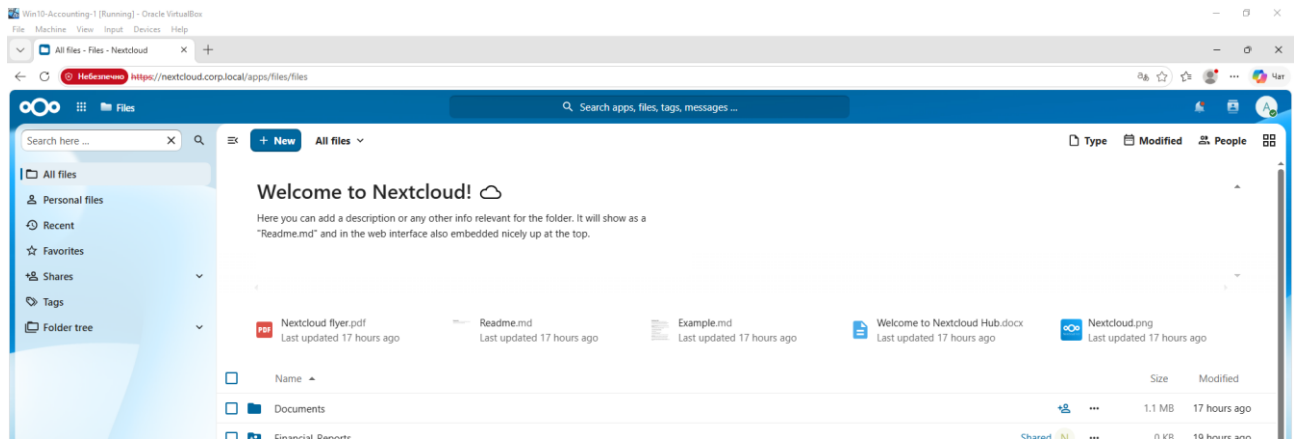


Рисунок 3.59 — Перевірка доступу користувача Accounting до Nextcloud після застосування ACL

Додатково з цієї ж робочої станції було перевірено роботу DNS і блокування прямого IP-доступу до заборонених сегментів. Команда `nslookup nextcloud.corp.local` успішно повернула адресу Linux-App-Server, що підтвердило доступність DNS-служби. Водночас ICMP-запити до Linux-App-Server, Database-Server, pfSense та мережі керування були заблоковані. Результат цієї перевірки наведено в додатку М на рисунку М.1.

Також було перевірено доступ до Nextcloud з робочої станції керівництва у VLAN 10. Вебінтерфейс сервісу відкрився коректно, що підтверджує доступність корпоративного хмарного сховища для дозволених користувацьких сегментів. Додаткову перевірку доступу з Management-сегмента наведено в додатку М на рисунку М.2.

Для перевірки ізоляції між користувацькими підмережами з робочої станції керівництва Win10-Management, яка розміщена у VLAN 10, було виконано спробу звернення до вузла бухгалтерського сегмента. Запит завершився повідомленням `Destination net unreachable`, що підтверджує блокування горизонтального переміщення між користувацькими VLAN. [3; 17]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

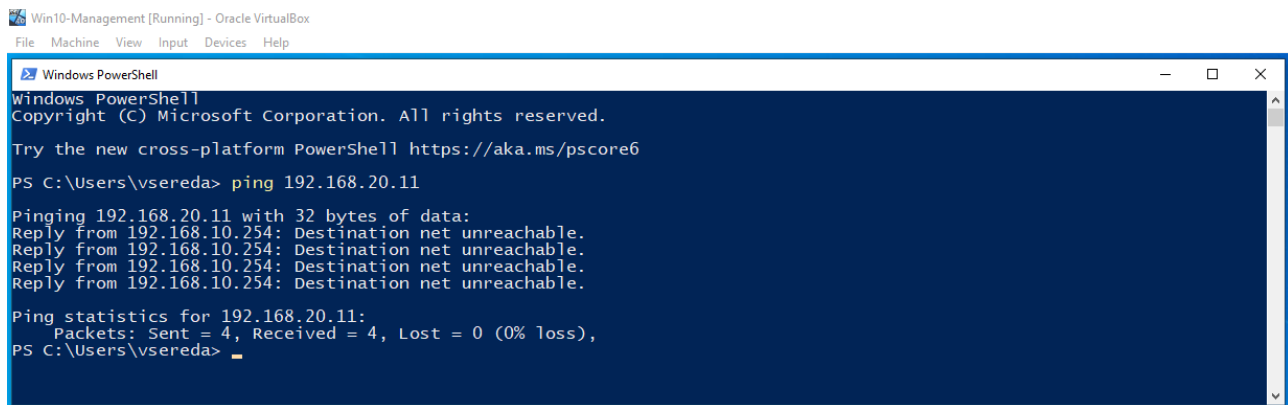


Рисунок 3.60 — Перевірка ізоляції між Management та Accounting VLAN

Окремо було перевірено роботу адміністративного сегмента. З адміністративної станції WS-IT-01 у VLAN 40 було виконано ICMP-запити до робочої станції бухгалтерії, Database-Server та Icinga2-Master-Server. Усі перевірки завершилися успішно, що підтверджує наявність адміністративного доступу до основних сегментів інфраструктури.

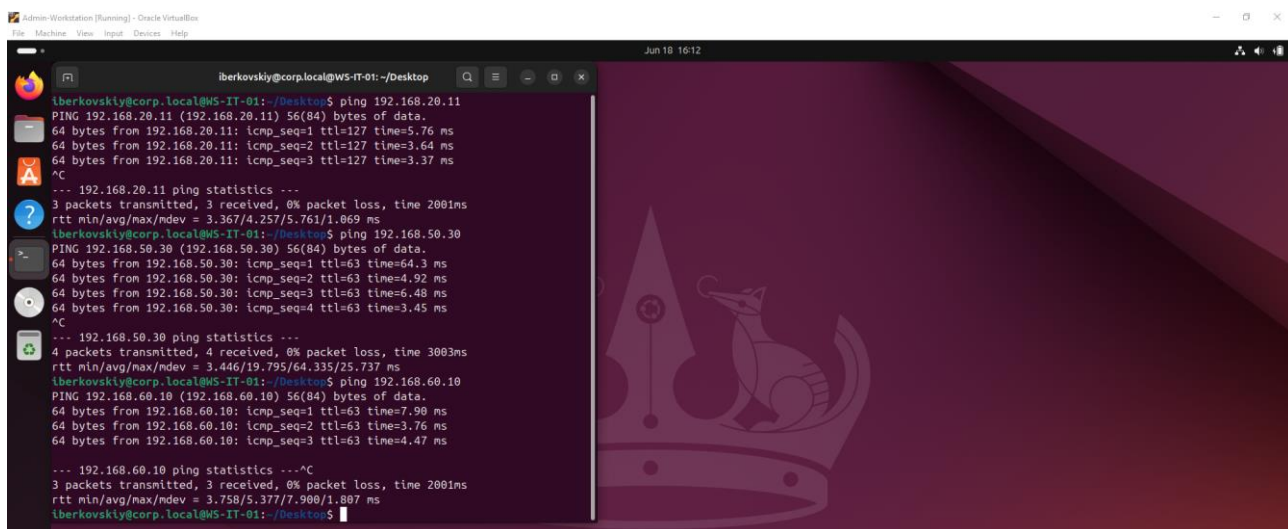


Рисунок 3.61 — Перевірка адміністративного доступу з WS-IT-01 до різних сегментів мережі

Результати перевірки показали, що реалізовані списки контролю доступу працюють відповідно до спроектованої моделі. Користувачки VLAN мають доступ до необхідних служб і корпоративного сервісу Nextcloud, але не мають прямого доступу до серверів, pfSense, мережі керування та системи моніторингу. Адміністративний сегмент VLAN 40 зберігає розширений доступ, необхідний для керування інфраструктурою та діагностики. [17; 18]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

Реалізація захисту мережевого периметра за допомогою Suricata IDS/IPS

Після реалізації внутрішньої сегментації мережі було налаштовано додатковий рівень захисту зовнішнього периметра. Для цього на граничному маршрутизаторі pfSense було встановлено та налаштовано систему Suricata IDS/IPS. Вона використовується для аналізу мережевого трафіку на зовнішньому інтерфейсі, виявлення підозрілої активності та блокування джерел потенційних атак. [14; 15; 16]

Suricata доповнює вже налаштовані правила firewall, NAT і внутрішні ACL. Якщо ACL на Cisco Core L3 Switch обмежують взаємодію між внутрішніми VLAN, то Suricata контролює трафік на WAN-периметрі та дозволяє виявляти спроби мережевої розвідки або атак ззовні. [14; 16; 17]

Встановлення Suricata було виконано через менеджер пакетів pfSense. У процесі інсталяції було завантажено пакет pfSense-pkg-suricata та необхідні залежності для роботи системи аналізу мережевого трафіку.

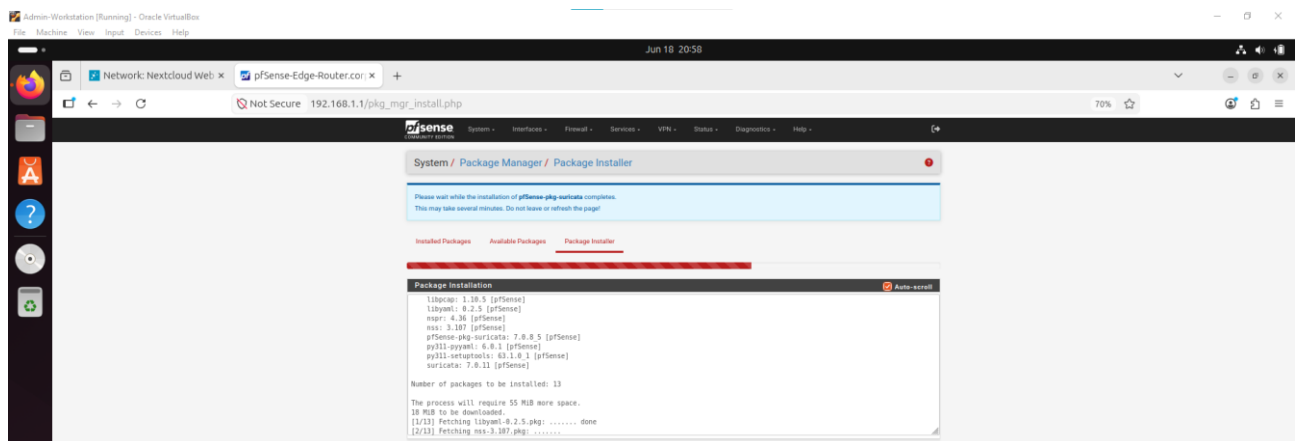


Рисунок 3.62 — Встановлення пакета Suricata на маршрутизаторі pfSense

Після встановлення було виконано глобальне налаштування Suricata. На цьому етапі було визначено джерело правил виявлення атак, параметри оновлення сигнатур і журналювання подій. Для роботи системи було використано відкритий набір правил Emerging Threats Open, а також увімкнено передавання повідомлень Suricata до системного журналу pfSense.

Після встановлення було виконано базове налаштування Suricata: визначено джерело правил виявлення атак, параметри оновлення сигнатур, журналювання подій і прив'язку системи до зовнішнього інтерфейсу WAN. Детальні параметри

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

глобальної конфігурації Suricata наведено в додатку Н на рисунку Н.1, а налаштування WAN-інтерфейсу — у додатку Н на рисунку Н.2.

Для актуалізації бази сигнатур було виконано оновлення правил Suricata. Це необхідно для того, щоб система могла використовувати актуальні шаблони виявлення мережових атак, сканування портів та іншої підозрілої активності. [16]

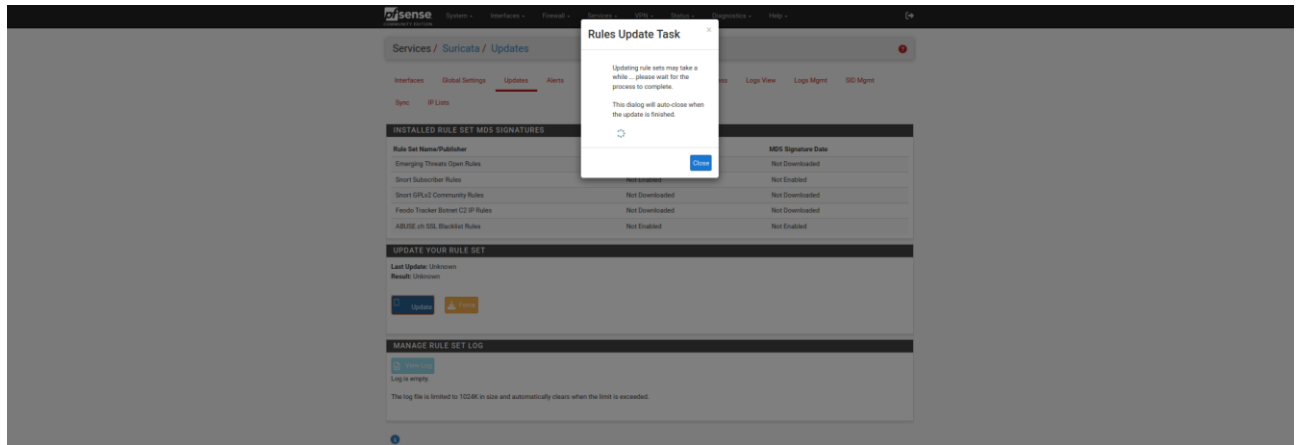


Рисунок 3.63 — Оновлення правил Suricata на pfSense

Після базового налаштування Suricata було переведено в активний режим запобігання вторгненням. Для цього було увімкнено параметр Block Offenders, який дозволяє системі не лише фіксувати спрацювання правил, а й блокувати джерело підозрілого трафіку. Також було активовано режим Legacy Mode і параметр Kill States, що дає змогу примусово скидати активні з'єднання заблокованого джерела. [15; 16]

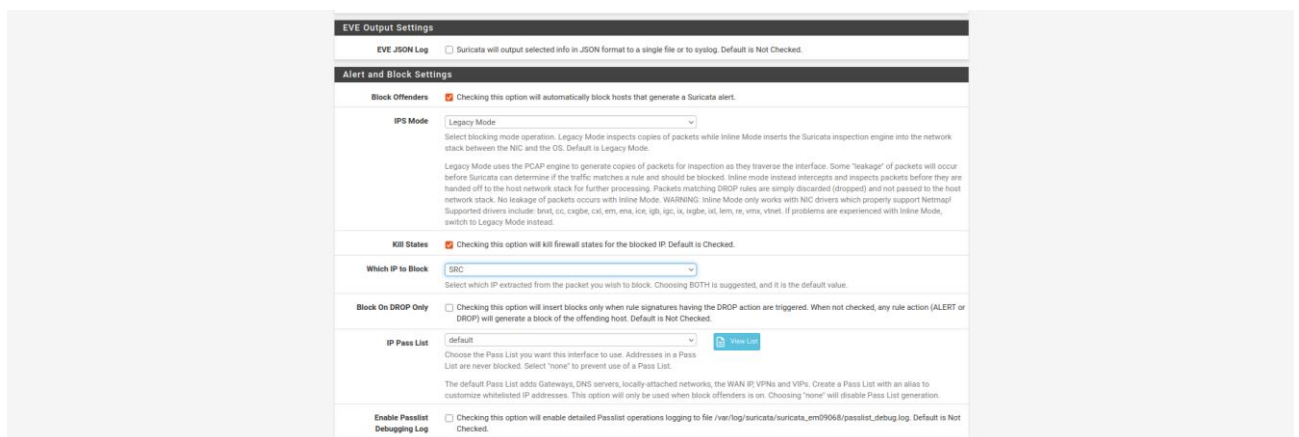


Рисунок 3.64 — Увімкнення режиму IPS та блокування джерел атак у Suricata

Після застосування налаштувань було перевірено стан інтерфейсу Suricata. У списку інтерфейсів pfSense для WAN відображається активний статус системи та режим блокування LEGACY MODE. Це підтверджує, що Suricata була успішно

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

запущена на зовнішньому інтерфейсі та отримала можливість блокувати підозрілий трафік.

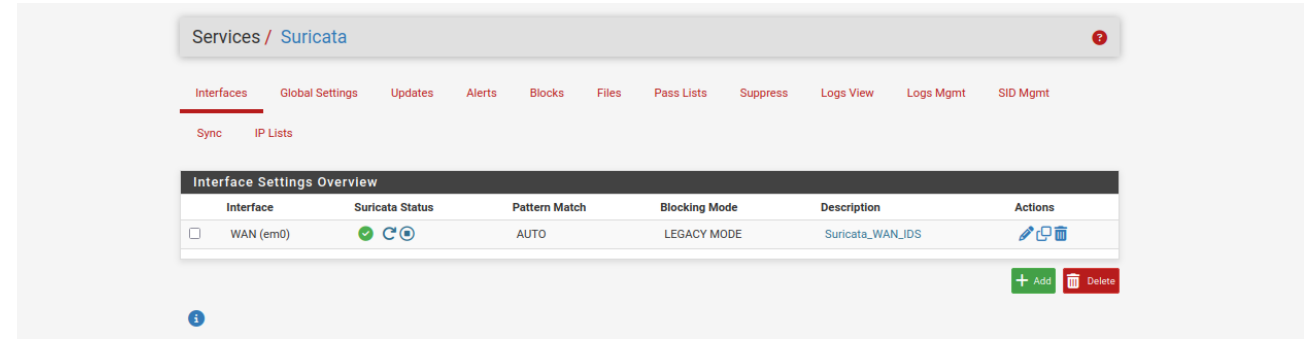


Рисунок 3.65 — Активний статус Suricata на WAN-інтерфейсі в режимі LEGACY MODE

Для практичної перевірки роботи Suricata було використано Kali Linux, розміщений поза корпоративною мережею. З нього було виконано SYN-сканування зовнішньої адреси pfSense за допомогою утиліти nmap. Така перевірка імітує типову спробу мережевої розвідки з боку зовнішнього вузла.

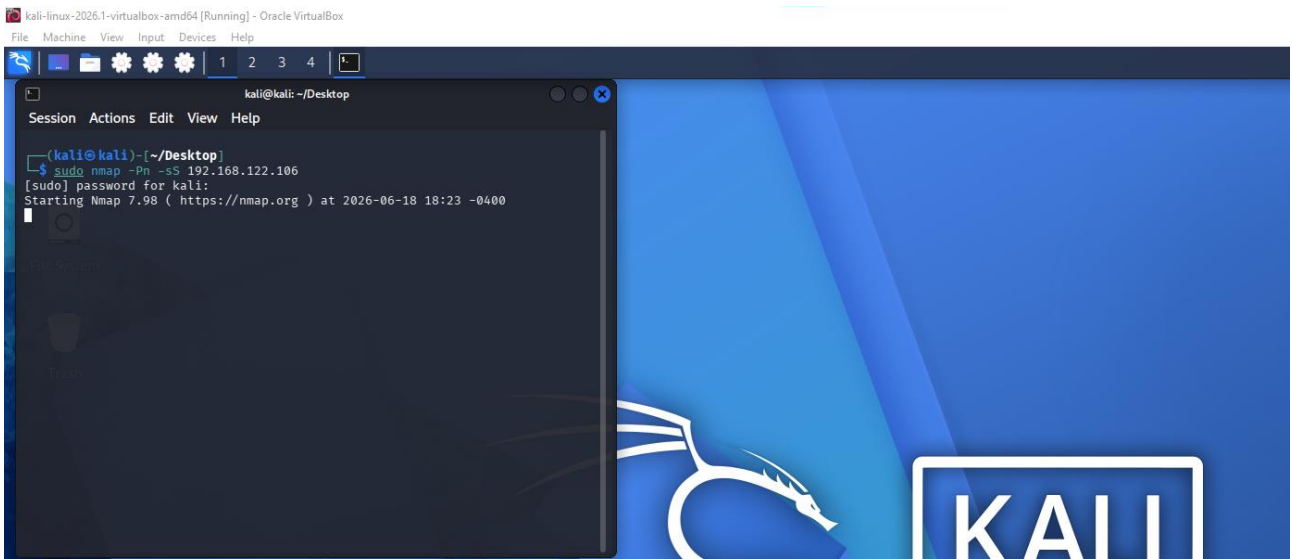


Рисунок 3.66 — Перевірка реакції Suricata на SYN-сканування з Kali Linux

У результаті тестування було підтверджено, що Suricata реагує на підозрілу активність на WAN-периметрі та блокує джерело сканування. Це дозволяє зменшити ризик несанкціонованої мережевої розвідки, доповнити фільтрацію pfSense та підвищити загальний рівень захисту зовнішнього периметра інфраструктури.

Таким чином, у межах захисту мережевого периметра було встановлено Suricata на pfSense, виконано базове налаштування правил, прив’язано систему до

WAN-інтерфейсу, увімкнено режим IPS і перевірено реакцію на сканування з зовнішнього вузла. У поєднанні з firewall-правилами pfSense та внутрішніми ACL це формує багаторівневу модель захисту мережі. [14; 15; 16; 17]

3.4. Реалізація системи моніторингу на базі Icinga 2

Метою підрозділу є розгортання централізованої системи моніторингу, яка контролює стан усіх ключових компонентів інфраструктури. На цьому етапі налаштовуються Icinga 2, Icinga Web 2, Icinga Director, агентний моніторинг Windows і Linux-серверів, SNMP-моніторинг Cisco та pfSense, а також прикладні перевірки Nextcloud, Docker, MariaDB, backup-журналу і Suricata. Це потрібно для того, щоб адміністратор мав єдину точку контролю стану мережевого, серверного, прикладного й безпекового рівнів. [5; 6; 7; 8; 9; 10; 19]

Розгортання Icinga2-Master-Server виконується для створення центрального вузла, який збирає, обробляє та відображає інформацію про стан хостів і сервісів. Icinga 2 виконує перевірки, MariaDB/IDO зберігає дані моніторингу, Icinga Web 2 надає вебінтерфейс, а Icinga Director використовується для централізованого керування конфігурацією. [5; 8; 9]

Підготовка контрольованих вузлів виконується для підключення серверів і мережевого обладнання до системи моніторингу. Windows Server 2022 і Linux-сервери контролюються через Icinga Agent, оскільки для них потрібні локальні перевірки служб і ресурсів. Cisco-комутатори та pfSense контролюються через SNMP, оскільки на них не встановлюється агент. [5; 6; 7; 19]

Створення хостів, шаблонів, Service Sets, Apply Rules, Data Fields і CheckCommands в Icinga Director виконується для впорядкування конфігурації моніторингу. Host Templates групують однотипні вузли, Service Sets призначають серверні перевірки, Apply Rules автоматизують перевірки мережевого обладнання, Data Fields передають змінні параметри, а CheckCommands визначають конкретні плагіни й скрипти перевірок. [6; 9; 10]

Моніторинг Windows Server 2022 виконується для контролю критичних доменних і мережевих служб. Система перевіряє стан AD DS, DNS, DHCP,

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		80

W32Time, RDP, ресурсів сервера, дисків і мережевого інтерфейсу. Це дозволяє швидко виявляти проблеми, які можуть вплинути на вхід користувачів у домен, видачу IP-адрес, резолвінг імен або адміністрування сервера. [5; 6; 20; 21; 22]

Моніторинг Linux-серверів виконується для контролю системних ресурсів і спеціалізованих сервісів. Linux-App-Server перевіряється не лише як хост, а й за доступністю Nextcloud через HTTPS і станом Docker-контейнера. Database-Server контролюється через перевірку MariaDB, а Backup-Server — через актуальність журналу резервного копіювання. Це дозволяє виявляти не тільки падіння сервера, а й збої конкретних служб. [5; 6; 24; 25; 26; 27]

Моніторинг Cisco-комутаторів через SNMPv3 виконується для контролю мережевої зв'язності. Для Core-L3-Switch перевіряються CPU, RAM, uptime, VLAN-інтерфейси та trunk-з'єднання. Для комутаторів доступу перевіряються базові параметри й uplink-порт. Це дозволяє визначати не лише загальний стан комутатора, а й стан ключових мережевих каналів. [18; 19]

Моніторинг pfSense та Suricata виконується для контролю граничного маршрутизатора й засобу захисту периметра. Icinga перевіряє WAN/LAN, uptime, CPU, RAM і процес Suricata. Окрема перевірка Suricata потрібна, оскільки маршрутизатор може бути доступним, але система захисту периметра може бути вимкнена або не працювати. [14; 15; 16]

Підсумкова перевірка Tactical Overview виконується для оцінки загального стану системи моніторингу. Вона дозволяє швидко побачити кількість недоступних хостів, критичних сервісів і проблемних компонентів. Нульова кількість критичних станів після налаштування підтверджує, що всі основні вузли та сервіси перебувають під контролем.

Розгортання центрального вузла моніторингу Icinga2-Master-Server

Центральним вузлом системи моніторингу було визначено Icinga2-Master-Server. Він розміщується в окремому сегменті Monitoring і виконує роль основної точки збору, обробки та відображення інформації про стан компонентів інфраструктури.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

[illegible]

Для зберігання даних моніторингу було використано СУБД MariaDB. Після встановлення MariaDB та Icinga 2 відповідні служби було додано до автозавантаження та запущено. Перевірка статусу служб показала, що MariaDB і Icinga 2 перебувають у стані active (running), що підтверджує готовність центрального вузла до подальшого налаштування. [27]

```

root@kali:~/# admin@icinga2-Master-Server:~$ sudo systemctl status mariadb
● mariadb.service - MariaDB 10.11.14 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: enabled)
   Active: active (running) since Mon 2026-06-08 23:35:49 UTC; 14min ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 11733 (mariadb)
   Status: "Taking your SQL requests now..."
     Tasks: 11 (limit: 1068)
    Memory: 78.7M (peak: 81.9M)
       CPU: 933ms
   CGroup: /system.slice/mariadb.service
           └─11733 /usr/sbin/mariadb

Jun 08 23:35:48 Icinga2-Master-Server mariadb[11733]: 2026-06-08 23:35:48 0 [Note] Plugin 'FEEDBACK' is disabled.
Jun 08 23:35:48 Icinga2-Master-Server mariadb[11733]: 2026-06-08 23:35:48 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/ib_buffer_pool
Jun 08 23:35:48 Icinga2-Master-Server mariadb[11733]: 2026-06-08 23:35:48 0 [warning] You need to use --log-bin to make --expire-logs-days or --binlog-expire-logs-seconds work.
Jun 08 23:35:48 Icinga2-Master-Server mariadb[11733]: 2026-06-08 23:35:48 0 [Note] Server socket created on IP: '127.0.0.1' port: '3306'
Jun 08 23:35:48 Icinga2-Master-Server mariadb[11733]: 2026-06-08 23:35:48 0 [Note] InnoDB: Buffer pool(s) load completed at 260608 23:35:48
Jun 08 23:35:48 Icinga2-Master-Server mariadb[11733]: 2026-06-08 23:35:48 0 [Note] /usr/sbin/mariadb: ready for connections.
Jun 08 23:35:48 Icinga2-Master-Server mariadb[11733]: Version: '10.11.14-MariaDB-Ubuntu-24.04.1' socket: '/run/mysqld/mysqld.sock' port: 3306 Ubuntu 24.04
Jun 08 23:35:49 Icinga2-Master-Server systemd[1]: Started mariadb.service - MariaDB 10.11.14 database server.
Jun 08 23:35:49 Icinga2-Master-Server etc/mysql/debian-start[11749]: Upgrading MariaDB tables if necessary.
Jun 08 23:35:49 Icinga2-Master-Server etc/mysql/debian-start[11749]: Triggering myisam-recover for all MyISAM tables and aria-recover for all Aria tables
admin@icinga2-Master-Server:~$ sudo systemctl status icinga2
● icinga2.service - Icinga host/service/network monitoring system
   Loaded: loaded (/usr/lib/systemd/system/icinga2.service; enabled; preset: enabled)
   Active: active (running) since Mon 2026-06-08 23:37:41 UTC; 14min ago
     Docs: https://icinga.com/docs/icinga2/latest/
   Main PID: 15885 (icinga2)
   Status: "Startup finished."
     Tasks: 17 (limit: 103)
    Memory: 13.3M (peak: 38.9M)
       CPU: 24.242s
   CGroup: /system.slice/icinga2.service
           └─15885 /usr/lib/x86_64-linux-gnu/icinga2/sbin/icinga2 --no-stack-rlimit daemon --close-stdio -e
             └─15908 /usr/lib/x86_64-linux-gnu/icinga2/sbin/icinga2 --no-stack-rlimit daemon --close-stdio -e
               └─15913 /usr/lib/x86_64-linux-gnu/icinga2/sbin/icinga2 --no-stack-rlimit daemon --close-stdio -e

Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ConfigItem: Instantiated 1 NotificationComponent.
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ConfigItem: Instantiated 246 CheckCommands.
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ConfigItem: Instantiated 1 UserGroup.
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ConfigItem: Instantiated 3 ServiceGroups.
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ConfigItem: Instantiated 3 TimePeriods.
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ConfigItem: Instantiated 1 ScheduledDowntime.
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ConfigItem: Instantiated 12 Services.
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15908]: [2026-06-08 23:37:41 +0000] Information/ScriptGlobal: Dumping variables to file '/var/cache/icinga2/icinga2.vars'
Jun 08 23:37:41 Icinga2-Master-Server icinga2[15883]: [2026-06-08 23:37:41 +0000] Information/CLI: Closing console log.
Jun 08 23:37:41 Icinga2-Master-Server systemd[1]: Started Icinga2.service - Icinga host/service/network monitoring system.

```

Для передавання інформації про стан хостів і сервісів до бази даних було налаштовано IDO MySQL. Після встановлення відповідного компонента було

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський П.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

імпортовано схему бази даних Icinga та активовано функцію ido-mysql. Службові етапи налаштування IDO MySQL наведено в додатку М на рисунках М.2–М.5. [5]

Після підготовки базової частини Icinga 2 було встановлено Icinga Web 2. Вебінтерфейс використовується для перегляду стану хостів і сервісів, виконання повторних перевірок, перегляду історії подій та адміністрування модулів. Під час налаштування Icinga Web 2 було створено setup token, підключено базу даних моніторингу та завершено конфігурацію monitoring module. Додаткові службові етапи первинного налаштування Icinga Web 2 наведено в додатку М на рисунку М.6. [8]

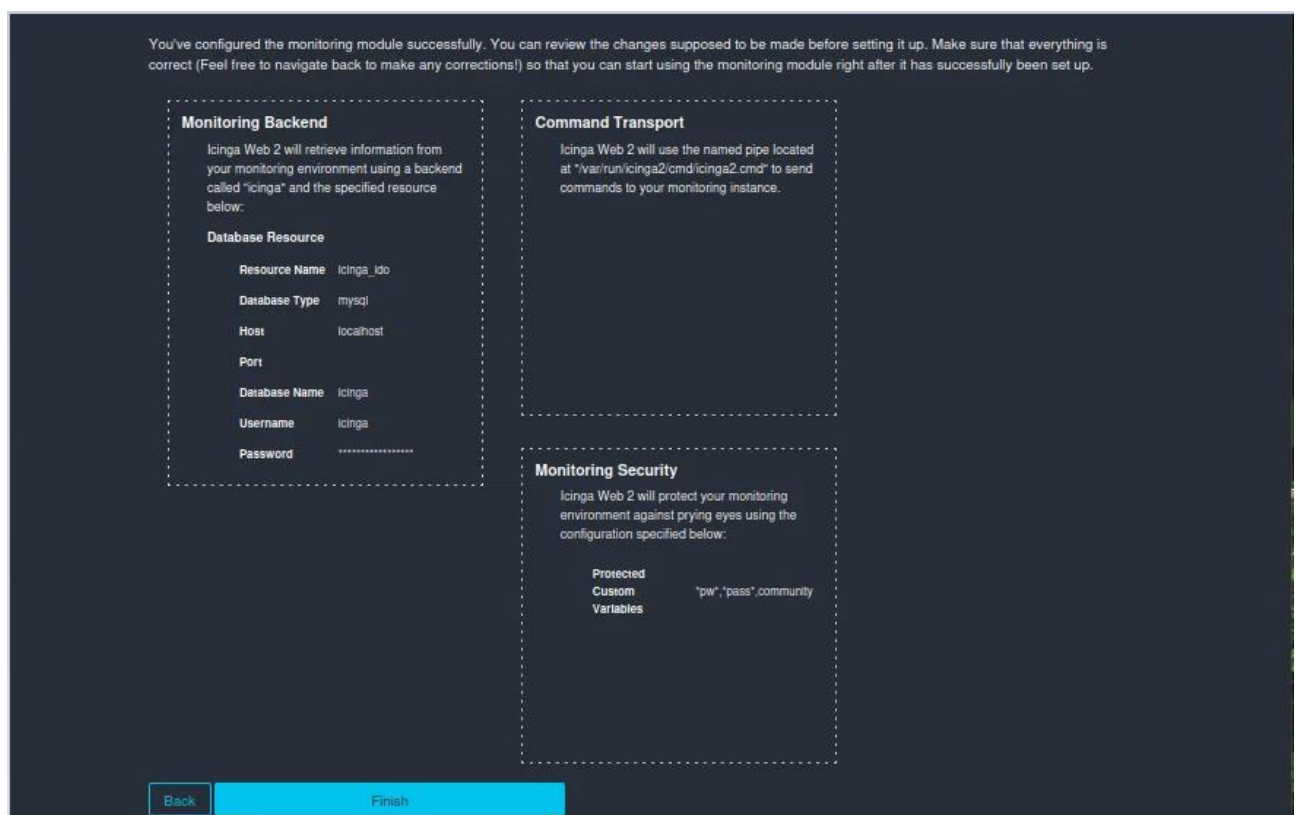


Рисунок 3.69 — Завершення налаштування monitoring module в Icinga Web 2

Для централізованого керування конфігурацією було встановлено модуль Icinga Director. Він використовується для створення хостів, шаблонів, сервісних наборів, правил автоматичного призначення перевірок, команд перевірки та змінних полів. Після встановлення модуль Director було активовано в Icinga Web 2, а також перевірено його доступність у переліку модулів. Налаштування ресурсу бази даних Director, Kickstart Wizard, сторінку стану Director та історію розгортань наведено в додатку М на рисунках М.7–М.10. [9]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

```
admin@icinga2-Master-Server:~$ sudo systemctl restart icinga2
admin@icinga2-Master-Server:~$ sudo apt install icingaweb2-module-director -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  icingaweb2-module-incubator icingaweb2-module-reactbundle
The following NEW packages will be installed:
  icingaweb2-module-director icingaweb2-module-incubator icingaweb2-module-reactbundle
0 upgraded, 3 newly installed, 0 to remove and 3 not upgraded.
Need to get 2,615 kB of archives.
After this operation, 12.4 MB of additional disk space will be used.
Get:1 http://ua.archive.ubuntu.com/ubuntu noble/universe amd64 icingaweb2-module-reactbundle all 0.9.0-1 [413 kB]
Get:2 http://ua.archive.ubuntu.com/ubuntu noble/universe amd64 icingaweb2-module-incubator all 0.20.0-2 [170 kB]
Get:3 http://ua.archive.ubuntu.com/ubuntu noble/universe amd64 icingaweb2-module-director all 1.10.2-2 [2,033 kB]
Fetched 2,615 kB in 4s (601 kB/s)
Preconfiguring packages ...
Selecting previously unselected package icingaweb2-module-reactbundle.
(Reading database ... 104861 files and directories currently installed.)
Preparing to unpack .../icingaweb2-module-reactbundle_0.9.0-1_all.deb ...
Unpacking icingaweb2-module-reactbundle (0.9.0-1) ...
Selecting previously unselected package icingaweb2-module-incubator.
Preparing to unpack .../icingaweb2-module-incubator_0.20.0-2_all.deb ...
Unpacking icingaweb2-module-incubator (0.20.0-2) ...
Selecting previously unselected package icingaweb2-module-director.
Preparing to unpack .../icingaweb2-module-director_1.10.2-2_all.deb ...
Unpacking icingaweb2-module-director (1.10.2-2) ...
Setting up icingaweb2-module-reactbundle (0.9.0-1) ...
Setting up icingaweb2-module-incubator (0.20.0-2) ...
Setting up icingaweb2-module-director (1.10.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/icingaweb2-module-director.service - /usr/lib/systemd/system/icingaweb2-module-director.service.
```

Рисунок 3.70 — Встановлення та активація модуля Icinga Director

Для взаємодії Icinga Director з Icinga 2 було налаштовано API. На сервері моніторингу було виконано ініціалізацію API, створено сертифікати, увімкнено API feature та додано API-користувача для Director. Службові конфігураційні файли API наведено в додатку М на рисунках М.11–М.13. [5; 9]

Після завершення налаштування центрального вузла Icinga2-Master-Server було підготовлено до подальшого створення об'єктів моніторингу, підключення агентів, налаштування шаблонів і розгортання сервісних перевірок.

Підготовка контрольованих вузлів до моніторингу

Після розгортання центрального вузла було виконано підготовку серверів і мережевого обладнання до моніторингу. У межах реалізованої інфраструктури використано два основні способи контролю: агентний моніторинг для серверів і SNMP-моніторинг для мережевого обладнання.

Для Windows Server 2022 було використано Icinga 2 Agent. У Icinga Director було сформовано інструкцію для агентного підключення хоста, яка містила параметри взаємодії з Icinga2-Master-Server, зокрема ticket, parent zone, parent endpoint та адресу центрального вузла. Приклад інструкції Director для підключення Windows Agent наведено в додатку Н на рисунку Н.1. [5; 6]

Безпосереднє налаштування Windows Agent було виконано за допомогою PowerShell-сценарію. Під час виконання сценарію було створено каталог сертифікатів, сформовано ключі, отримано сертифікат від Icinga CA, налаштовано взаємодію з Icinga2-Master-Server та перезапущено службу Icinga 2 Agent. Підготовку сценарію встановлення Windows Agent наведено в додатку Н на рисунку Н.2.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

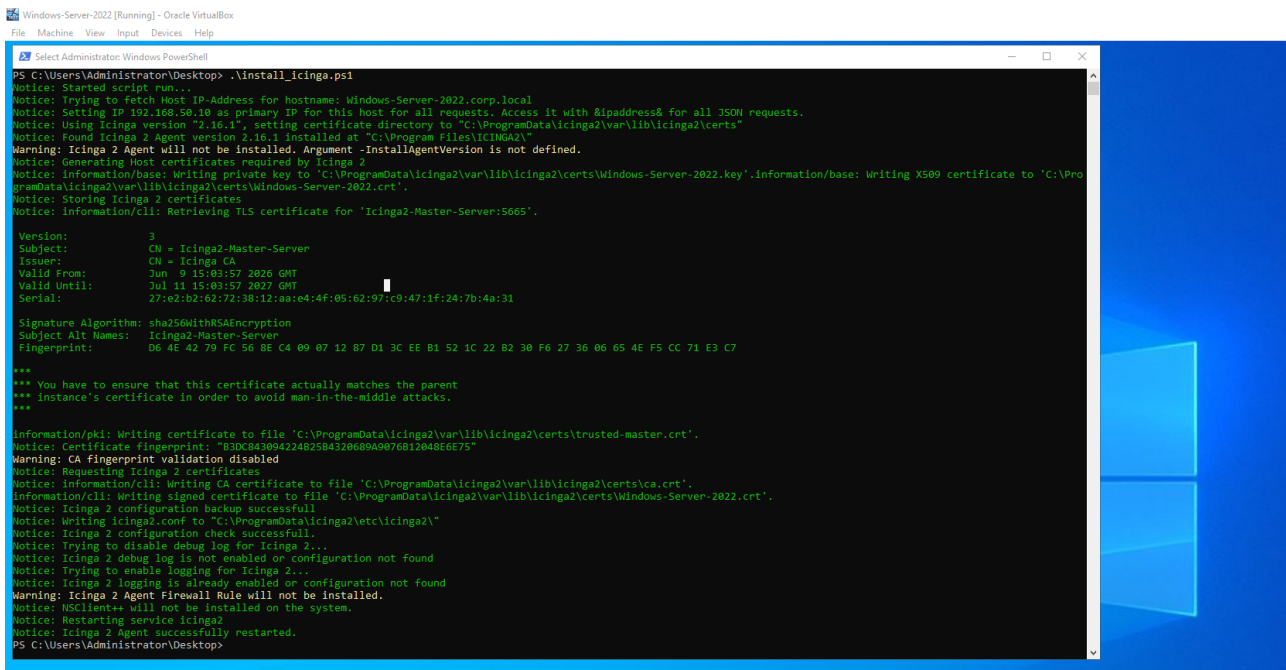


Рисунок 3.71 — Ініціалізація Icinga 2 Agent на Windows Server 2022

Після виконання сценарію було перевірено стан служби Icinga 2 на Windows Server 2022. У списку служб операційної системи служба Icinga 2 відображається у стані Running і має автоматичний тип запуску, що підтверджує коректну підготовку Windows-сервера до агентного моніторингу.

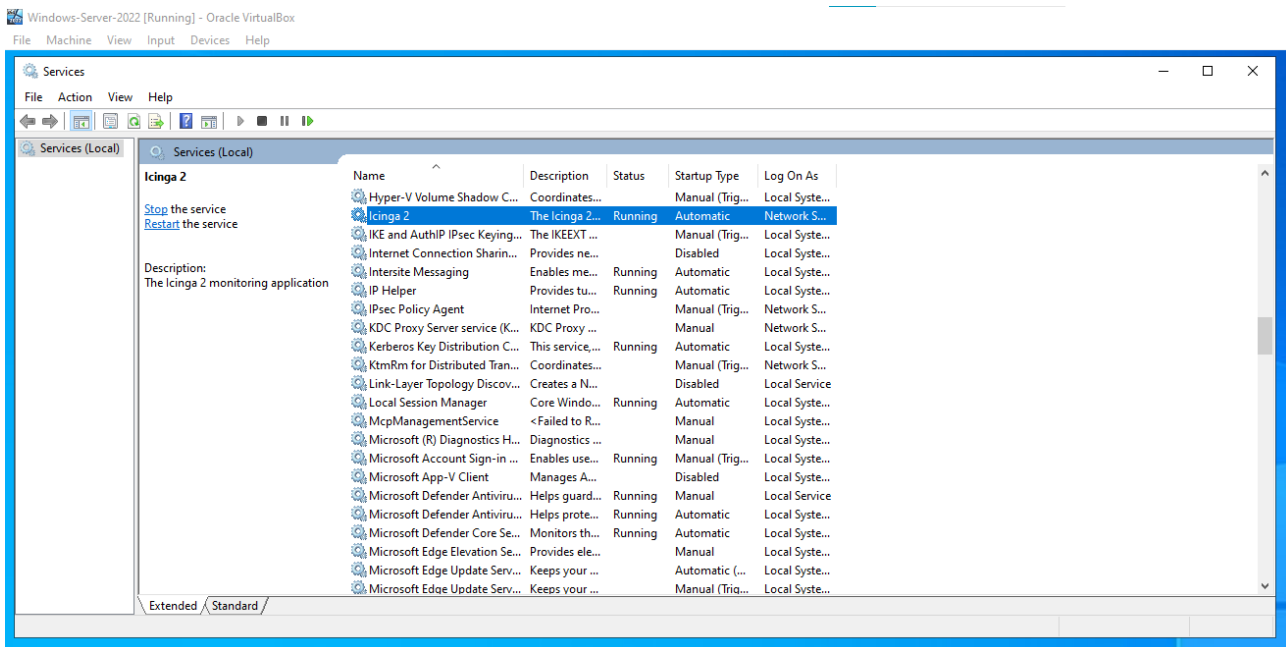


Рисунок 3.72 — Перевірка роботи служби Icinga 2 Agent на Windows Server 2022

Для Linux-серверів також було застосовано агентний підхід. У Icinga Director було створено відповідні хости та підготовлено командний сценарій ініціалізації агента. Він містить назву вузла, ticket, parent zone, parent endpoint та глобальну зону

		Берковський І.Ю.					ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.						85
Змн.	Арк.	№ докум.	Підпис	Дата				

director-global. Приклад створення Linux-хоста в Icinga Director та фрагмент сценарію ініціалізації агента наведено в додатку Н на рисунках Н.3. [5; 6; 29]

На Linux-App-Server було виконано сценарій `install_icinga.sh`. У процесі його виконання було перевірено наявність Icinga 2, створено каталог сертифікатів, отримано сертифікат центрального вузла, записано СА-сертифікат і підписаний сертифікат агента, увімкнено API feature та перевірено коректність конфігураційних файлів Icinga 2.

```
admin@Linux-App-Server ~$ sudo chmod +x install_icinga.sh
admin@Linux-App-Server ~$ sudo ./install_icinga.sh
INFO: This should be a Debian system
check: icinga2 installed - OK: 2.14.2-1
INFO: using new ssl directory: /var/lib/icinga2/certs
information/base: writing private key to '/var/lib/icinga2/certs/Linux-App-Server.key'.
information/base: writing X509 certificate to '/var/lib/icinga2/certs/Linux-App-Server.crt'.
information/base: writing certificate signing request to '/var/lib/icinga2/certs/Linux-App-Server.csr'.
information/cli: retrieving TLS certificate for 'Icinga2-Master-Server:5665'.
version: 3
Subject: CN = Icinga2-Master-Server
Issuer: CN = Icinga2
Valid From: Jun  9 15:03:57 2026 GMT
Valid until: Jul 11 15:03:57 2027 GMT
Serial: 27:c2:02:62:72:38:12:a4:e4:4f:05:62:97:c9:47:1f:24:7b:4a:31
Signature Algorithm: sha256withRSAEncryption
Subject Alt Names: Icinga2-Master-Server
Fingerprint: D6 4E 42 79 FC 58 8E C4 09 07 12 87 D1 3C EE B1 52 1C 22 B2 30 F6 27 36 06 65 4E F5 CC 71 E3 C7
***
*** You have to ensure that this certificate actually matches the parent
*** instance's certificate in order to avoid man-in-the-middle attacks.
***
information/pki: writing certificate to file '/var/lib/icinga2/certs/trusted-master.crt'.
information/cli: writing CA certificate to file '/var/lib/icinga2/certs/ca.crt'.
information/cli: writing signed certificate to file '/var/lib/icinga2/certs/Linux-App-Server.crt'.
INFO: creating a backup at /etc/icinga2/icinga2.conf.orig
writing config to /etc/icinga2/icinga2.conf
INFO: creating a backup at /etc/icinga2/zones.conf.orig
writing config to /etc/icinga2/zones.conf
INFO: creating a backup at /etc/icinga2/features-available/api.conf.orig
writing config to /etc/icinga2/features-available/api.conf
enabling feature api. Make sure to restart icinga 2 for these changes to take effect.
[2026-06-11 00:33:01 +0000] information/cli: Icinga application loader (version: r2.14.2-1)
[2026-06-11 00:33:01 +0000] information/cli: Loading configuration file(s).
[2026-06-11 00:33:01 +0000] information/ConfigItem: Committing config file(s).
[2026-06-11 00:33:01 +0000] information/Applister: My API identity: Linux-App-Server
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 1 IcingaApplication.
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 1 FileLogger.
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 3 Zones.
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 1 CheckerComponent.
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 2 Endpoints.
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 1 Apilister.
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 1 NotificationComponent.
[2026-06-11 00:33:02 +0000] information/ConfigItem: Instantiated 246 CheckCommands.
[2026-06-11 00:33:02 +0000] information/ScriptGlobal: Dumping variables to file '/var/cache/icinga2/icinga2.vars'
[2026-06-11 00:33:02 +0000] information/cli: Finished validating the configuration file(s).
Please restart icinga2.
systemctl restart icinga2
admin@Linux-App-Server ~$
```

Рисунок 3.73 — Ініціалізація Icinga 2 Agent на Linux-App-Server

Аналогічний підхід було застосовано для Database-Server та Backup-Server. Це дозволило забезпечити контроль базових параметрів Linux-серверів, зокрема доступності SSH, використання процесора, оперативної пам'яті, дискового простору, swar і кількості процесів.

Для мережевого обладнання агентний підхід не використовувався. Cisco-комутатори було підготовлено до моніторингу через SNMPv3, що дозволяє без встановлення агента отримувати інформацію про час роботи пристрою, завантаження процесора, оперативну пам'ять, стан VLAN, trunk-каналів і uplink-портів. Використання SNMPv3 забезпечує автентифікований і захищений обмін даними між Icinga2-Master-Server та мережевим обладнанням. [18; 19]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Core-L3-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#vlan 100
Core-L3-Switch(config-vlan)#name Net_Mgmt
Core-L3-Switch(config-vlan)#exit
Core-L3-Switch(config)#interface vlan 100
Core-L3-Switch(config-if)#
*Jun 12 17:20:23.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, c
hanged state to down
Core-L3-Switch(config-if)#ip address 192.168.100.254 255.255.255.0
Core-L3-Switch(config-if)#no shutdown
Core-L3-Switch(config-if)#exit
Core-L3-Switch(config)#
*Jun 12 17:20:31.614: %LINK-3-UPDOWN: Interface Vlan100, changed state to up
*Jun 12 17:20:32.616: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, c
hanged state to up
Core-L3-Switch(config)#ip access-list standard ACL_ICINGA
Core-L3-Switch(config-std-nacl)#permit 192.168.60.10
Core-L3-Switch(config-std-nacl)#exit
Core-L3-Switch(config)#snmpgroup v3 priv read vdefault access ACL_ICINGA
Core-L3-Switch(config)#v3 auth sha IcingaAuth123 priv aes 128 IcingaPriv123
Core-L3-Switch(config)#
*Jun 12 17:20:51.035: Configuring snmpv3 USM user, persisting snmpEngineBoots. P
lease wait...
Core-L3-Switch(config)#end
Core-L3-Switch#write memory
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 2535 bytes to 1360 bytes[OK]
Core-L3-Switch#
*Jun 12 17:20:57.098: %SYS-5-CONFIG_I: Configured from console by console
Core-L3-Switch#

```

Рисунок 3.74 — Підготовка Cisco-комутатора до SNMPv3-моніторингу

Підготовка всіх Cisco-комутаторів до моніторингу виконувалася за єдиним принципом. На кожному пристрої було передбачено керування через окремий мережевий сегмент, дозвіл доступу з боку Icinga2-Master-Server та SNMPv3-параметри для зчитування стану пристрою. Надалі відмінність між комутаторами полягала не в способі підготовки, а в наборі призначених перевірок: для Core-L3-Switch контролювалися також VLAN-інтерфейси та trunk-з'єднання, а для комутаторів доступу — базові параметри пристрою та стан uplink-порту.

Для pfSense було налаштовано SNMP-доступ, який використовується для контролю стану WAN- і LAN-інтерфейсів, часу безперервної роботи, завантаження процесора, доступної оперативної пам'яті та процесу Suricata. Це дозволяє контролювати не лише доступність граничного маршрутизатора, а й роботу засобу захисту периметра. Налаштування SNMP-сервісу на pfSense наведено в додатку П на рисунку П.1.

Таким чином, у межах підготовчого етапу було розгорнуто центральний вузол моніторингу, налаштовано вебінтерфейс і модуль Director, підготовлено Windows і Linux-сервери до агентного моніторингу, а Cisco-комутатори та pfSense — до безагентного SNMP-моніторингу. Для мережевого обладнання було застосовано уніфікований принцип підготовки, після чого різним типам пристроїв призначалися відповідні перевірки залежно від їхньої ролі в інфраструктурі. Це створило основу для подальшого створення хостів, шаблонів, сервісних наборів, правил призначення перевірок і спеціалізованих команд моніторингу.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

3.4.3. Створення хостів, шаблонів і правил моніторингу в Icinga Director

Після розгортання центрального вузла моніторингу та підготовки контрольованих систем було виконано створення об'єктів моніторингу в Icinga Director. На цьому етапі в системі було зареєстровано сервери, мережеве обладнання, граничний маршрутизатор pfSense та сам центральний сервер моніторингу. Такий підхід дозволяє централізовано керувати всіма контрольованими вузлами через вебінтерфейс Icinga Director. [6; 9]

У переліку хостів Icinga Director було створено об'єкти для Windows Server 2022, Linux-App-Server, Database-Server, Backup-Server, Icinga2-Master-Server, Core-L3-Switch, комутаторів доступу та pfSense Edge Router. Для кожного хоста було визначено його ім'я та IP-адресу, що надалі використовується під час виконання перевірок доступності, агентних перевірок або SNMP-запитів.

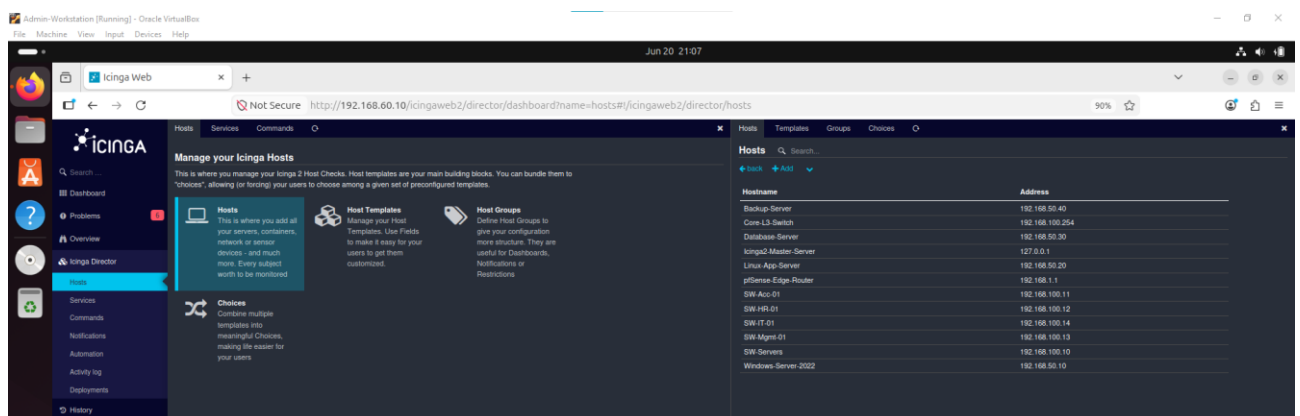


Рисунок 3.75 — Перелік контрольованих хостів у Icinga Director

Для спрощення адміністрування в Icinga Director було створено набір шаблонів хостів. Шаблони використовуються для групування спільних параметрів, які повторюються для однотипних вузлів. Наприклад, Windows-сервери успадковують параметри від шаблонів Windows-Base-Template та Windows-DC-Template, Linux-сервери — від Linux-Base-Template і рольових шаблонів, а мережеве обладнання — від шаблонів tpl-switch-core, tpl-switch-access і tpl-router-pfsense.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

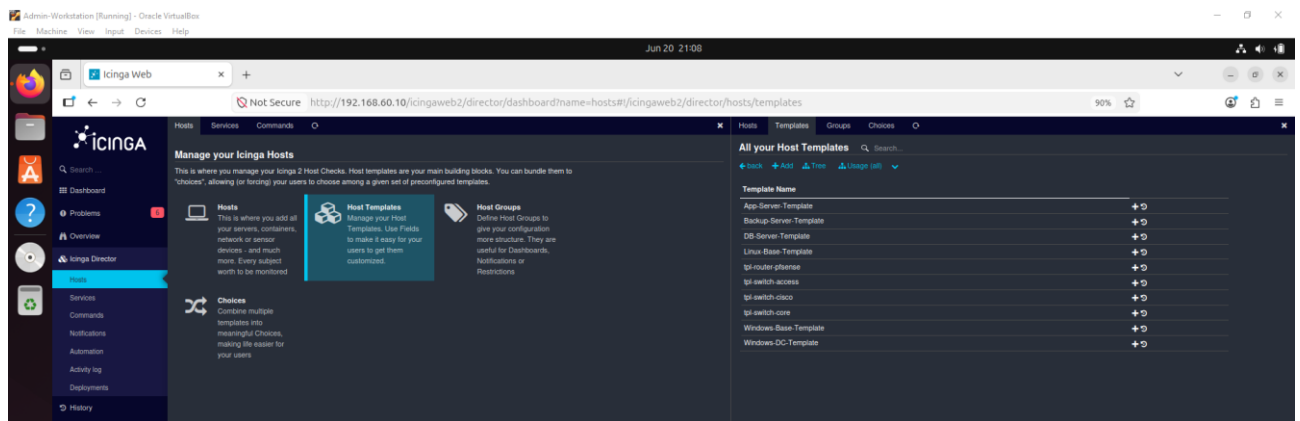


Рисунок 3.76 — Шаблони хостів для різних типів вузлів інфраструктури

Детальні приклади налаштування шаблонів хостів наведено в додатку Р на рисунках Р.1–Р.5. У цих шаблонах визначено спадкування базових параметрів, команду перевірки доступності `hostalive` та належність хоста до відповідного типу інфраструктурного вузла.

Для серверної частини інфраструктури було використано сервісні набори `Service Sets`. Вони дозволяють призначати одразу групу перевірок до відповідного типу хоста. Такий підхід зменшує кількість ручних дій і робить конфігурацію більш структурованою. У системі було створено окремі набори для базових Windows-перевірок, доменних служб, базових Linux-перевірок, прикладного сервера, сервера баз даних, `Backup-Server` та `Icinga2-Master-Server`.

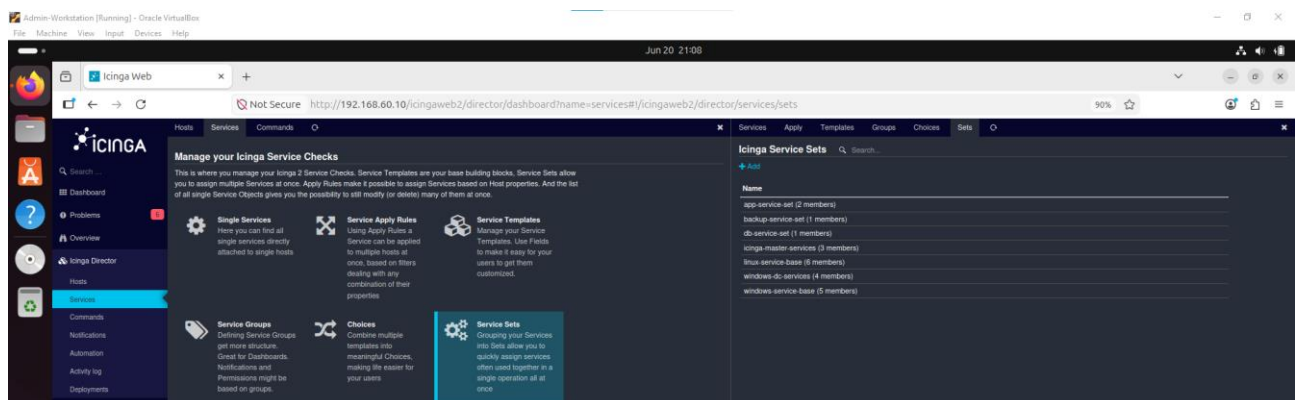


Рисунок 3.77 — Сервісні набори Icinga Director для автоматичного призначення перевірок

Детальні приклади сервісних шаблонів і сервісних наборів наведено в додатку С на рисунках С.1–С.8. Вони демонструють, які саме перевірки входять до базових і рольових наборів для Windows- та Linux-серверів.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

Для мережевого обладнання та pfSense було використано правила автоматичного призначення сервісів Apply Rules. На відміну від серверів, де доцільно застосовувати Service Sets, для Cisco-комутаторів і pfSense зручніше створювати правила, які автоматично призначають потрібні перевірки відповідно до шаблону хоста або його імені. Наприклад, базові SNMP-перевірки Cisco застосовуються до хостів із шаблоном tpl-switch-cisco, перевірки VLAN і trunk-з'єднань — до Core-L3-Switch, а перевірки pfSense — до хостів із шаблоном tpl-router-pfsense.

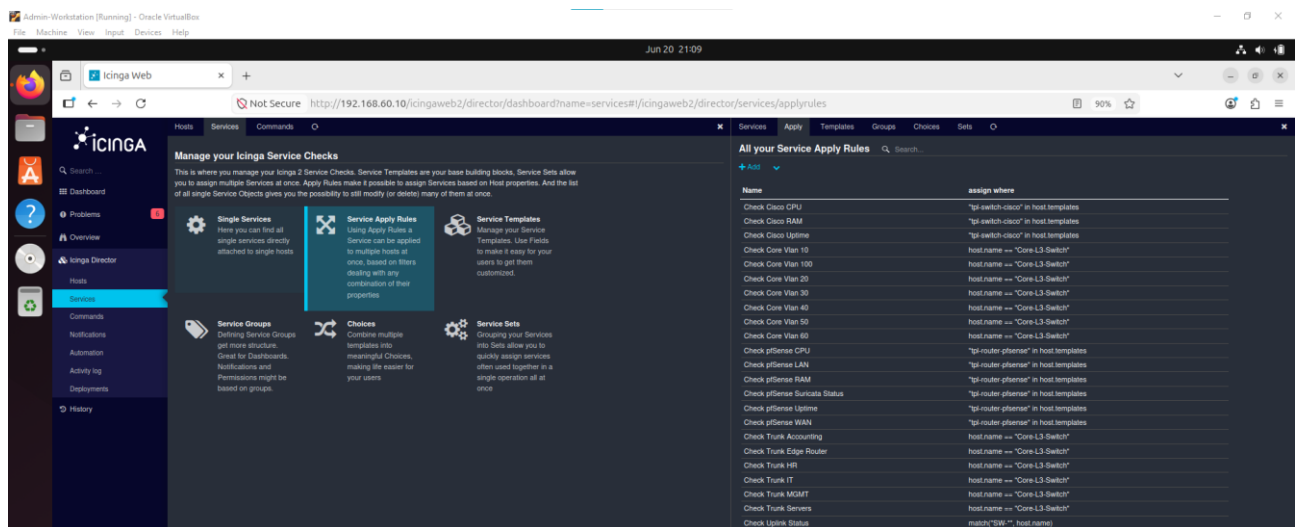


Рисунок 3.78 — Apply Rules для автоматичного призначення перевірок мережевому обладнанню та pfSense

Приклади правил Apply Rules для Cisco-комутаторів, VLAN, trunk-з'єднань, uplink-портів, pfSense та Suricata наведено в додатку Т на рисунках Т.1–Т.7.

Окремо в Icinga Director було налаштовано Data Fields та CheckCommands. Data Fields використовуються для передавання змінних значень у команди перевірок, наприклад назви служби Windows, імені Docker-контейнера, шляху до backup-журналу, режиму SNMP-перевірки або назви процесу. CheckCommands визначають, який саме плагін або скрипт буде виконуватися під час перевірки. Приклади Data Fields і CheckCommands наведено в додатку У на рисунках У.1–У.16. [9; 10]

Таким чином, у межах цього етапу було створено повну логічну модель моніторингу в Icinga Director: хости, шаблони, сервісні набори, правила автоматичного призначення перевірок, змінні поля та команди перевірки. Це

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		90

забезпечило централізоване керування моніторингом усіх основних компонентів інфраструктури.

3.4.4. Реалізація моніторингу Windows Server 2022

Після створення хостів, шаблонів і сервісних наборів було реалізовано моніторинг Windows Server 2022. Цей сервер є одним із ключових вузлів інфраструктури, оскільки на ньому розміщуються доменні та мережеві служби Active Directory Domain Services, DNS і DHCP. [5; 6; 20; 21; 22]

Для Windows Server 2022 було призначено базові перевірки продуктивності й доступності, а також спеціалізовані перевірки доменних служб. До базових перевірок належать контроль використання процесора, оперативної пам'яті, логічних дисків, мережевого інтерфейсу та доступності RDP. Це дозволяє відстежувати загальний технічний стан сервера та можливість адміністративного підключення до нього.

Окремо було реалізовано перевірки служб Active Directory Domain Services, Domain Name System, Dynamic Host Configuration Protocol та Windows Time Synchronization. Контроль цих служб є важливим, оскільки від них залежить автентифікація користувачів, робота доменного середовища, видача IP-адрес клієнтським станціям і синхронізація часу.

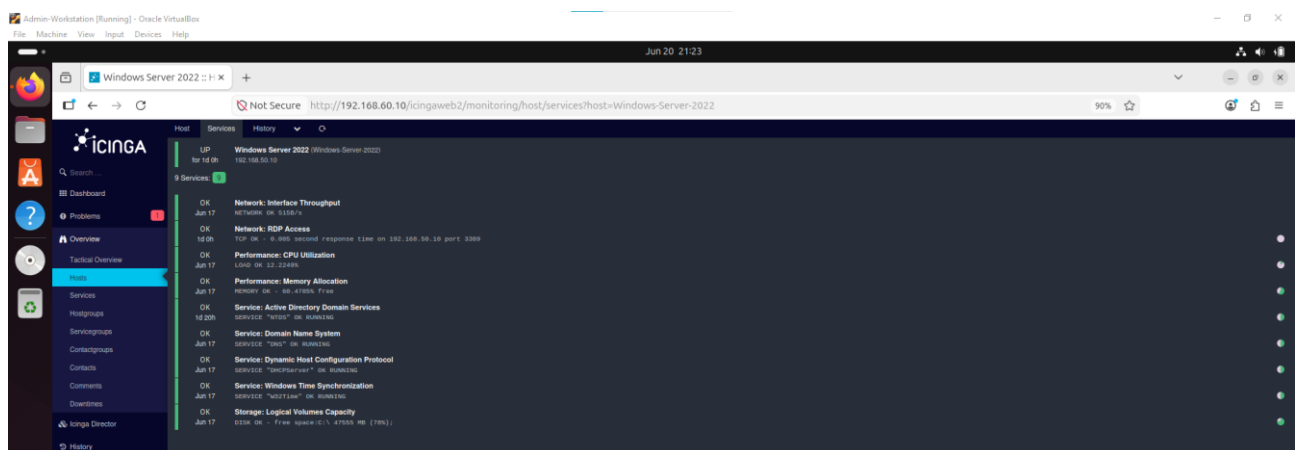


Рисунок 3.79 — Сервісні перевірки Windows Server 2022 у Icinga Web 2

На рисунку 3.79 видно, що Windows Server 2022 перебуває у стані UP, а всі призначені сервіси мають стан OK. Це підтверджує коректну роботу агентного моніторингу Windows-сервера та доступність основних доменних служб.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський П.Г.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

3.4.5. Реалізація моніторингу Linux-серверів і прикладних сервісів

Для Linux-серверів було реалізовано агентний моніторинг базових системних параметрів і спеціалізованих сервісів відповідно до ролі кожного вузла. До базового набору перевірок Linux-серверів входять доступність SSH, використання процесора, оперативної пам'яті, swar, кількість процесів і стан логічних томів.

На Linux-App-Server додатково було реалізовано контроль прикладного сервісу Nextcloud. Для цього використано перевірку доступності вебсервісу через HTTPS та перевірку стану Docker-контейнера Nextcloud. Такий підхід дозволяє контролювати не лише доступність самого сервера, а й фактичну працездатність прикладного сервісу. [24; 25; 26; 28]

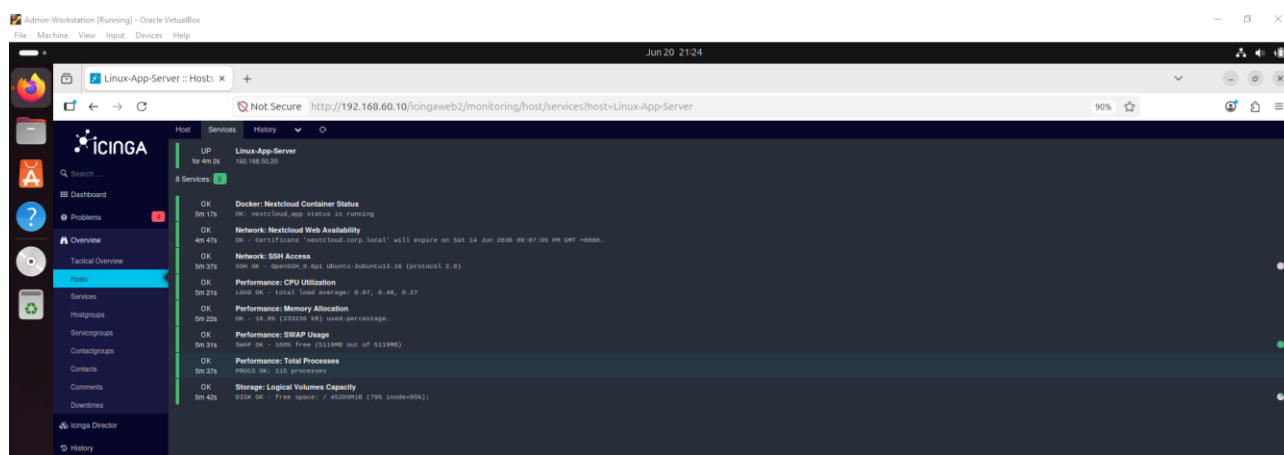


Рисунок 3.80 — Моніторинг Linux-App-Server та сервісу Nextcloud

На рисунку 3.80 показано, що Linux-App-Server перебуває у стані UP, а перевірки SSH, системних ресурсів, Docker-контейнера та вебдоступності Nextcloud мають стан OK. Це підтверджує працездатність прикладного рівня інфраструктури.

Для Database-Server було реалізовано базовий Linux-моніторинг і спеціалізовану перевірку MariaDB. Контроль MariaDB дозволяє відстежувати доступність сервера баз даних, який використовується сервісом Nextcloud для зберігання інформації. [27]

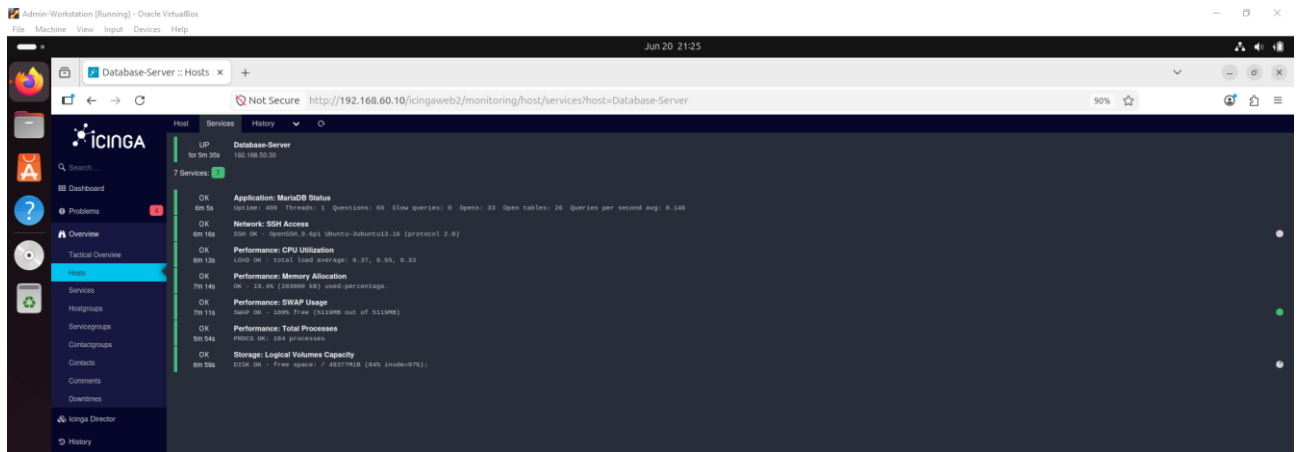


Рисунок 3.81 — Моніторинг Database-Server та служби MariaDB

На рисунку 3.81 видно, що Database-Server доступний, а служба MariaDB перебуває у стані ОК. Це підтверджує коректність налаштування перевірки бази даних і доступність СУБД для прикладного сервера.

Для Backup-Server було реалізовано базові перевірки Linux-сервера та окрему перевірку актуальності журналу резервного копіювання. Перевірка Backup Log Freshness дозволяє визначати, чи виконувався backup-сценарій у встановлений проміжок часу, і таким чином контролювати не лише наявність сервера, а й фактичну активність процесу резервного копіювання. [4]

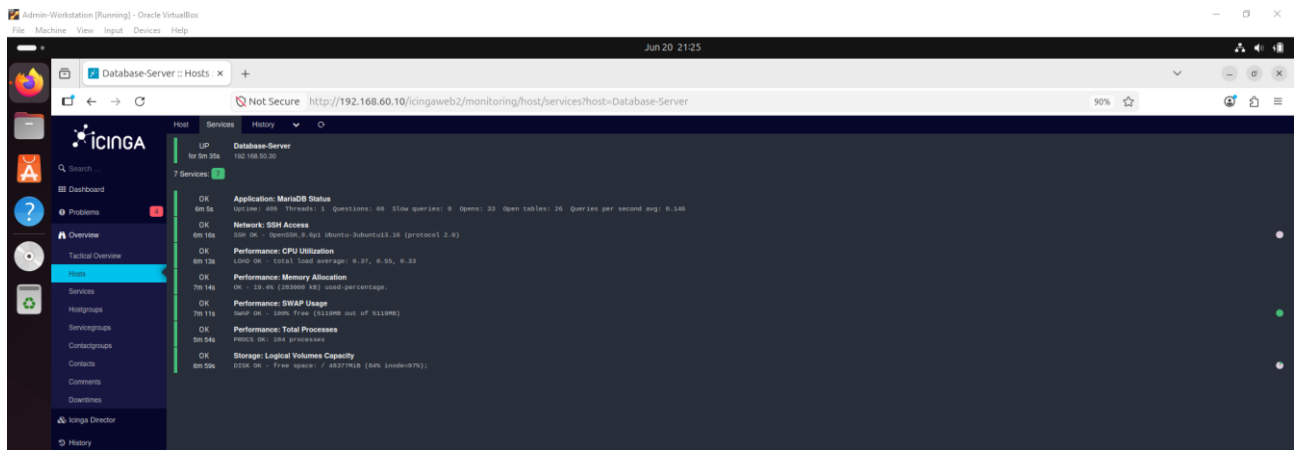


Рисунок 3.82 — Моніторинг Backup-Server та актуальності журналу резервного копіювання

На рисунку 3.82 показано, що Backup-Server доступний, базові системні перевірки мають стан ОК, а журнал резервного копіювання є актуальним. Це підтверджує працездатність контрольного механізму для backup-процесів.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

Таким чином, для Linux-серверів було реалізовано як базовий контроль операційної системи, так і рольові перевірки прикладного сервісу, бази даних і резервного копіювання.

3.4.6. Реалізація моніторингу Cisco-комутаторів

Для Cisco-комутаторів було реалізовано безагентний моніторинг через SNMPv3. Такий підхід дозволяє контролювати мережеве обладнання без встановлення додаткового програмного забезпечення на самі комутатори. Основними перевітками для Cisco-пристроїв стали контроль доступності, часу безперервної роботи, завантаження процесора та використання оперативної пам'яті. [18; 19]

Для Core-L3-Switch було створено розширений набір перевірок, оскільки цей пристрій виконує роль центрального маршрутизуючого вузла внутрішньої мережі. Окрім базових SNMP-перевірок, для нього було реалізовано контроль VLAN-інтерфейсів і trunk-з'єднань до комутаторів доступу, серверного сегмента та граничного маршрутизатора.

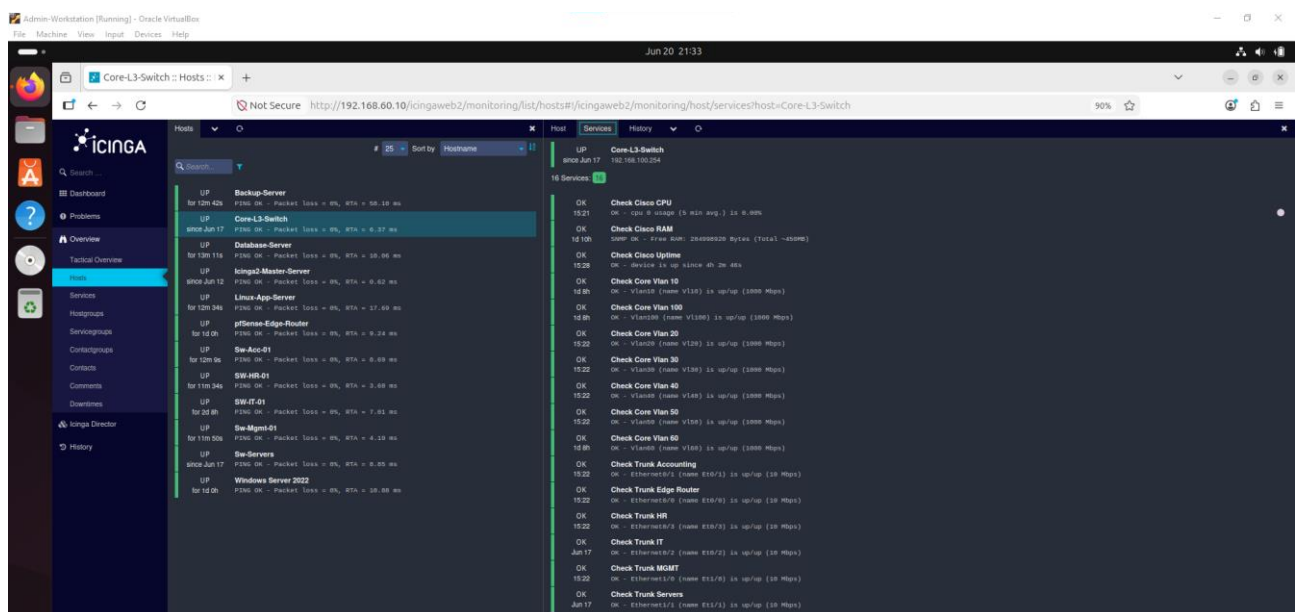


Рисунок 3.83 — Моніторинг Core-L3-Switch через SNMPv3

На рисунку 3.83 видно, що Core-L3-Switch перебуває у стані UP, а всі перевірки CPU, RAM, uptime, VLAN і trunk-з'єднань мають стан OK. Це підтверджує працездатність центрального комутатора та ключових мережевих зв'язків інфраструктури.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		94

Для комутаторів доступу було використано спрощений набір перевірок. Він включає контроль доступності пристрою, завантаження процесора, оперативної пам'яті, часу безперервної роботи та стану uplink-порту до комутатора ядра. Оскільки комутатори доступу мають однакову роль у мережі, для демонстрації достатньо навести приклад одного з них.

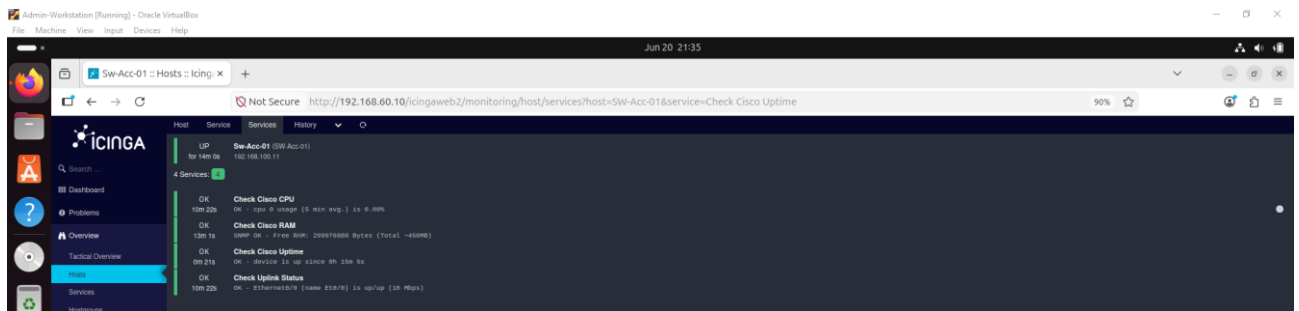


Рисунок 3.84 — Моніторинг комутатора доступу SW-Асс-01 через SNMPv3

На рисунку 3.84 показано, що SW-Асс-01 доступний, а його базові SNMP-перевірки та uplink-порт перебувають у стані ОК. Інші комутатори доступу контролюються за аналогічним принципом.

Таким чином, моніторинг Cisco-комутаторів охоплює як загальний стан пристроїв, так і ключові мережеві інтерфейси, від яких залежить зв'язність між сегментами корпоративної мережі.

3.4.7. Реалізація моніторингу pfSense та Suricata

Для граничного маршрутизатора pfSense було реалізовано безагентний моніторинг через SNMP. Оскільки pfSense виконує роль точки виходу корпоративної мережі до зовнішнього середовища та забезпечує роботу мережевого периметра, контроль його стану є важливим для стабільності всієї інфраструктури. [14]

У межах моніторингу pfSense було реалізовано перевірки часу безперервної роботи пристрою, завантаження процесора, доступної оперативної пам'яті, стану WAN- і LAN-інтерфейсів, а також процесу Suricata.

Окрема перевірка Suricata Status дозволяє контролювати працездатність засобу виявлення та запобігання вторгненням, який використовується для захисту зовнішнього периметра. [15; 16]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		95

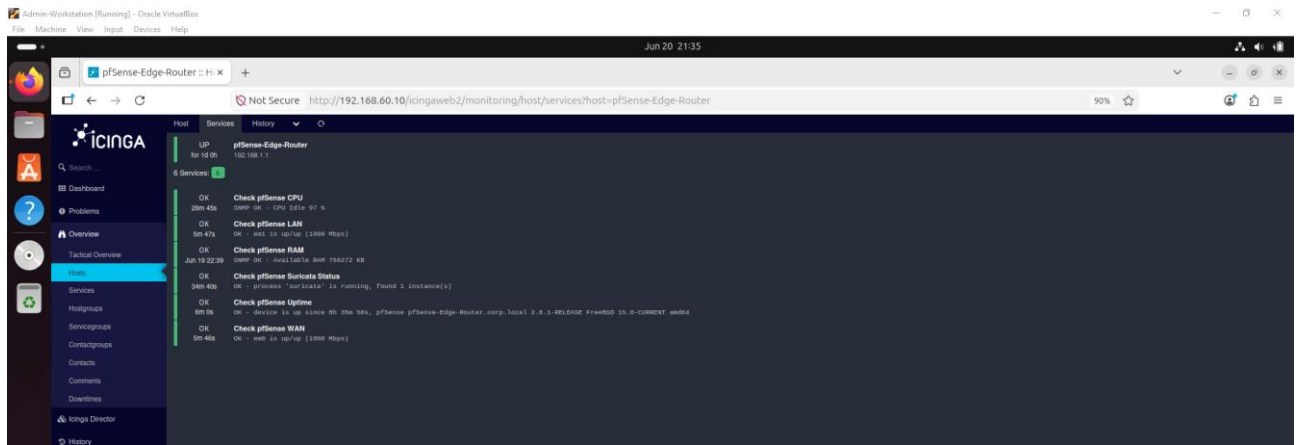


Рисунок 3.85 — Моніторинг pfSense та процеси Suricata в Icinga Web 2

На рисунку 3.85 видно, що pfSense-Edge-Router перебуває у стані UP, а перевірки CPU, RAM, WAN, LAN, uptime і Suricata Status мають стан OK. Це підтверджує, що граничний маршрутизатор і засіб захисту периметра контролюються централізовано через Icinga 2.

3.4.8. Підсумкова структура контрольованих вузлів і сервісів

Після налаштування хостів, шаблонів, сервісних наборів, Apply Rules, Data Fields і CheckCommands система моніторингу охоплює всі основні компоненти спроектованої інфраструктури. До моніторингу включено Windows Server 2022, Linux-App-Server, Database-Server, Backup-Server, Icinga2-Master-Server, Cisco Core-L3-Switch, комутатори доступу та pfSense Edge Router.

Загальний стан системи було перевірено через Tactical Overview в Icinga Web 2. Ця панель дозволяє швидко оцінити, чи є недоступні хости або сервіси в критичному стані. [8]

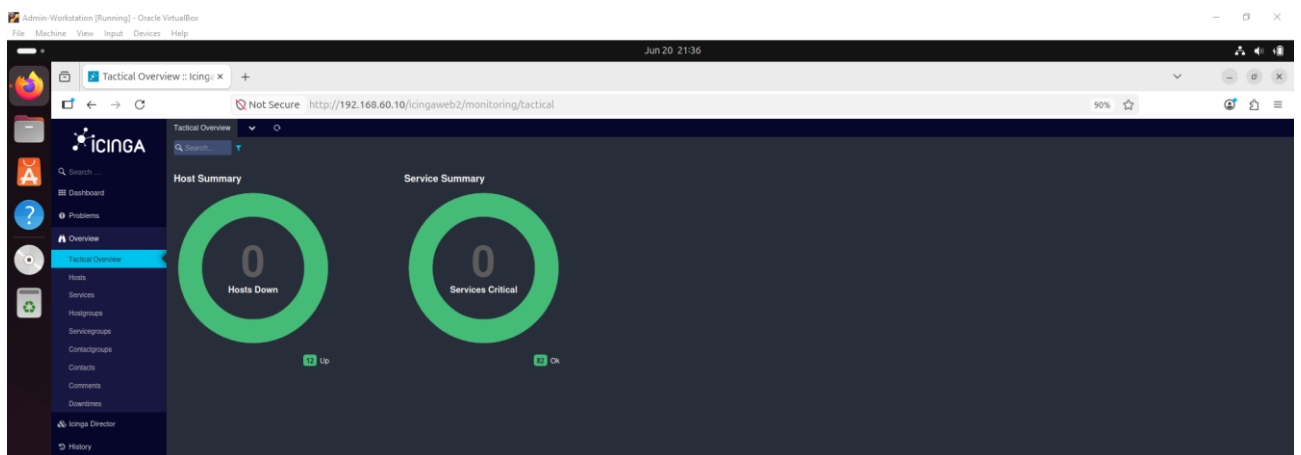


Рисунок 3.86 — Підсумковий стан хостів і сервісів у Icinga Web 2

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

На рисунку 3.86 показано, що кількість недоступних хостів дорівнює нулю, а критичних сервісів також немає. Це означає, що після завершення налаштування всі основні компоненти інфраструктури перебувають у робочому стані та успішно контролюються засобами Icinga 2.

Таким чином, у межах розділу було реалізовано централізовану систему моніторингу на базі Icinga 2. Вона забезпечує контроль серверів Windows і Linux, прикладного сервісу Nextcloud, бази даних MariaDB, процесу резервного копіювання, Cisco-комутаторів, pfSense та Suricata. Реалізована система створює основу для подальшого тестування реакції моніторингу на контрольовані збої. [5; 6; 8; 9]

3.5 Реалізація заходів забезпечення кібербезпеки

Оскільки розроблена система забезпечує автоматизовану взаємодію користувачів із сервісом штучного інтелекту через Telegram-бота, важливим аспектом її функціонування є забезпечення належного рівня кібербезпеки. Незважаючи на відносно просту архітектуру, система повинна бути захищеною від втрати даних, несанкціонованого доступу та можливих відмов у роботі. [1; 2; 31]

Одним із базових заходів є логічна сегментація мережі. Сервер, на якому розгортається застосунок, доцільно відокремити від інших сервісів за допомогою окремого мережевого сегмента або віртуальної мережі. Це дозволяє обмежити доступ до критичних компонентів системи та мінімізувати можливість поширення потенційних атак. Безпосередній доступ до бази даних повинен бути дозволений лише серверу застосунку, тоді як зовнішні користувачі взаємодіють виключно через Telegram API. [2; 3; 18; 31]

Не менш важливим є резервне копіювання інформації. Регулярне створення резервних копій бази даних дозволяє швидко відновити працездатність системи у випадку програмного збою, пошкодження даних або відмови обладнання. Резервні копії доцільно створювати автоматично через визначені проміжки часу із подальшим зберіганням на окремому носії або віддаленому сервері. [4]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

Для своєчасного виявлення можливих проблем доцільно здійснювати моніторинг критичних параметрів системи. До таких параметрів належать завантаження процесора, використання оперативної пам'яті, вільне місце на диску, доступність бази даних, швидкодія застосунку та стабільність підключення до зовнішніх сервісів. Постійний контроль цих показників дозволяє своєчасно виявляти відхилення та запобігати відмовам системи. [5; 6; 8]

Важливою складовою забезпечення кібербезпеки є журналювання подій. У журналі повинні фіксуватися запуск і завершення роботи застосунку, підключення до бази даних, виникнення помилок, отримання та обробка запитів, а також критичні системні події. Аналіз журналів дозволяє встановити причини можливих збоїв, виявити підозрілу активність та значно спрощує процес адміністрування системи. [1; 2]

У випадку виникнення критичних ситуацій система повинна оперативно повідомляти адміністратора. Наприклад, при втраті з'єднання з базою даних, багаторазових помилках роботи застосунку або недоступності зовнішнього API може автоматично надсилатися повідомлення електронною поштою або через окремий Telegram-бот. Це дозволяє швидко реагувати на інциденти та скоротити час простою сервісу. [31]

Окрему увагу слід приділити контролю доступності сервісів. Для цього можуть використовуватися засоби автоматичної перевірки працездатності застосунку, бази даних та мережевих служб. У разі виявлення недоступності окремого компонента система повинна зафіксувати подію в журналі та повідомити адміністратора. Регулярний контроль доступності забезпечує стабільну роботу програмного комплексу та підвищує його надійність. [5; 6; 8; 10]

Таким чином, реалізація наведених заходів дозволяє підвищити рівень захищеності інформаційної системи, забезпечити її безперервне функціонування та мінімізувати ризики втрати даних і виникнення критичних відмов. Навіть використання базових механізмів кіберзахисту значно покращує надійність програмного забезпечення та відповідає сучасним вимогам щодо безпечної експлуатації інформаційних систем. [1; 2; 3; 4]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		98

3.6. Тестування та оцінка результатів реалізованої системи моніторингу

Метою підрозділу є перевірка реакції системи моніторингу на контрольовані збої в різних компонентах інфраструктури. Для цього було штучно створено несправності в Windows-службі, SSH-доступі, Nextcloud HTTPS, MariaDB, backup-журналі, trunk-з'єднанні Cisco та процесі Suricata на pfSense. [5; 6; 8]

Тестування W32Time дозволяє перевірити контроль служби синхронізації часу Windows Server 2022, яка важлива для коректної роботи доменного середовища. Перевірка SSH-доступу показує, чи здатна Icinga виявити втрату основного каналу адміністрування Linux-сервера. [20; 21; 22]

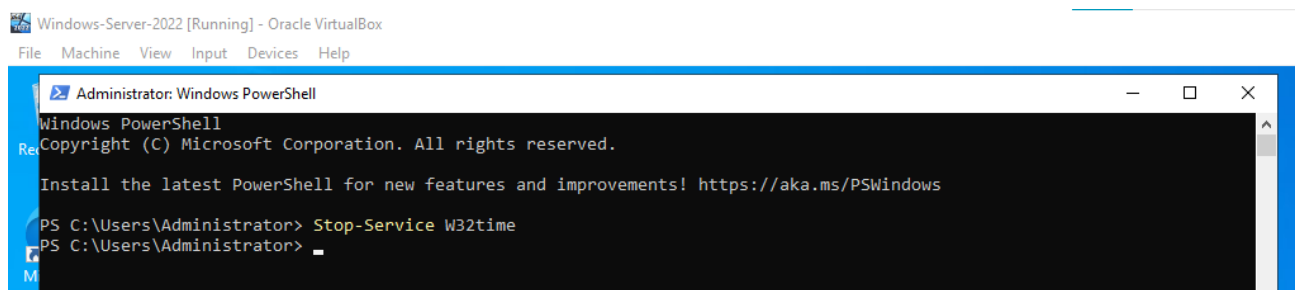
Тестування Nextcloud HTTPS і MariaDB використовується для перевірки прикладного рівня: перша перевірка показує доступність корпоративного вебсервісу, друга — працездатність бази даних, від якої залежить Nextcloud. Перевірка Backup Log Freshness дозволяє контролювати актуальність виконання резервного копіювання, а не лише доступність Backup-Server. [26; 27; 28]

Тестування trunk-з'єднання Cisco перевіряє реакцію моніторингу на порушення мережевої зв'язності. Тестування Suricata підтверджує, що Icinga контролює не тільки доступність pfSense, а й роботу окремого засобу захисту периметра. [15; 16; 18; 19]

3.5.1. Тестування моніторингу служби W32Time на Windows Server 2022

Першим тестом було перевірено реакцію системи моніторингу на зупинку служби синхронізації часу Windows Time. Ця служба важлива для доменного середовища, оскільки коректна синхронізація часу впливає на автентифікацію користувачів, роботу Kerberos і узгодженість подій у журналах. [20]

Для створення контрольованого збою на Windows Server 2022 було зупинено службу W32Time за допомогою PowerShell.



		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		99

Рисунок 3.87 — Зупинка служби W32Time на Windows Server 2022 для перевірки моніторингу

Після зупинки служби Icinga Web 2 зафіксувала зміну стану відповідної перевірки. Сервіс Windows Time Synchronization перейшов у стан CRITICAL, а в повідомленні перевірки було вказано, що служба W32Time не запущена.



Рисунок 3.88 — Спрацювання перевірки Windows Time Synchronization після зупинки служби W32Time

Результат тесту підтверджує, що агентний моніторинг Windows Server 2022 коректно відстежує стан окремих системних служб і може виявляти їх зупинку.

3.5.2. Тестування моніторингу SSH-доступу на Linux-сервері

Наступним тестом було перевірено моніторинг доступності SSH на Linux-сервері. SSH використовується як основний канал адміністрування Linux-серверів, тому його недоступність є важливою подією для адміністратора. [29]

Для створення збою на Database-Server було зупинено службу SSH та відповідний socket. Додатково було перевірено, що порт 22 більше не прослуховується.

```
admin@Database-Server:~$ sudo systemctl stop ssh
Stopping 'ssh.service', but its triggering units are still active:
ssh.socket
admin@Database-Server:~$ sudo systemctl stop ssh.socket
admin@Database-Server:~$ sudo systemctl stop ssh.service
admin@Database-Server:~$ sudo ss -lntp | grep ':22'
admin@Database-Server:~$ _
```

Рисунок 3.89 — Зупинка SSH-служби на Database-Server для перевірки моніторингу

Після цього перевірка Network: SSH Access у Icinga Web 2 перейшла у стан CRITICAL. У повідомленні було зазначено, що підключення до адреси Database-Server на порт 22 відхилено.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

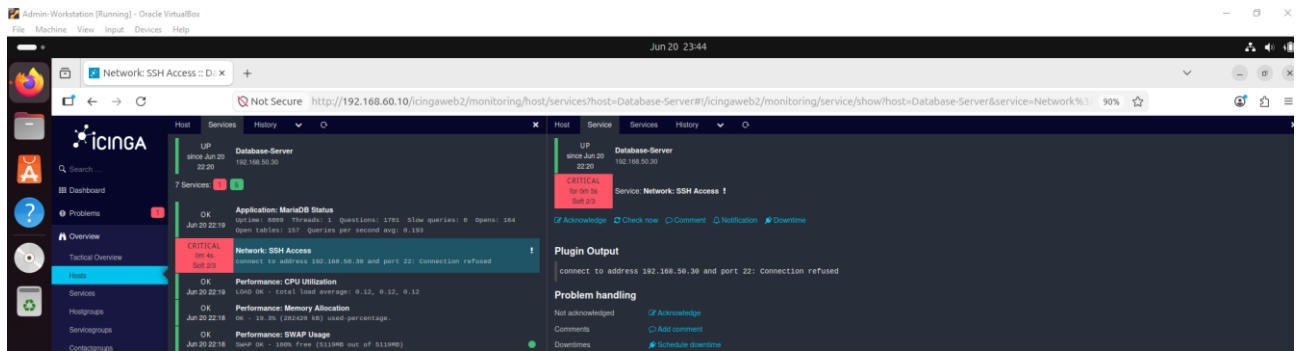


Рисунок 3.90 — Спрацювання перевірки SSH Access після зупинки SSH-служби на Database-Server

Результат тесту підтверджує, що система моніторингу коректно визначає недоступність адміністративного SSH-доступу до Linux-сервера.

3.5.3. Тестування моніторингу доступності Nextcloud через HTTPS

Для перевірки прикладного рівня було протестовано доступність вебсервісу Nextcloud. Цей сервіс є основним корпоративним файловим сховищем, тому його доступність через HTTPS є важливою для користувачів. [26; 28]

Контрольований збій було створено на Linux-App-Server шляхом додавання правила iptables, яке блокує вхідні з'єднання на TCP-порт 443. Це дозволило зімітувати недоступність HTTPS-сервісу без зупинки всього сервера.



Рисунок 3.91 — Блокування HTTPS-доступу до Nextcloud на Linux-App-Server

Після блокування порту Icinga Web 2 зафіксувала проблему з перевіркою Network: Nextcloud Web Availability. Сервіс перейшов у стан CRITICAL, а повідомлення перевірки вказало на неможливість відкрити TCP-з'єднання з портом 443.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		101

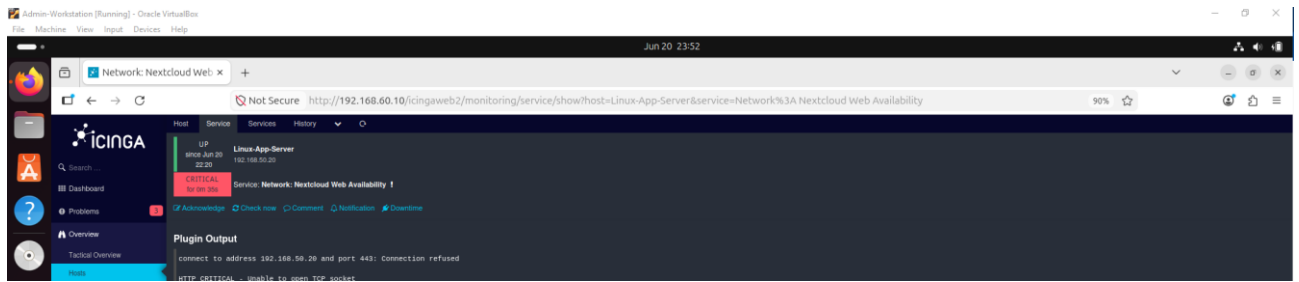


Рисунок 3.92 — Спрацювання перевірки доступності Nextcloud після блокування HTTPS-доступу

Результат тесту підтверджує, що Icinga 2 контролює не лише доступність Linux-App-Server як вузла, а й фактичну доступність прикладного вебсервісу Nextcloud.

3.5.4. Тестування моніторингу служби MariaDB

Наступним етапом було перевірено моніторинг сервера баз даних MariaDB. Ця служба використовується корпоративним сервісом Nextcloud для зберігання даних, тому її недоступність може вплинути на роботу прикладного рівня. [27]

Для створення контрольованої несправності на Database-Server було зупинено службу MariaDB.

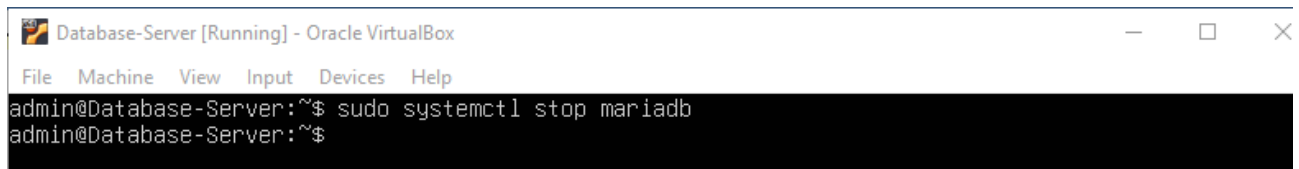


Рисунок 3.93 — Зупинка служби MariaDB на Database-Server для перевірки моніторингу

Після зупинки служби перевірка Application: MariaDB Status у Icinga Web 2 перейшла у стан CRITICAL. У повідомленні було зазначено, що система не може підключитися до MySQL/MariaDB-сервера на порт 3306.



Рисунок 3.94 — Спрацювання перевірки MariaDB після зупинки служби бази даних

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		102

Результат тесту підтверджує, що система моніторингу коректно виявляє зупинку служби бази даних і відображає причину збою в інтерфейсі Icinga Web 2.

3.5.5. Тестування моніторингу актуальності журналу резервного копіювання

Для перевірки контролю резервного копіювання було протестовано сервіс Backup Log Freshness. Його призначення полягає у визначенні актуальності журналу виконання backup-сценарію. Такий підхід дозволяє контролювати не лише доступність Backup-Server, а й факт регулярного виконання резервного копіювання. [4]

Для створення тестового збою було штучно змінено дату модифікації файлу журналу backup_run.log на значення триденної давності.

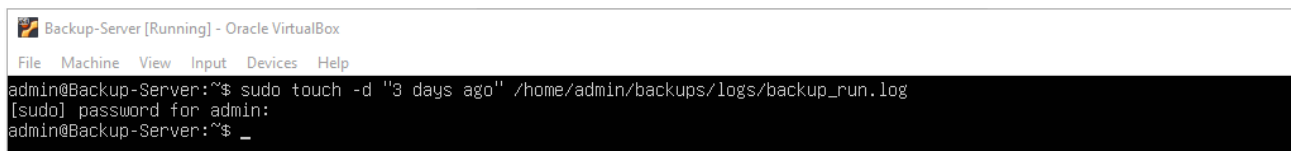


Рисунок 3.95 — Зміна дати журналу резервного копіювання для перевірки Backup Log Freshness

Після цього перевірка System: Backup Log Freshness у Icinga Web 2 перейшла у стан CRITICAL. У повідомленні перевірки було вказано, що файл журналу резервного копіювання має застарілий час модифікації.

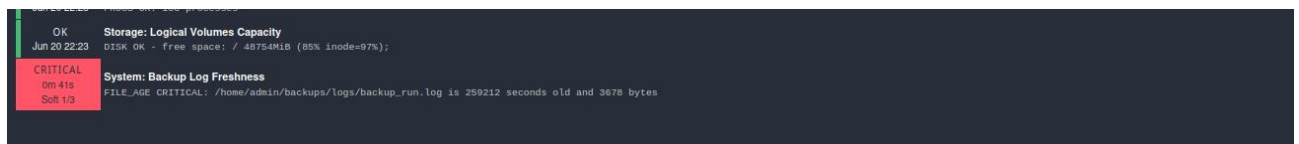


Рисунок 3.96 — Спрацювання перевірки Backup Log Freshness при застарілому журналі резервного копіювання

Результат тесту підтверджує, що система моніторингу здатна виявляти не лише повну відмову сервера, а й логічні проблеми в роботі службового процесу резервного копіювання.

3.5.6. Тестування моніторингу trunk-з'єднання Cisco Core-L3-Switch

Для перевірки моніторингу мережевого рівня було протестовано реакцію Icinga 2 на вимкнення інтерфейсу Cisco Core-L3-Switch. Оскільки trunk-з'єднання забезпечує передавання VLAN-трафіку між мережевими пристроями, його недоступність може впливати на роботу цілих сегментів інфраструктури. [18; 19]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		103

Для створення контрольованого збою на Core-L3-Switch було вимкнено інтерфейс Ethernet0/1 командою shutdown.

```
Core-L3-Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#interface Ethernet0/1
Core-L3-Switch(config-if)#shutdown
Core-L3-Switch(config-if)#end
Core-L3-Switch#
*Jun 21 00:03:32.028: %SYS-5-CONFIG_I: Configured from console by console
*Jun 21 00:03:33.012: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to a
dministratively down
Core-L3-Switch#
*Jun 21 00:03:34.013: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
Core-L3-Switch#
```

Рисунок 3.97 — Вимкнення інтерфейсу Ethernet0/1 на Cisco Core-L3-Switch

Після вимкнення інтерфейсу перевірка Check Trunk Accounting у Icinga Web 2 перейшла у стан CRITICAL. Це свідчить про те, що SNMPv3-моніторинг коректно визначив зміну стану контрольованого trunk-з'єднання.



Рисунок 3.98 — Спрацювання перевірки trunk-з'єднання Core-L3-Switch після вимкнення інтерфейсу

Додатково було зафіксовано, що після вимкнення відповідного інтерфейсу один із комутаторів доступу перейшов у стан DOWN. Це демонструє залежність доступу до частини мережі від стану trunk/uplink-з'єднання.



Рисунок 3.99 — Перехід комутатора доступу SW-Асс-01 у стан DOWN після порушення мережевого з'єднання

Результат тесту підтверджує, що система моніторингу виявляє не лише відмову окремого порту, а й наслідки цієї відмови для пов'язаного мережевого обладнання.

3.5.7. Тестування моніторингу процесу Suricata на pfSense

Останнім тестом було перевірено контроль роботи Suricata на граничному маршрутизаторі pfSense. Suricata використовується як засіб виявлення та

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		104

запобігання вторгненням, тому її працездатність є важливою для захисту зовнішнього периметра. [15; 16]

Для створення контрольованої ситуації Suricata на WAN-інтерфейсі pfSense було вимкнено. У вебінтерфейсі pfSense стан Suricata для інтерфейсу WAN відображається як вимкнений.

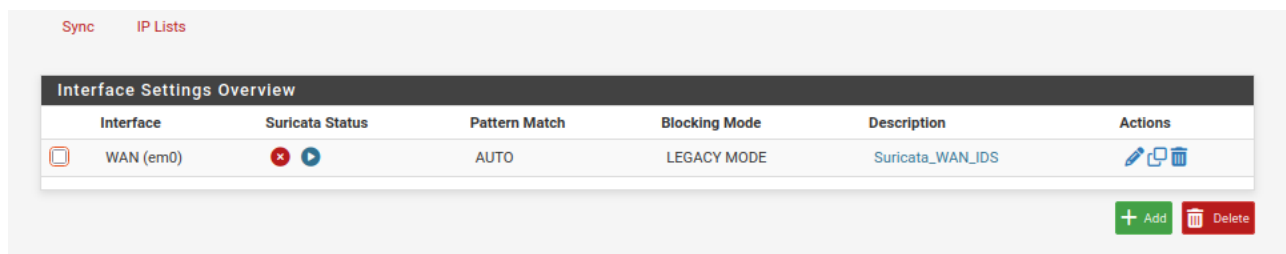


Рисунок 3.100 — Вимкнення Suricata на WAN-інтерфейсі pfSense

Після цього перевірка Check pfSense Suricata Status у Icinga Web 2 перейшла у стан CRITICAL. Це підтверджує, що Icinga 2 контролює не лише загальний стан pfSense, а й працездатність окремого процесу захисту периметра.



Рисунок 3.101 — Спрацювання перевірки Suricata Status після вимкнення Suricata на pfSense

Результат тесту підтверджує, що система моніторингу здатна виявляти зупинку або недоступність засобу захисту периметра, що є важливим для контролю безпеки мережі.

Висновки до розділу 3

У третьому розділі було виконано практичну реалізацію спроектованої IT-інфраструктури організації та системи її моніторингу. Спочатку було налаштовано мережеву основу: граничний маршрутизатор pfSense, Cisco Core L3 Switch, комутатори доступу, VLAN-сегментацію, транзитний сегмент між pfSense і ядром мережі, статичну маршрутизацію, NAT, DHCP Relay, trunk/access-порти та базові правила доступу. Це забезпечило логічне розділення інфраструктури та

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		105

контрольовану взаємодію між користувацькими, серверними, адміністративними й моніторинговими сегментами.

Було реалізовано доменну, клієнтську, серверну та прикладну частину інфраструктури. Windows Server 2022 було налаштовано для роботи Active Directory, DNS і DHCP. Клієнтські робочі станції було підключено до відповідних VLAN і доменного середовища. Адміністративна станція була виділена в окремий IT-сегмент для керування серверами, мережевим обладнанням, pfSense та системою моніторингу. На Linux-серверах було розгорнуто MariaDB, Nextcloud, Docker, Nginx, HTTPS-доступ і механізм централізованого резервного копіювання.

У межах реалізації політик доступу було застосовано групові політики Active Directory, обмеження між VLAN за допомогою Extended ACL, правила доступу до адміністративних інтерфейсів та захист периметра на базі Suricata IDS/IPS. Це дозволило обмежити доступ звичайних користувачів до критичних серверів, мережевого обладнання, pfSense та системи моніторингу, а також забезпечити контроль підозрілої активності на WAN-рівні. [1; 2; 3; 14; 16; 17; 23]

Окремим етапом було реалізовано систему моніторингу на базі Icinga 2. На Icinga2-Master-Server було розгорнуто Icinga 2, Icinga Web 2, MariaDB/IDO та Icinga Director. Для Windows Server 2022 і Linux-серверів було використано агентний моніторинг, а для Cisco-комутаторів і pfSense — SNMP-моніторинг. У Icinga Director було створено хости, шаблони, сервісні набори, Apply Rules, Data Fields і CheckCommands, що дозволило централізовано керувати перевітками різних типів вузлів. [5; 6; 8; 9]

Реалізована система моніторингу охоплює ключові компоненти інфраструктури: Windows Server 2022, Linux-App-Server, Database-Server, Backup-Server, Icinga2-Master-Server, Cisco Core L3 Switch, комутатори доступу, pfSense, Nextcloud, Docker-контейнер, MariaDB, backup-журнал, VLAN/trunk/uplink-з'єднання та процес Suricata. Це дозволяє контролювати не лише доступність хостів, а й стан конкретних служб, прикладних сервісів, мережевих інтерфейсів і механізмів захисту.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		106

Проведене тестування підтвердило працездатність реалізованої системи. Icinga 2 коректно реагувала на контрольовані збої: зупинку W32Time, недоступність SSH, блокування HTTPS-доступу до Nextcloud, зупинку MariaDB, застарілий backup-журнал, вимкнення trunk/uplink-інтерфейсу Cisco та вимкнення Suricata на pfSense. У кожному випадку відповідна перевірка переходила у стан CRITICAL або DOWN і відображала причину проблеми. [5; 6; 8]

Таким чином, у третьому розділі було підтверджено, що спроектована інфраструктура може бути реалізована в лабораторному середовищі, а система моніторингу на базі Icinga 2 здатна централізовано контролювати її основні компоненти. Реалізоване рішення відповідає темі кваліфікаційної роботи, оскільки поєднує побудову IT-інфраструктури організації з практичним розгортанням, налаштуванням і тестуванням системи моніторингу.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				107
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У кваліфікаційній роботі було виконано проектування, реалізацію та тестування системи моніторингу IT-інфраструктури організації на базі Icinga 2. У межах роботи було розглянуто корпоративну IT-інфраструктуру як об'єкт моніторингу, визначено її основні компоненти, залежності між ними та типові проблеми, які можуть виникати під час експлуатації.

У першому розділі було проаналізовано особливості моніторингу мережевих, серверних, доменних і прикладних компонентів IT-інфраструктури. Розглянуто основні підходи до моніторингу, зокрема агентний, безагентний, комбінований і шаблонний підхід. Також було виконано порівняльний аналіз систем Icinga 2, Zabbix, Nagios та Prometheus. За результатами аналізу для реалізації було обрано Icinga 2, оскільки вона підтримує агентний і SNMP-моніторинг, роботу з плагінами, шаблонами, правилами призначення перевірок, Icinga Web 2 та Icinga Director. [5; 6; 8; 9; 11; 12; 13]

У другому розділі було спроектовано IT-інфраструктуру організації та систему її моніторингу. Визначено зональну архітектуру, VLAN-сегментацію, адресний простір, ролі серверних вузлів, підхід до резервного копіювання, політики доступу, захист мережевого периметра та модель централізованого моніторингу. Запропонована модель передбачає розмежування користувацьких, серверних, адміністративних, моніторингових і management-сегментів, що створює основу для контрольованого доступу та зменшення ризику горизонтального переміщення в мережі. [1; 2; 3; 4; 14; 17; 18; 20; 21; 22; 23]

У третьому розділі було виконано практичну реалізацію спроектованої інфраструктури. Було налаштовано граничний маршрутизатор pfSense, Cisco Core L3 Switch, комутатори доступу, VLAN-сегментацію, маршрутизацію, DHCP Relay, NAT і правила доступу. Також було розгорнуто Windows Server 2022 з ролями Active Directory, DNS і DHCP, клієнтські робочі станції, адміністративну станцію, Linux-сервери, Nextcloud, MariaDB, Backup-Server, Nginx, HTTPS-доступ і Suricata IDS/IPS. [14; 16; 18; 20; 21; 22; 24; 25; 26; 27; 28; 29]

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		108

На завершальному етапі було реалізовано систему моніторингу на базі Icinga 2. На Icinga2-Master-Server було розгорнуто Icinga 2, Icinga Web 2, MariaDB/IDO та Icinga Director. Для Windows Server 2022 і Linux-серверів було використано агентний моніторинг, а для Cisco-комутаторів і pfSense — SNMP-моніторинг. У Icinga Director було створено хости, шаблони, сервісні набори, Apply Rules, Data Fields і CheckCommands. [5; 6; 8; 9]

Реалізована система моніторингу охоплює Windows Server 2022, Linux-App-Server, Database-Server, Backup-Server, Cisco Core L3 Switch, комутатори доступу, pfSense, Nextcloud, Docker-контейнер, MariaDB, backup-журнал і процес Suricata. Це дозволяє контролювати не лише доступність вузлів, а й стан конкретних служб, прикладних сервісів, мережевих інтерфейсів, резервного копіювання та засобів захисту периметра.

Проведене тестування підтвердило працездатність реалізованої системи моніторингу. Icinga 2 коректно реагувала на контрольовані збої, зокрема зупинку W32Time, недоступність SSH, блокування HTTPS-доступу до Nextcloud, зупинку MariaDB, застарілий backup-журнал, вимкнення trunk/uplink-інтерфейсу Cisco та вимкнення Suricata на pfSense. У кожному випадку відповідна перевірка переходила у стан CRITICAL або DOWN і відображала причину проблеми. [5; 6; 8]

Отже, мету кваліфікаційної роботи досягнуто. Було спроектовано, реалізовано та протестовано систему централізованого моніторингу ІТ-інфраструктури організації на базі Icinga 2. Реалізоване рішення дає змогу адміністратору централізовано контролювати стан ключових компонентів інфраструктури, швидко виявляти проблеми та оцінювати їхній вплив на роботу мережевих, серверних, прикладних і безпекових сервісів.

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		109

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
2. Center for Internet Security. CIS Critical Security Controls Version 8.1. URL: <https://www.cisecurity.org/controls/v8-1>
3. National Institute of Standards and Technology. Zero Trust Architecture. NIST Special Publication 800-207. URL: <https://csrc.nist.gov/pubs/sp/800/207/final>
4. National Institute of Standards and Technology. Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Revision 1. URL: <https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>
5. Icinga 2 Documentation. Installation. URL: <https://icinga.com/docs/icinga-2/latest/doc/02-installation/>
6. Icinga 2 Documentation. Monitoring Basics. URL: <https://icinga.com/docs/icinga-2/latest/doc/03-monitoring-basics/>
7. Icinga 2 Documentation. Features. URL: <https://icinga.com/docs/icinga-2/latest/doc/14-features/>
8. Icinga Web Documentation. URL: <https://icinga.com/docs/icinga-web/latest/>
9. Icinga Director Documentation. Director Setup Walkthrough. URL: <https://icinga.com/docs/get-started/latest/doc/12-director/>
10. Monitoring Plugins. Development Guidelines. URL: <https://www.monitoring-plugins.org/doc/guidelines.html>
11. Zabbix Documentation. URL: <https://www.zabbix.com/documentation/current/en/start>
12. Nagios Core Documentation. URL: <https://www.nagios.org/documentation/>
13. Prometheus Documentation. Overview. URL: <https://prometheus.io/docs/introduction/overview/>
14. Netgate Documentation. Firewall. pfSense Documentation. URL: <https://docs.netgate.com/pfsense/en/latest/firewall/index.html>
15. Netgate Documentation. IDS / IPS. pfSense Documentation. URL: <https://docs.netgate.com/pfsense/en/latest/packages/snort/index.html>

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				110
Змн.	Арк.	№ докум.	Підпис	Дата		

- 16.Suricata User Guide. URL: <https://docs.suricata.io/>
- 17.Cisco. Configure IP Access Lists. URL: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html>
- 18.Cisco. Configuring VLANs. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-9/configuration_guide/vlan/b_179_vlan_9200_cg/configuring_vlans.html
- 19.Cisco. SNMP Version 3. URL: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xr-3se/3650/snmp-xr-3se-3650-book/nm-snmp-snmpv3.pdf>
- 20.Microsoft Learn. Active Directory Domain Services Overview. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- 21.Microsoft Learn. Domain Name System DNS Overview. URL: <https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-overview>
- 22.Microsoft Learn. Install and Configure DHCP Server on Windows Server. URL: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server>
- 23.Microsoft Learn. Group Policy Overview. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview>
- 24.Docker Docs. Docker Documentation. URL: <https://docs.docker.com/>
- 25.Docker Docs. Docker Compose. URL: <https://docs.docker.com/compose/>
- 26.Nextcloud Documentation. Administration Manual. URL: https://docs.nextcloud.com/server/latest/admin_manual/
- 27.MariaDB Documentation. URL: <https://mariadb.com/docs/>
- 28.NGINX Documentation. NGINX Reverse Proxy. URL: <https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/>
- 29.Ubuntu Server Documentation. URL: <https://documentation.ubuntu.com/server/>
- 30.GNS3 Documentation. URL: <https://docs.gns3.com/>
- 31.Telegram Bot API. URL: <https://core.telegram.org/bots/api>

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				111
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				112
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальна логічна схема ІТ-інфраструктури організації

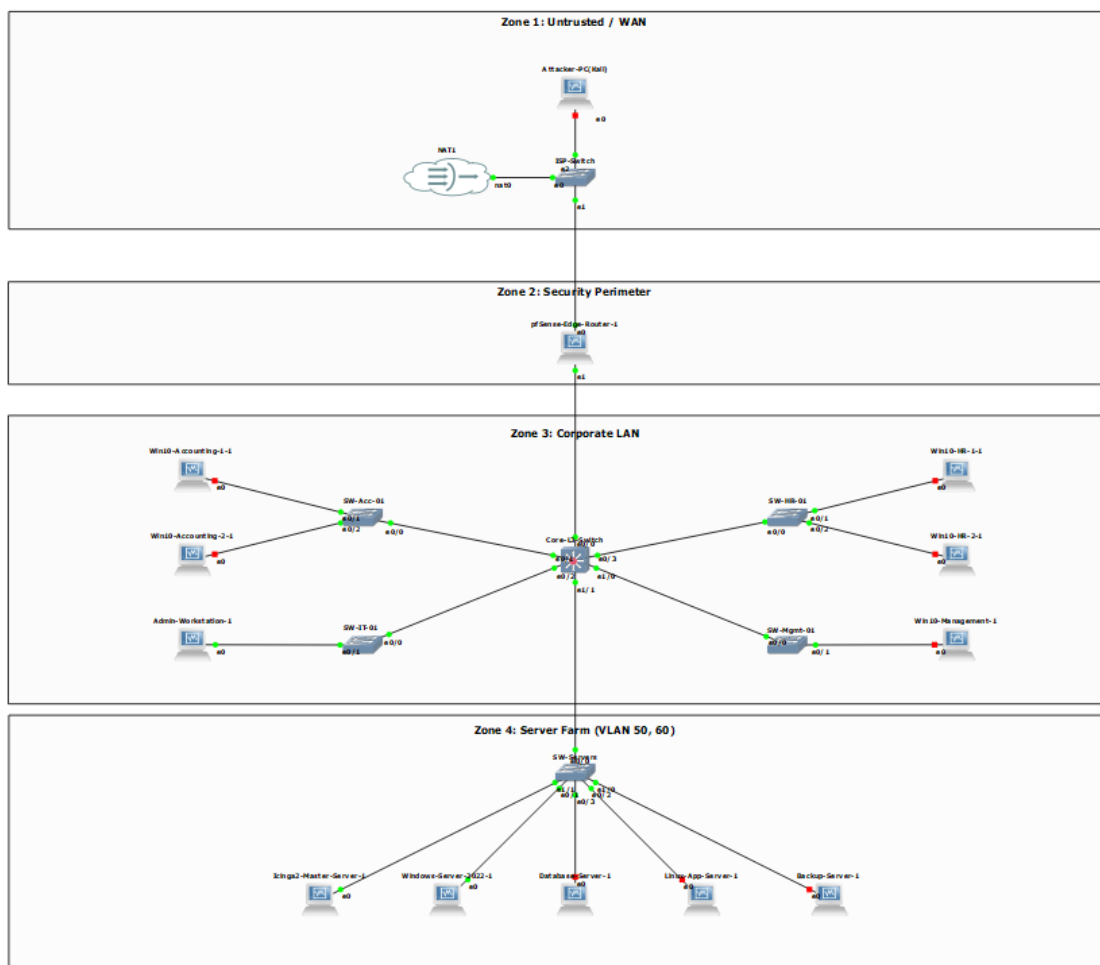


Рисунок А.1 — Загальна логічна схема ІТ-інфраструктури організації в середовищі GNS3

Компонент ІТ-інфраструктури	Розміщення в архітектурі	Основне призначення
pfSense-Edge-Router	зона безпекового периметра	Забезпечення виходу корпоративної мережі до зовнішньої мережі, виконання NAT, фільтрація трафіку та захист мережевого периметра
Cisco Core L3 Switch	ядро корпоративної локальної мережі	Центральна маршрутизація між логічними сегментами мережі, створення шлюзів VLAN та передача трафіку до граничного маршрутизатора
Комутатори доступу	рівень доступу корпоративної мережі	Підключення користувацьких, адміністративних і серверних вузлів до відповідних логічних сегментів
Користувацькі робочі станції	корпоративна локальна мережа	Робочі місця працівників підрозділів організації, які використовують доменну автентифікацію та корпоративні сервіси
Адміністративна станція	адміністративний сегмент	Довірене робоче місце для керування серверами, мережевим обладнанням, доменом і системою моніторингу
Windows Server 2022	серверна ферма	Виконання ролей Active Directory Domain Services, DNS-сервера та DHCP-сервера
Linux-App-Server	серверна ферма	Розміщення прикладного сервісу Nextcloud, Docker, Nginx та HTTPS-доступу до корпоративного сховища
Database-Server	серверна ферма	Розміщення СУБД MariaDB для зберігання даних прикладного сервісу Nextcloud
Backup-Server	серверна ферма	Централізоване зберігання резервних копій даних, конфігурацій і службових файлів
Icinga2-Master-Server	сегмент моніторингу	Централізований моніторинг серверів, мережевого обладнання, граничного маршрутизатора та прикладних сервісів

Таблиця А.1 — Основні компоненти ІТ-інфраструктури та їх призначення

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				114
Змн.	Арк.	№ докум.	Підпис	Дата		

Компонент ІТ-інфраструктури	Основні залежності	Призначення залежності
Клієнтські робочі станції	Windows Server 2022, Cisco Core L3 Switch	Отримання мережевих параметрів, доменна автентифікація користувачів і доступ до внутрішніх сервісів організації
Windows Server 2022	Cisco Core L3 Switch, серверна ферма	Забезпечення роботи Active Directory, DNS і DHCP для користувачів та комп'ютерів домену
Linux-App-Server	Database-Server, Windows Server 2022, Cisco Core L3 Switch	Функціонування прикладного сервісу Nextcloud, доступ до бази даних і коректне розв'язання внутрішніх доменних імен
Database-Server	Linux-App-Server, серверна ферма	Зберігання даних корпоративного хмарного сховища та забезпечення роботи прикладного сервісу
Backup-Server	серверні вузли інфраструктури	Централізоване збереження резервних копій даних, конфігурацій і службових файлів
pfSense-Edge-Router	Cisco Core L3 Switch, зовнішня мережа	Забезпечення виходу корпоративної мережі до зовнішніх ресурсів, NAT і базовий захист периметра
Cisco Core L3 Switch	pfSense, комутатори доступу, серверні та клієнтські вузли	Центральна маршрутизація всередині інфраструктури та передача трафіку між основними частинами мережі
Комутатори доступу	Cisco Core L3 Switch, кінцеві пристрої	Підключення клієнтських, адміністративних і серверних вузлів до корпоративної мережі
Icinga2-Master-Server	сервери, мережеве обладнання, pfSense	Централізований контроль доступності, стану служб, ресурсів серверів і мережевого обладнання
Адміністративна станція	сервери, мережеве обладнання, система моніторингу	Централізоване адміністрування ІТ-інфраструктури, перевірка працездатності сервісів і керування конфігураціями

Таблиця А.2 — Основні залежності між компонентами ІТ-інфраструктури

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		115

VLAN-сегментація, адресація та прив'язка комутаторів доступу

VLAN	Назва сегмента	Призначення	Підмережа (CIDR)	Шлюз VLAN / SVI на Core-L3-Switch	DHCP / адресація
10	Management	Робочі станції керівництва / management-сегмент	192.168.10.0/24	192.168.10.254	DHCP через Windows Server 2022
20	Accounting	Робочі станції бухгалтерії	192.168.20.0/24	192.168.20.254	DHCP через Windows Server 2022
30	HR	Робочі станції відділу кадрів	192.168.30.0/24	192.168.30.254	DHCP через Windows Server 2022
40	IT_Dept	Адміністративна станція та доступ адміністратора	192.168.40.0/24	192.168.40.254	Статична адресація
50	Servers	Серверний сегмент	192.168.50.0/24	192.168.50.254	Статична адресація
60	Monitoring	Сегмент системи моніторингу	192.168.60.0/24	192.168.60.254	Статична адресація
99	Transit	Транзит між Core-L3-Switch і pfSense	192.168.1.0/24	192.168.1.2 на Core; 192.168.1.1 на pfSense	Статична адресація
100	Net_Mgmt	Керування мережевими обладнаннями	192.168.100.0/24	192.168.100.254	Статична адресація

Таблиця Б.1 — VLAN-сегментація та шлюзи підмереж

Пристрій / віртуальна машина	Інтерфейс / мережний адаптер	ІР-адреса	Маска підмережі	Префікс	Підмережа (CIDR)	ІР-адреса шлюзу (Gateway)
pfSense-Edge-Router	WAN	DHCP	DHCP	DHCP	зовнішня мережа	DHCP
pfSense-Edge-Router	LAN / Transit	192.168.1.1	255.255.255.0	/24	192.168.1.0/24	сам є шлюзом
Core-L3-Switch	SVI Vlan99 / Transit	192.168.1.2	255.255.255.0	/24	192.168.1.0/24	192.168.1.1
Win10-Management-1 / WS-MGMT-01	мережний адаптер користувачк ої станції	DHCP	255.255.255.0	/24	192.168.10.0/24	192.168.10.254
Win10-Accounting-1-1 / WS-ACC-01	мережний адаптер користувачк ої станції	DHCP	255.255.255.0	/24	192.168.20.0/24	192.168.20.254
Win10-Accounting-2-1 / WS-ACC-02	мережний адаптер користувачк ої станції	DHCP	255.255.255.0	/24	192.168.20.0/24	192.168.20.254
Win10-HR-1-1 / WS-HR-01	мережний адаптер користувачк ої станції	DHCP	255.255.255.0	/24	192.168.30.0/24	192.168.30.254
Win10-HR-2-1 / WS-HR-02	мережний адаптер користувачк ої станції	DHCP	255.255.255.0	/24	192.168.30.0/24	192.168.30.254
Admin-Workstation-1 / WS-IT-01	мережний адаптер адміністративної станції	192.168.40.10	255.255.255.0	/24	192.168.40.0/24	192.168.40.254
Windows Server 2022	мережний адаптер сервера AD/DNS/DHCP	192.168.50.10	255.255.255.0	/24	192.168.50.0/24	192.168.50.254
Linux-App-Server	enp0s3	192.168.50.20	255.255.255.0	/24	192.168.50.0/24	192.168.50.254
Database-Server	enp0s3	192.168.50.30	255.255.255.0	/24	192.168.50.0/24	192.168.50.254
Backup-Server	enp0s3	192.168.50.40	255.255.255.0	/24	192.168.50.0/24	192.168.50.254

Таблиця Б.2 — Адресація основних вузлів ІТ-інфраструктури

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		117

Пристрій / віртуальна машина	Інтерфейс / мережний адаптер	ІР-адреса	Маска підмережі	Префікс	Підмережа (CIDR)	ІР-адреса шлюзу (Gateway)
Icinga2-Master-Server	мережний адаптер сервера моніторингу	192.168.60.10	255.255.255.0	/24	192.168.60.0/24	192.168.60.254
Core-L3-Switch	SVI Vlan100 / інтерфейс керування	192.168.100.254	255.255.255.0	/24	192.168.100.0/24	сам є шлюзом VLAN 100
SW-Servers	SVI Vlan100 / інтерфейс керування	192.168.100.10	255.255.255.0	/24	192.168.100.0/24	192.168.100.254
SW-Acc-01	SVI Vlan100 / інтерфейс керування	192.168.100.11	255.255.255.0	/24	192.168.100.0/24	192.168.100.254
SW-HR-01	SVI Vlan100 / інтерфейс керування	192.168.100.12	255.255.255.0	/24	192.168.100.0/24	192.168.100.254
SW-Mgmt-01	SVI Vlan100 / інтерфейс керування	192.168.100.13	255.255.255.0	/24	192.168.100.0/24	192.168.100.254
SW-IT-01	SVI Vlan100 / інтерфейс керування	192.168.100.14	255.255.255.0	/24	192.168.100.0/24	192.168.100.254

Таблиця Б.2 — Продовження. Адресація основних вузлів ІТ-інфраструктури

Комутатор доступу	Management IP	Trunk-порт до Core-L3- Switch	Порт на Core-L3- Switch	Користувачькі / службові VLAN	Access-порти
SW-Servers	192.168.100.10	Ethernet0/0	Ethernet1/1	VLAN 50 Servers; VLAN 60 Monitoring	VLAN 50: Ethernet0/1, Ethernet0/2, Ethernet0/3, Ethernet1/0; VLAN 60: Ethernet1/1
SW-Acc-01	192.168.100.11	Ethernet0/0	Ethernet0/1	VLAN 20 Accounting	Ethernet0/1, Ethernet0/2
SW-HR-01	192.168.100.12	Ethernet0/0	Ethernet0/3	VLAN 30 HR	Ethernet0/1, Ethernet0/2
SW-Mgmt- 01	192.168.100.13	Ethernet0/0	Ethernet1/0	VLAN 10 Management	Ethernet0/1
SW-IT-01	192.168.100.14	Ethernet0/0	Ethernet0/2	VLAN 40 IT_Dept	Ethernet0/1

Таблиця Б.3 — прив'язка комутаторів доступу до VLAN і trunk-з'єднань.

Налаштування pfSense та Cisco Core L3 Switch

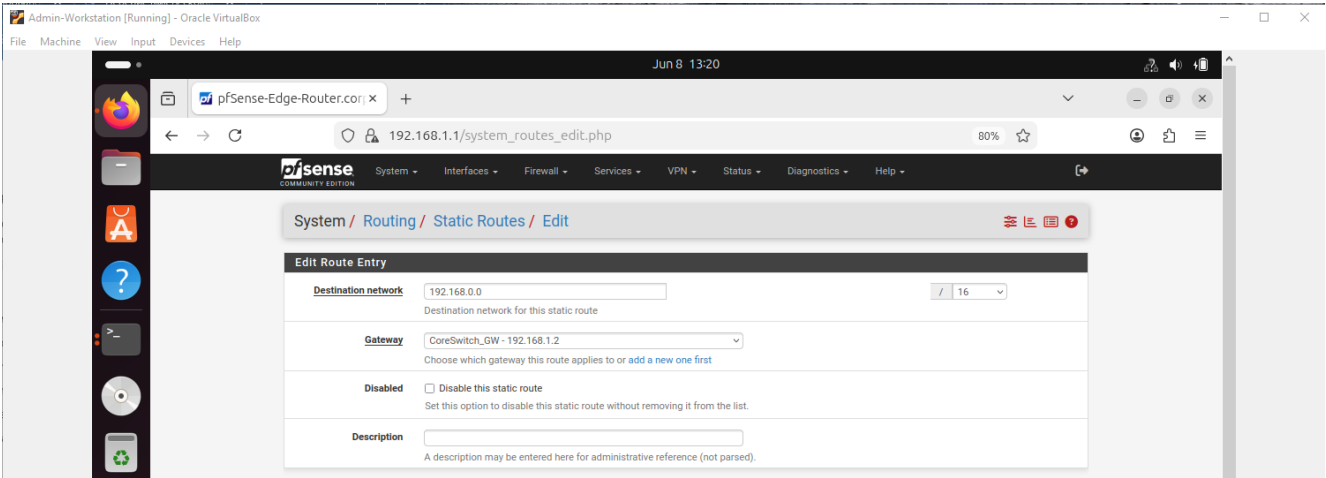


Рисунок В.1 — Налаштування шлюзу CoreSwitch_GW на pfSense

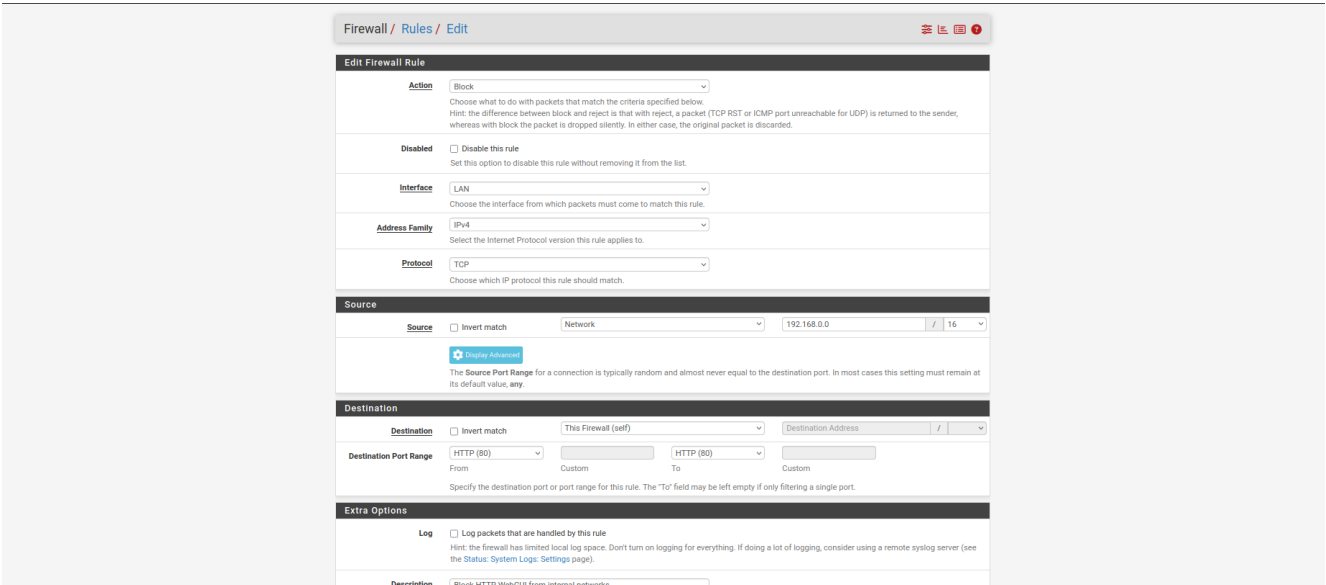


Рисунок В.2 — Додавання статичного маршруту 192.168.0.0/16 на pfSense

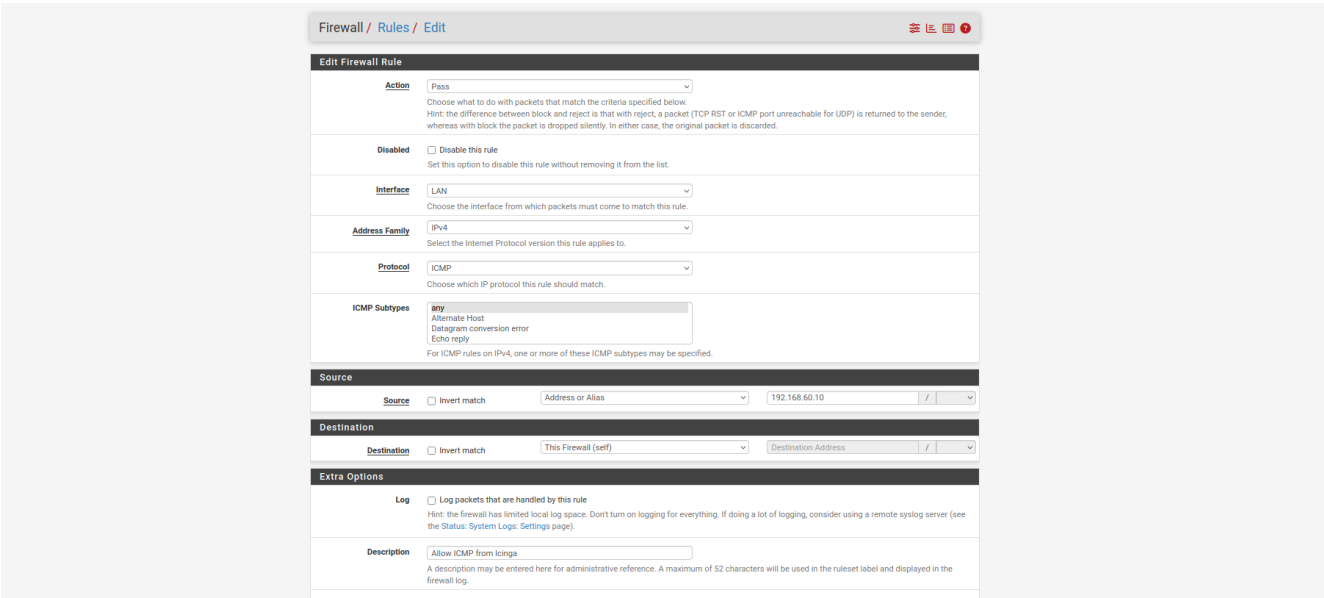


Рисунок В.3 — Блокування HTTP-доступу до WebGUI pfSense

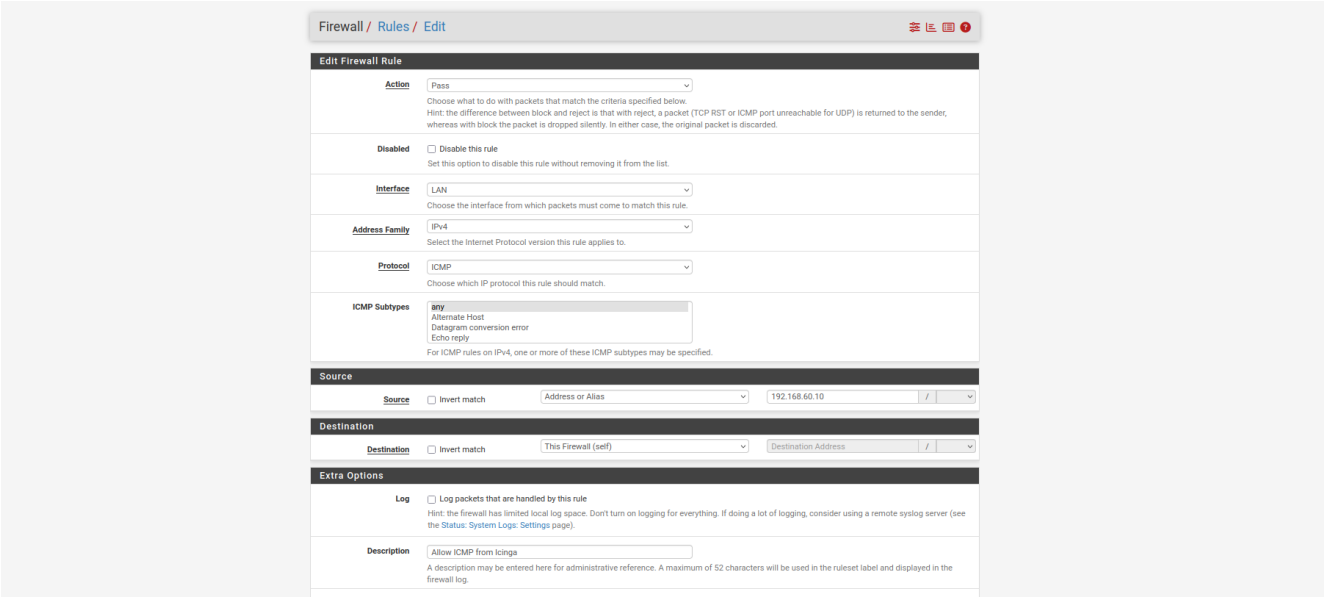


Рисунок В.4 — Дозвіл ICMP від Icinga2-Master-Server до pfSense

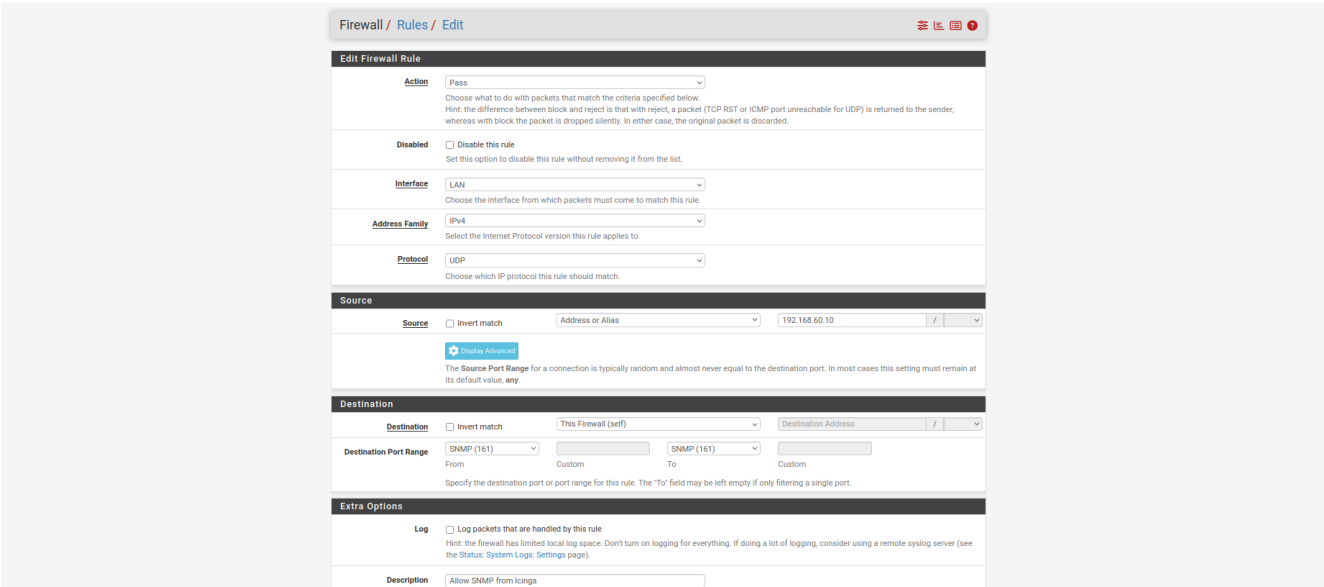


Рисунок В.5 — Дозвіл SNMP від Icinga2-Master-Server до pfSense

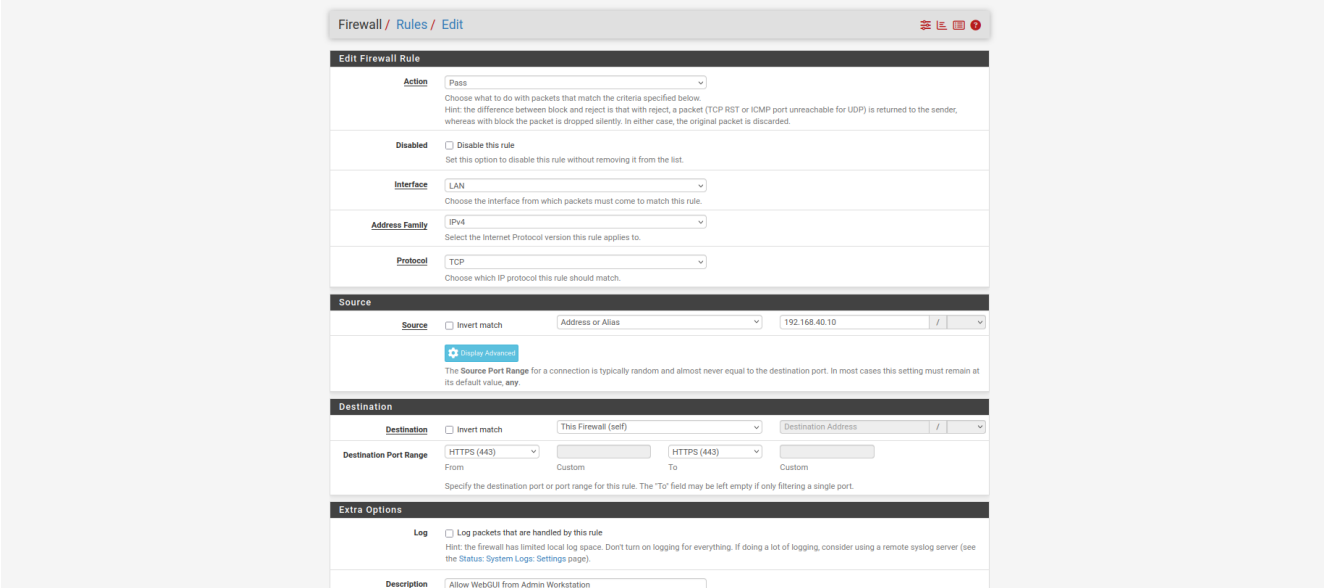


Рисунок В.6 — Доступ до WebGUI pfSense з адміністративної станції

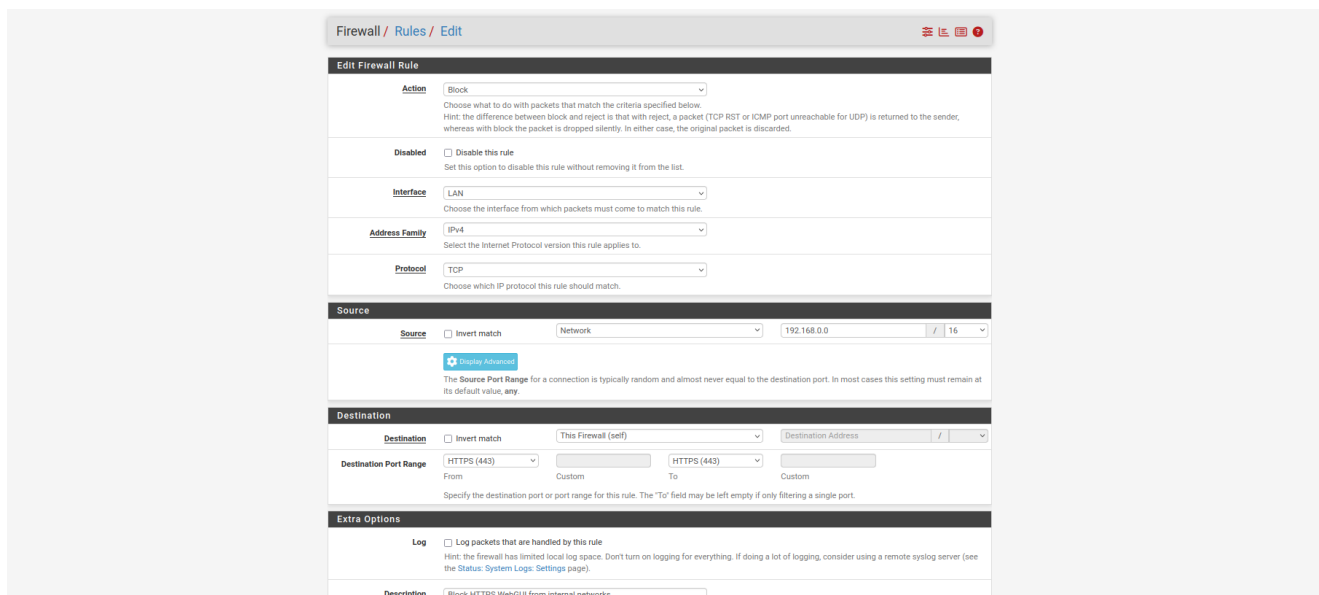


Рисунок В.7 — Блокування HTTPS-доступу до WebGUI pfSense

```
Core-L3-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-L3-Switch(config)#vlan 10
Core-L3-Switch(config-vlan)#name Management
Core-L3-Switch(config-vlan)#vlan 20
Core-L3-Switch(config-vlan)# name Accounting
Core-L3-Switch(config-vlan)#vlan 30
Core-L3-Switch(config-vlan)# name HR
Core-L3-Switch(config-vlan)#vlan 40
Core-L3-Switch(config-vlan)# name IT_Dept
Core-L3-Switch(config-vlan)#vlan 50
Core-L3-Switch(config-vlan)# name Servers
Core-L3-Switch(config-vlan)#vlan 60
Core-L3-Switch(config-vlan)# name Monitoring
Core-L3-Switch(config-vlan)#exit
Core-L3-Switch(config)#interface Vlan 10
Core-L3-Switch(config-if)#
*Jun 1 02:59:43.109: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, ch
anged state to down
Core-L3-Switch(config-if)#ip address 192.168.10.254 255.255.255.0
Core-L3-Switch(config-if)#no shutdown
Core-L3-Switch(config-if)#interface Vlan 20
Core-L3-Switch(config-if)#
*Jun 1 02:59:52.740: %LINK-3-UPDOWN: Interface Vlan10, changed state to down
Core-L3-Switch(config-if)#
*Jun 1 02:59:55.153: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, ch
anged state to down
Core-L3-Switch(config-if)#ip address 192.168.20.254 255.255.255.0
Core-L3-Switch(config-if)#no shutdown
Core-L3-Switch(config-if)#interface Vlan 30
Core-L3-Switch(config-if)#
*Jun 1 03:00:02.891: %LINK-3-UPDOWN: Interface Vlan20, changed state to down
Core-L3-Switch(config-if)#ip address 192.168.30.254 255.255.255.0
*Jun 1 03:00:04.837: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, ch
anged state to down
Core-L3-Switch(config-if)#ip address 192.168.30.254 255.255.255.0
Core-L3-Switch(config-if)#no shutdown
Core-L3-Switch(config-if)#interface Vlan 40
Core-L3-Switch(config-if)#
*Jun 1 03:00:12.075: %LINK-3-UPDOWN: Interface Vlan30, changed state to down
Core-L3-Switch(config-if)#ip address 192.168.40.254 255.255.255.0
*Jun 1 03:00:14.240: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, ch
anged state to down
Core-L3-Switch(config-if)#ip address 192.168.40.254 255.255.255.0
Core-L3-Switch(config-if)#no shutdown
Core-L3-Switch(config-if)#interface Vlan 50
Core-L3-Switch(config-if)#
*Jun 1 03:00:20.878: %LINK-3-UPDOWN: Interface Vlan40, changed state to down
Core-L3-Switch(config-if)#ip address 192.168.50.254 255.255.255.0
*Jun 1 03:00:23.037: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, ch
anged state to down
Core-L3-Switch(config-if)#ip address 192.168.50.254 255.255.255.0
Core-L3-Switch(config-if)#no shutdown
Core-L3-Switch(config-if)#interface Vlan 60
Core-L3-Switch(config-if)#
*Jun 1 03:00:30.554: %LINK-3-UPDOWN: Interface Vlan50, changed state to down
Core-L3-Switch(config-if)#
*Jun 1 03:00:32.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, ch
anged state to down
Core-L3-Switch(config-if)#ip address 192.168.60.254 255.255.255.0
Core-L3-Switch(config-if)#no shutdown
Core-L3-Switch(config-if)#exit
Core-L3-Switch(config)#
```

Рисунок В.8 — Створення VLAN та SVI-інтерфейсів на Cisco Core L3 Switch

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				
Змн.	Арк.	№ докум.	Підпис	Дата		123

```

*Jun 1 03:00:39.696: %LINK-3-UPDOWN: Interface Vlan60, changed state to down
Core-L3-Switch(config)#interface range Ethernet 0/1 - 3, Ethernet 1/0 - 1
Core-L3-Switch(config-if-range)#switchport trunk encapsulation dot1q
Core-L3-Switch(config-if-range)#switchport mode trunk
Core-L3-Switch(config-if-range)#
*Jun 1 03:00:57.404: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
*Jun 1 03:00:57.404: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
2, changed state to down
*Jun 1 03:00:57.405: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
3, changed state to down
*Jun 1 03:00:57.405: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to down
*Jun 1 03:00:57.405: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
1, changed state to down
Core-L3-Switch(config-if-range)#no shutdown
Core-L3-Switch(config-if-range)#
*Jun 1 03:01:00.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to up
*Jun 1 03:01:00.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
2, changed state to up
*Jun 1 03:01:00.408: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
3, changed state to up
*Jun 1 03:01:00.408: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to up
*Jun 1 03:01:00.409: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
1, changed state to up
Core-L3-Switch(config-if-range)#exit
Core-L3-Switch(config)#
*Jun 1 03:01:31.413: %LINK-3-UPDOWN: Interface Vlan10, changed state to up
*Jun 1 03:01:31.414: %LINK-3-UPDOWN: Interface Vlan20, changed state to up
*Jun 1 03:01:31.414: %LINK-3-UPDOWN: Interface Vlan30, changed state to up
*Jun 1 03:01:31.414: %LINK-3-UPDOWN: Interface Vlan40, changed state to up
*Jun 1 03:01:31.414: %LINK-3-UPDOWN: Interface Vlan50, changed state to up
*Jun 1 03:01:31.414: %LINK-3-UPDOWN: Interface Vlan60, changed state to up
*Jun 1 03:01:32.413: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Core-L3-Switch(config)#
*Jun 1 03:01:32.421: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
*Jun 1 03:01:32.422: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
*Jun 1 03:01:32.422: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up
*Jun 1 03:01:32.422: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up
*Jun 1 03:01:32.422: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to up
Core-L3-Switch(config)#

```

Рисунок В.9 — Налаштування trunk-портів до комутаторів доступу

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				124
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевірка мережевої та доменної зв'язності

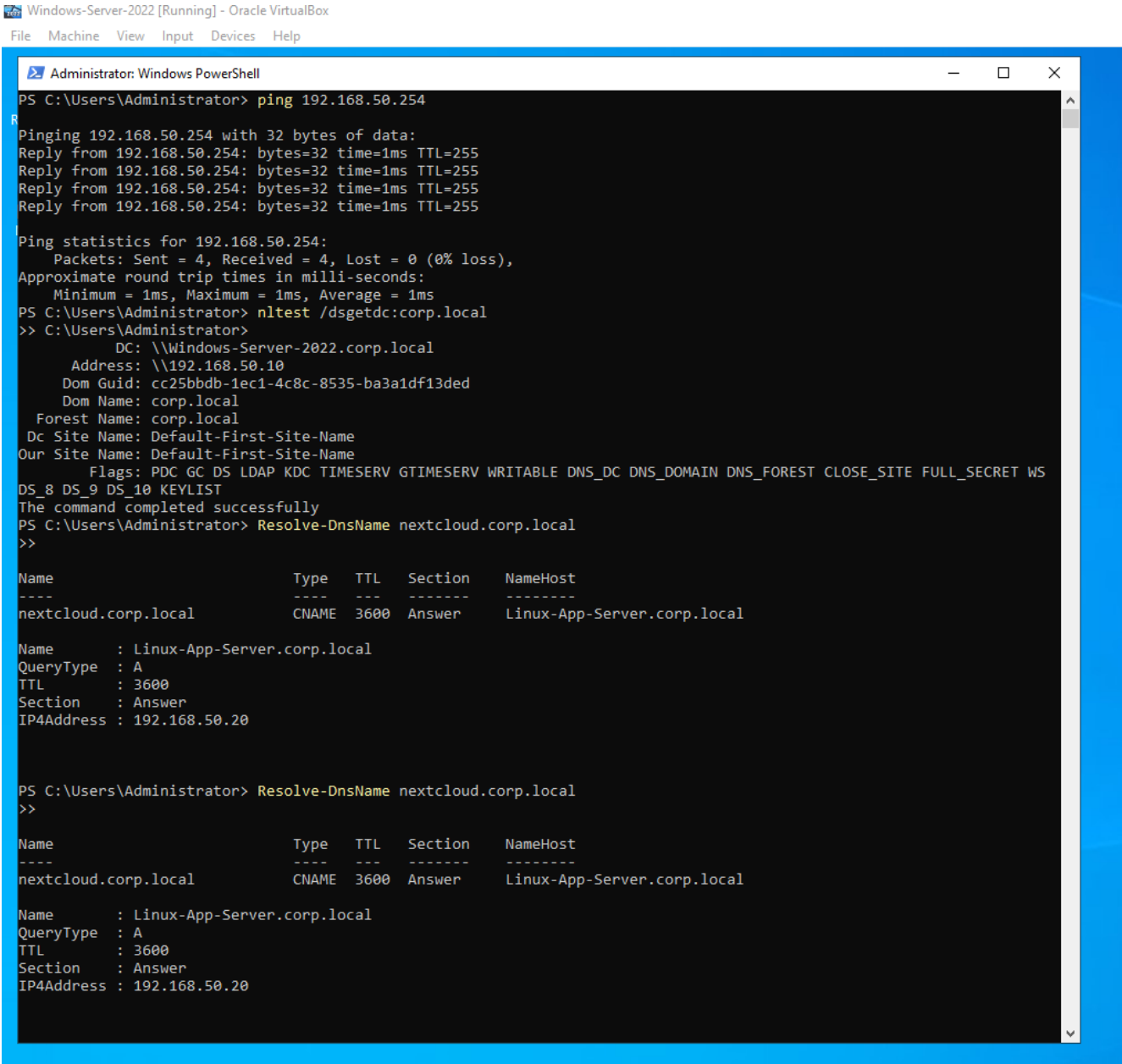


Рисунок Г.1 — Перевірка доступності шлюзу серверного сегмента, домену corp.local та DNS-записів внутрішніх сервісів.

Налаштування віддаленого адміністративного доступу

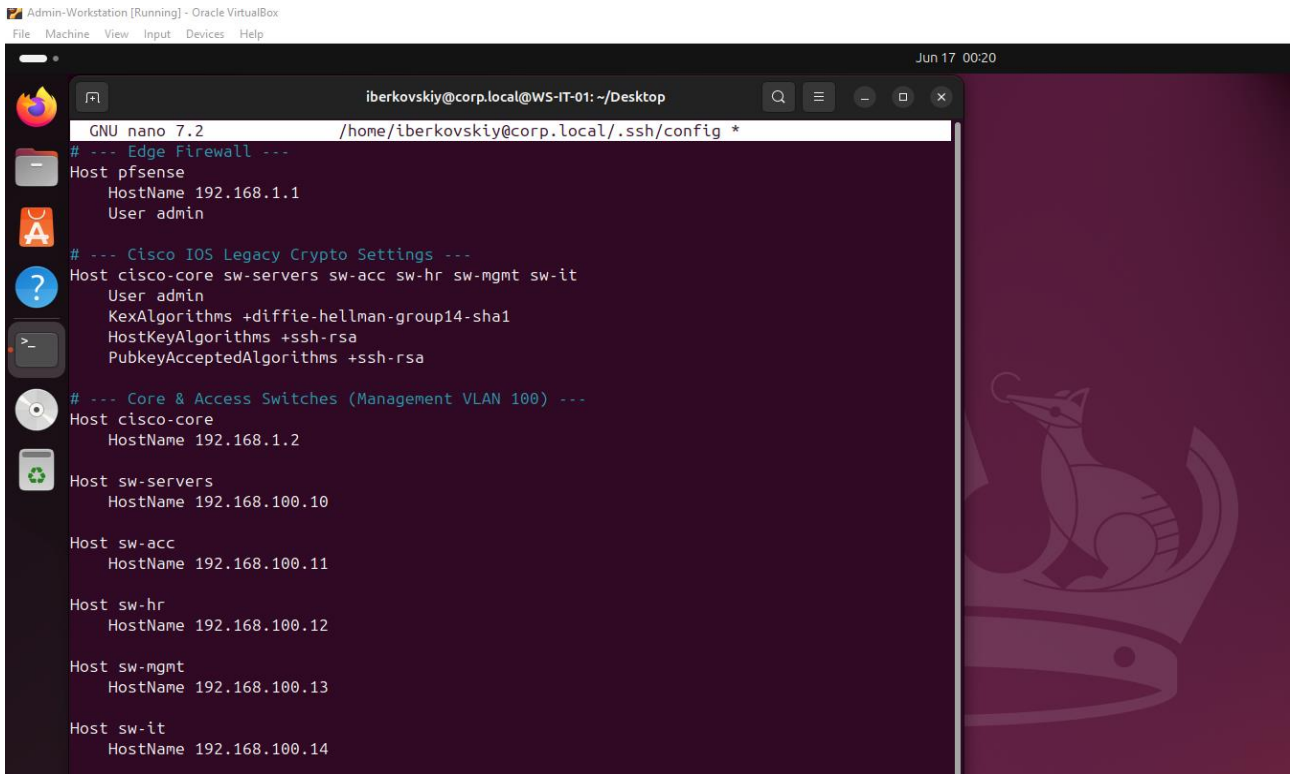


Рисунок Д.1 — Конфігураційний файл SSH-профілів на WS-IT-01 для pfSense та мережевого обладнання Cisco

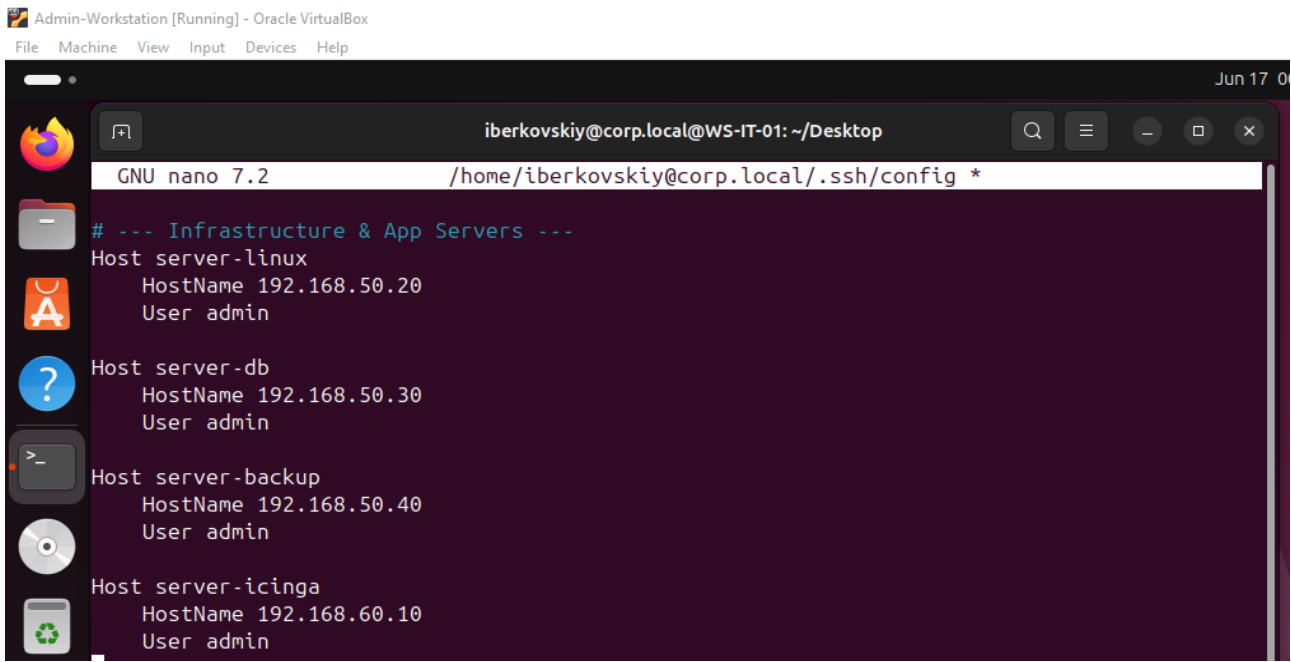


Рисунок Д.2 — Конфігураційний файл SSH-профілів на WS-IT-01 для інфраструктурних Linux-серверів

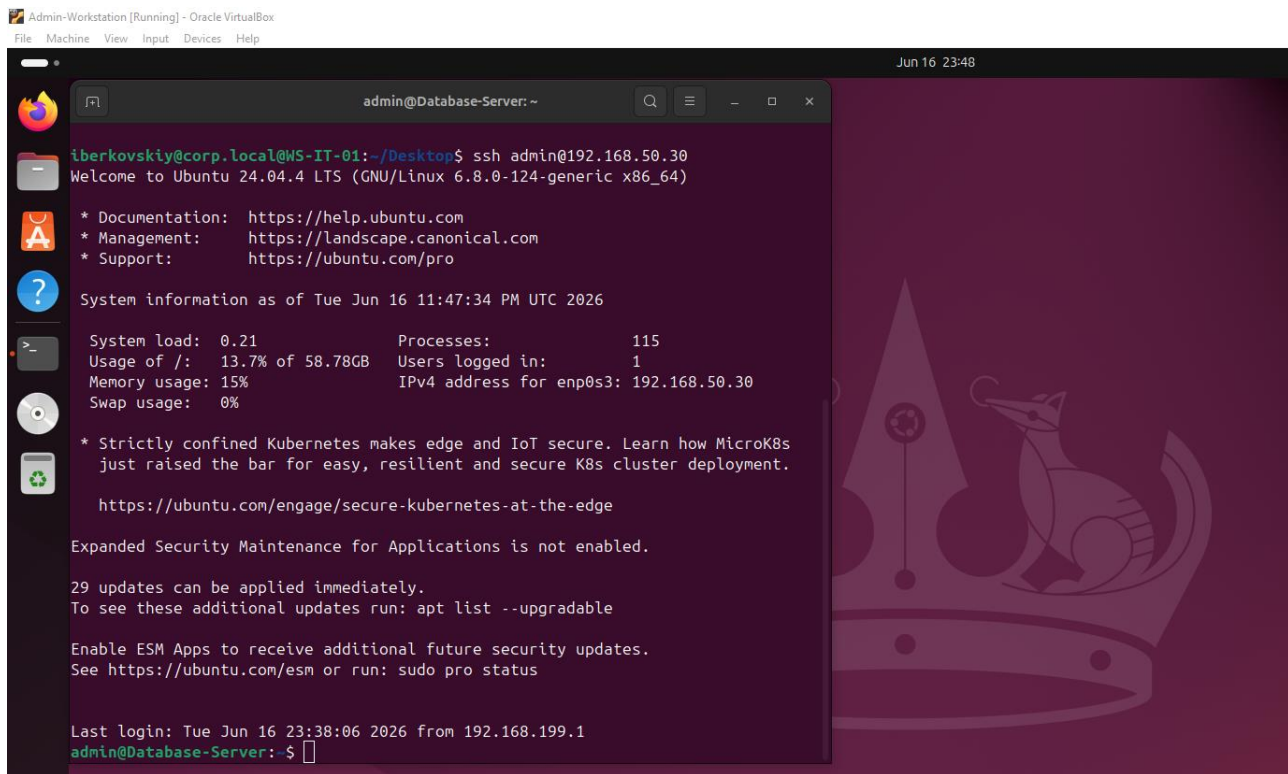


Рисунок Д.3 — Приклад перевірки SSH-доступу з адміністративної станції WS-IT-01 до Database-Server

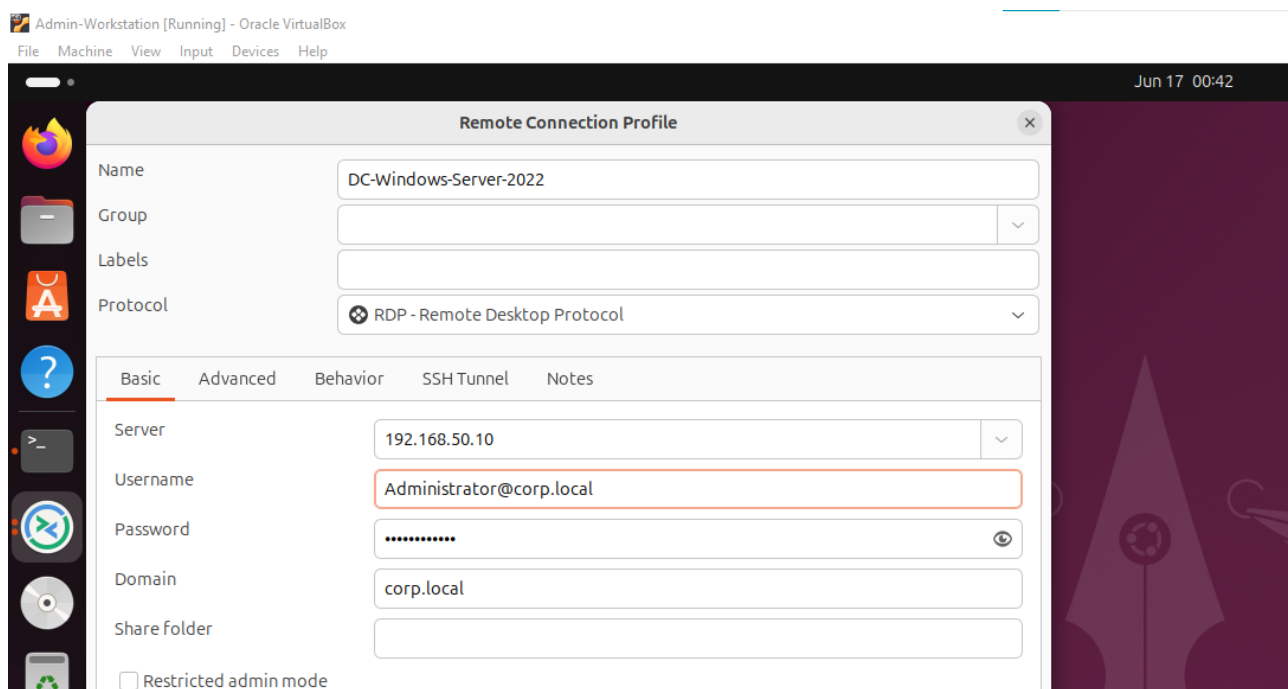


Рисунок Д.4 — Профіль RDP-підключення до Windows Server 2022 у Remmina на адміністративній станції WS-IT-01

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		127

Налаштування MariaDB на Database-Server

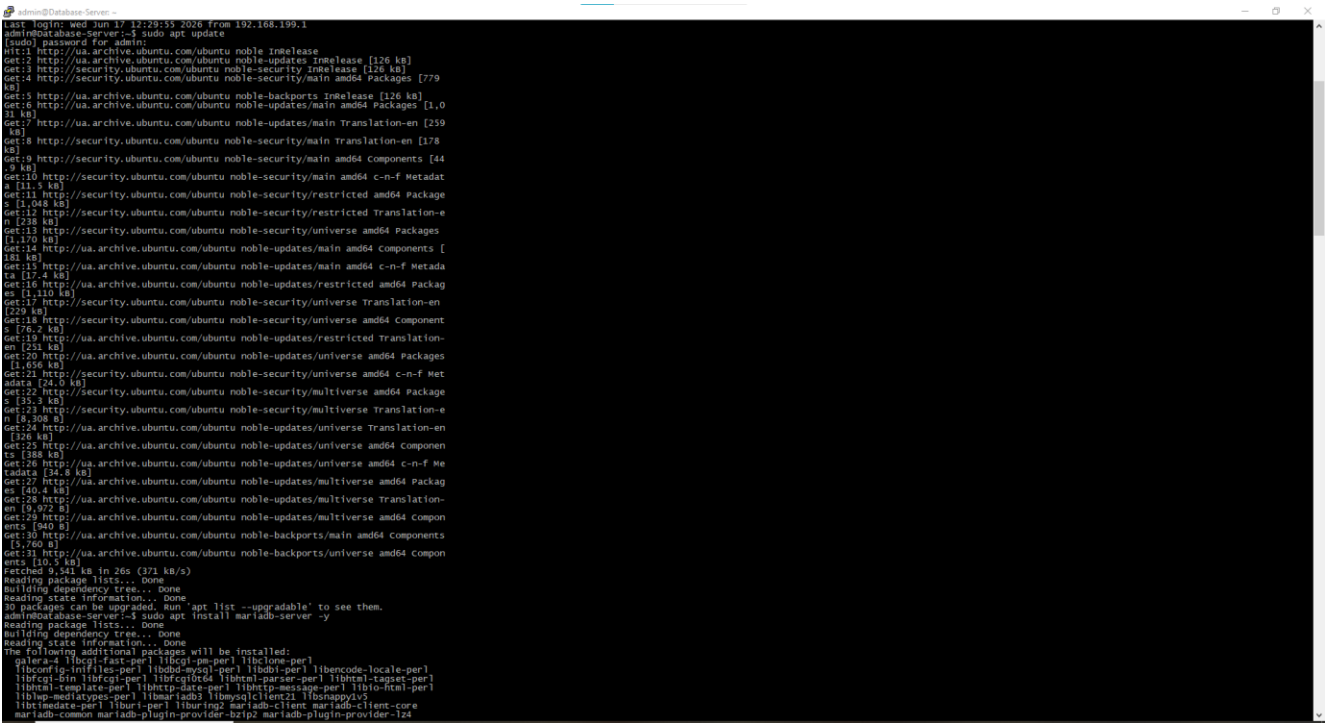


Рисунок Е.1 — Оновлення індексів пакетів на Database-Server перед встановленням MariaDB

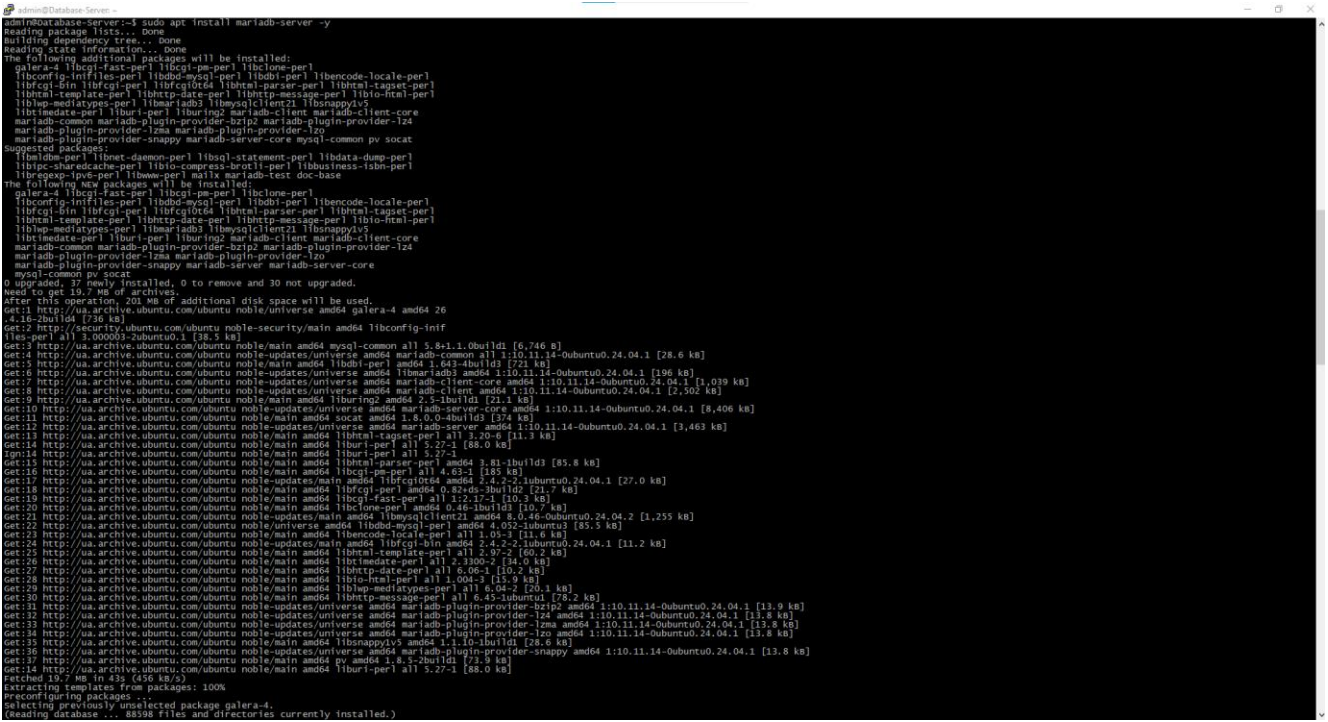


Рисунок Е.2 — Встановлення пакета MariaDB Server на Database-Server

	Берковський І.Ю.				Арк.
	Фальковський П.				
Змн.	Арк.	№ докум.	Підпис	Дата	128

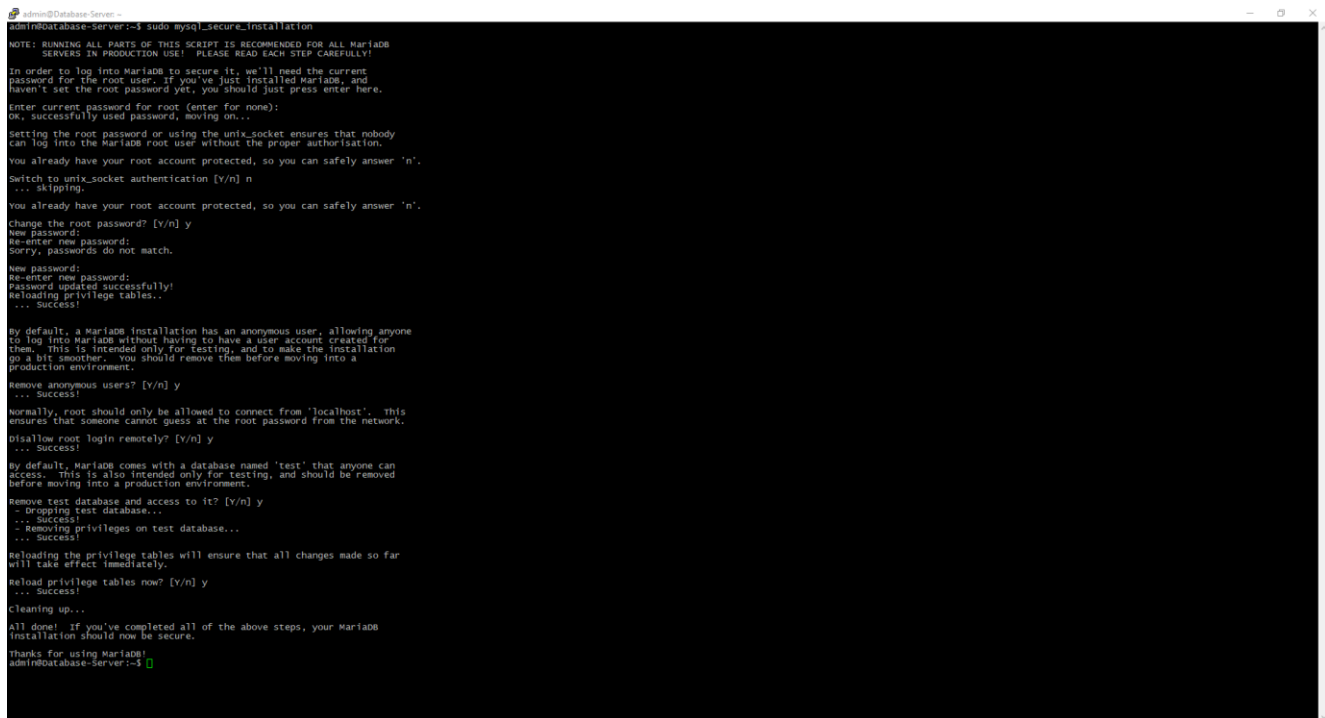


Рисунок Е.3 — Виконання базового гартування MariaDB за допомогою
mysql_secure_installation

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				129
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування Linux-App-Server, Docker, Nginx та Nextcloud

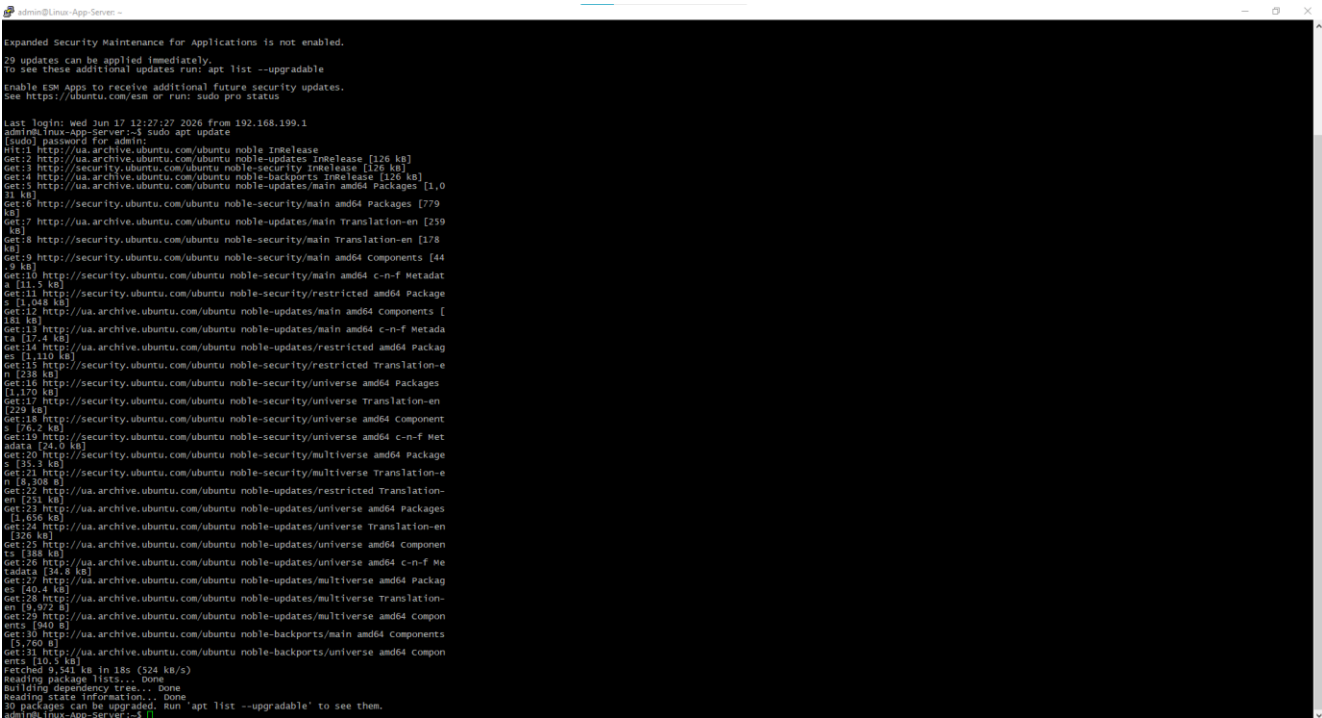


Рисунок Ж.1 — Оновлення індексів пакетів на Linux-App-Server перед встановленням компонентів прикладного середовища

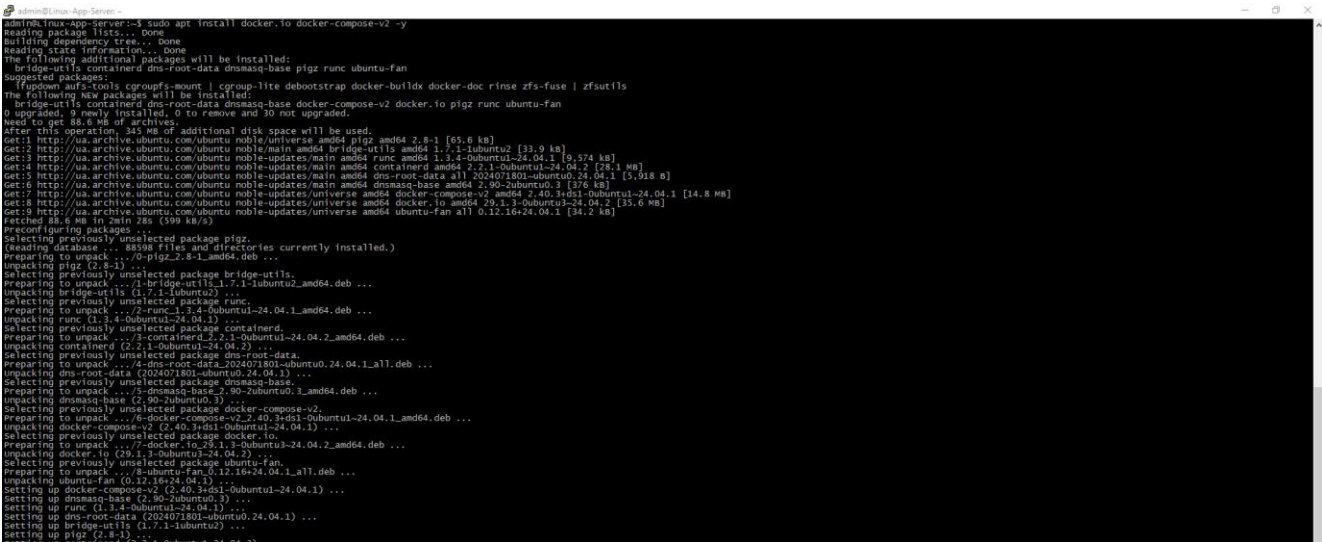


Рисунок Ж.2 — Встановлення Docker та Docker Compose на Linux-App-Server

```
admin@Linux-App-Server: ~/nextcloud
admin@Linux-App-Server:~/nextcloud$ sudo apt install nginx openssl -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl is already the newest version (3.0.13-0ubuntu3.11).
openssl set to manually installed.
Suggested packages:
  fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  nginx nginx-common
0 upgraded, 2 newly installed, 0 to remove and 30 not upgraded.
Need to get 568 kB of archives.
After this operation, 1,599 kB of additional disk space will be used.
Get:1 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx-common all 1.24.0-2ubuntu7.12 [44.5 kB]
Get:2 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx amd64 1.24.0-2ubuntu7.12 [524 kB]
Fetched 568 kB in 3s (202 kB/s)
Preconfiguring packages ...
Selecting previously unselected package nginx-common.
(Reading database ... 88977 files and directories currently installed.)
Preparing to unpack .../nginx-common_1.24.0-2ubuntu7.12_all.deb ...
Unpacking nginx-common (1.24.0-2ubuntu7.12) ...
Selecting previously unselected package nginx.
Preparing to unpack .../nginx_1.24.0-2ubuntu7.12_amd64.deb ...
Unpacking nginx (1.24.0-2ubuntu7.12) ...
Setting up nginx-common (1.24.0-2ubuntu7.12) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service -> /usr/lib/systemd/system/nginx.service.
Setting up nginx (1.24.0-2ubuntu7.12) ...
* upgrading binary nginx
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for ufw (0.36.2-6) ...
Scanning processes...
Scanning linux images...
[ OK ]
```

Рисунок Ж.3 — Встановлення Nginx та OpenSSL на Linux-App-Server

```
admin@Linux-App-Server: ~
admin@Linux-App-Server:~$ sudo docker exec --user www-data nextcloud_app php occ config:system:set trusted_domains 1 --value="nextcloud.corp.local"
[sudo] password for admin:
System config value trusted_domains => 1 set to string nextcloud.corp.local
admin@Linux-App-Server:~$
```

Рисунок Ж.4 — Додавання домену nextcloud.corp.local до списку trusted_domains у Nextcloud

```
admin@Linux-App-Server: ~/nextcloud
admin@Linux-App-Server:~/nextcloud$ sudo docker exec --user www-data nextcloud_app php occ config:system:set overwriteprotocol --value="https"
System config value overwriteprotocol set to string https
admin@Linux-App-Server:~/nextcloud$ sudo docker exec --user www-data nextcloud_app php occ config:system:set overwritehost --value="nextcloud.corp.local"
[sudo] password for admin:
System config value overwritehost set to string nextcloud.corp.local
admin@Linux-App-Server:~/nextcloud$ sudo docker exec --user www-data nextcloud_app php occ config:system:set overwrite.cli.url --value="https://nextcloud.corp.local"
System config value overwrite.cli.url set to string https://nextcloud.corp.local
admin@Linux-App-Server:~/nextcloud$
```

Рисунок Ж.5 — Налаштування параметрів overwritehost та overwrite.cli.url для Nextcloud

Налаштування системи резервного копіювання

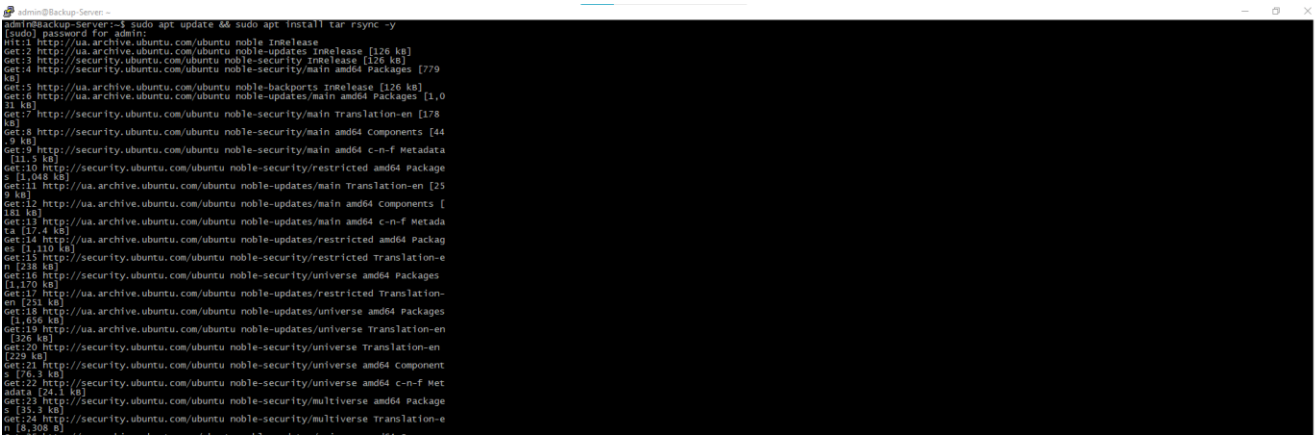


Рисунок К.1 — Встановлення tar та rsync на Backup-Server

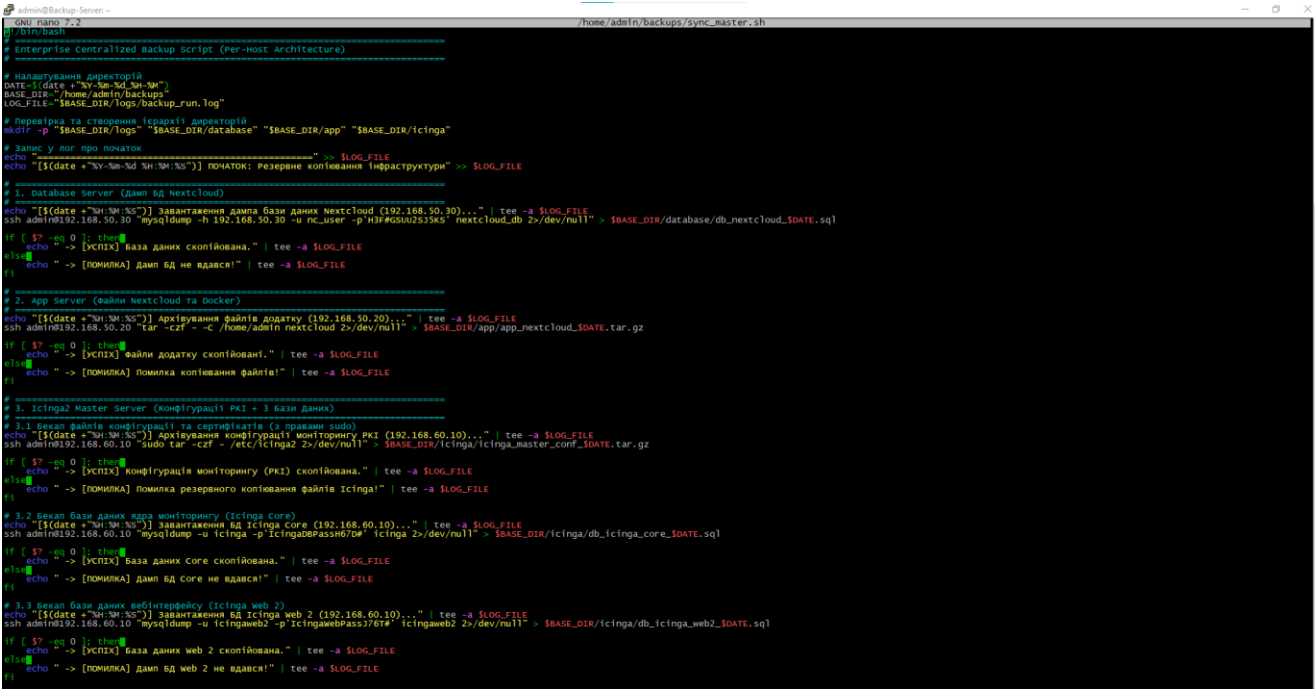


Рисунок К.2 — Скрипт централізованого резервного копіювання sync_master.sh, частина 1

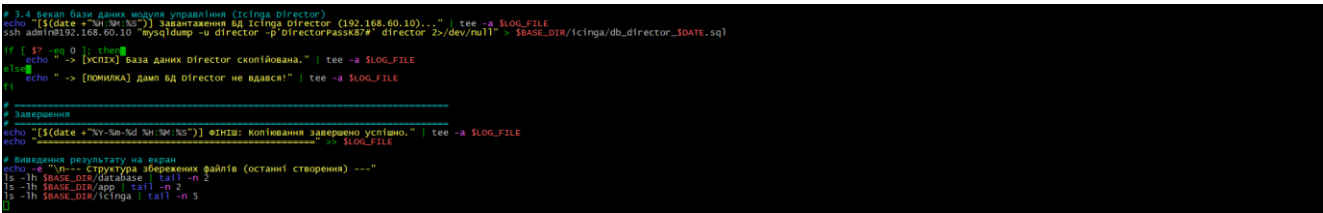


Рисунок К.3 — Скрипт централізованого резервного копіювання sync_master.sh, частина 2

```
admin@Database-Server:~$ sudo mysql -u root -p
[sudo] password for admin:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.14-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nc_user'@'192.168.5
0.40' IDENTIFIED BY 'H3F#GSUU2S35KS';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye
admin@Database-Server:~$
```

Рисунок К.4 — Налаштування локальних прав сервісного користувача nc_user у MariaDB, частина 1

```
admin@Database-Server:~$ sudo mysql -u root -p
Server version: 10.11.14-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nc_user'@'localhost' IDENTIFIED BY 'H3F#GSUU2S35KS';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nc_user'@'192.168.50.30' IDENTIFIED BY 'H3F#GSUU2S35KS';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nc_user'@'Database-Server' IDENTIFIED BY 'H3F#GSUU2S35KS';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT;
Bye
admin@Database-Server:~$
```

Рисунок К.5 — Налаштування локальних прав сервісного користувача nc_user у MariaDB, частина 2

```
admin@Backup-Server:~$ crontab -e
no crontab for admin - using an empty one
crontab: installing new crontab
admin@Backup-Server:~$ crontab -l | tail -n 2
0 20 * * * /bin/bash /home/admin/backups/sync_master.sh

admin@Backup-Server:~$
```

Рисунок К.6 — Налаштування розкладу запуску sync_master.sh у crontab

Налаштування групових політик Active Directory

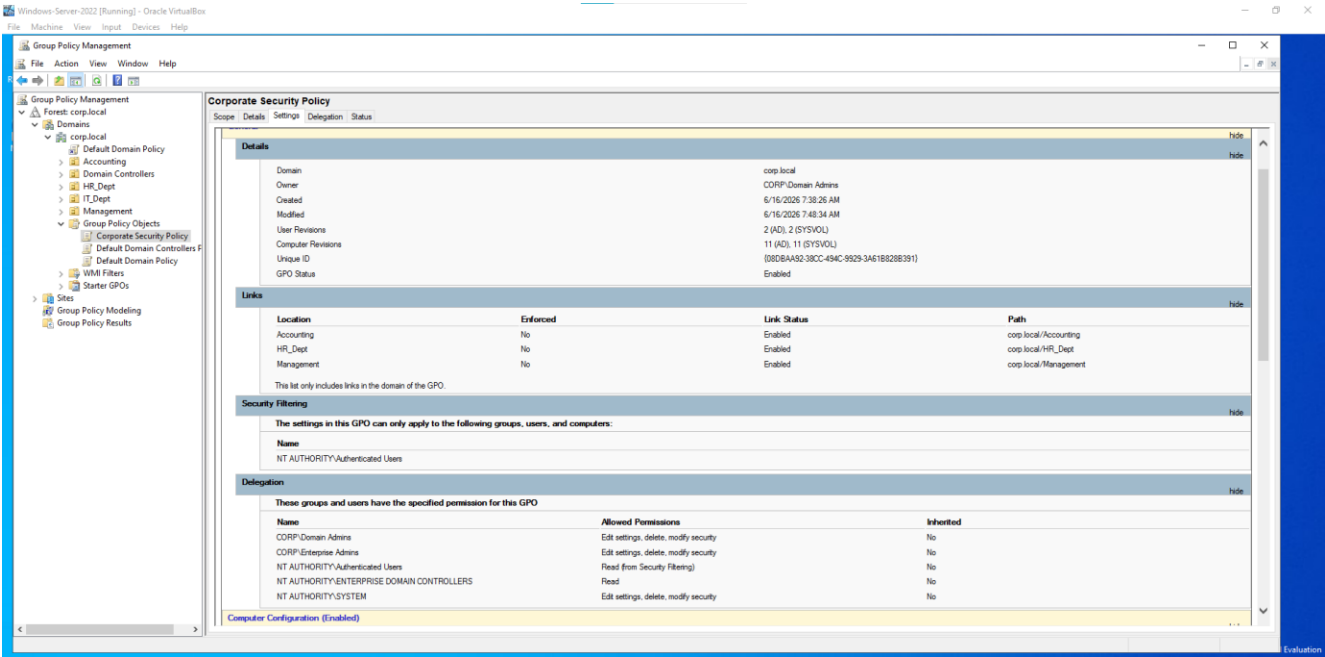


Рисунок Л.1 — Загальні відомості та прив’язки групової політики Corporate Security Policy

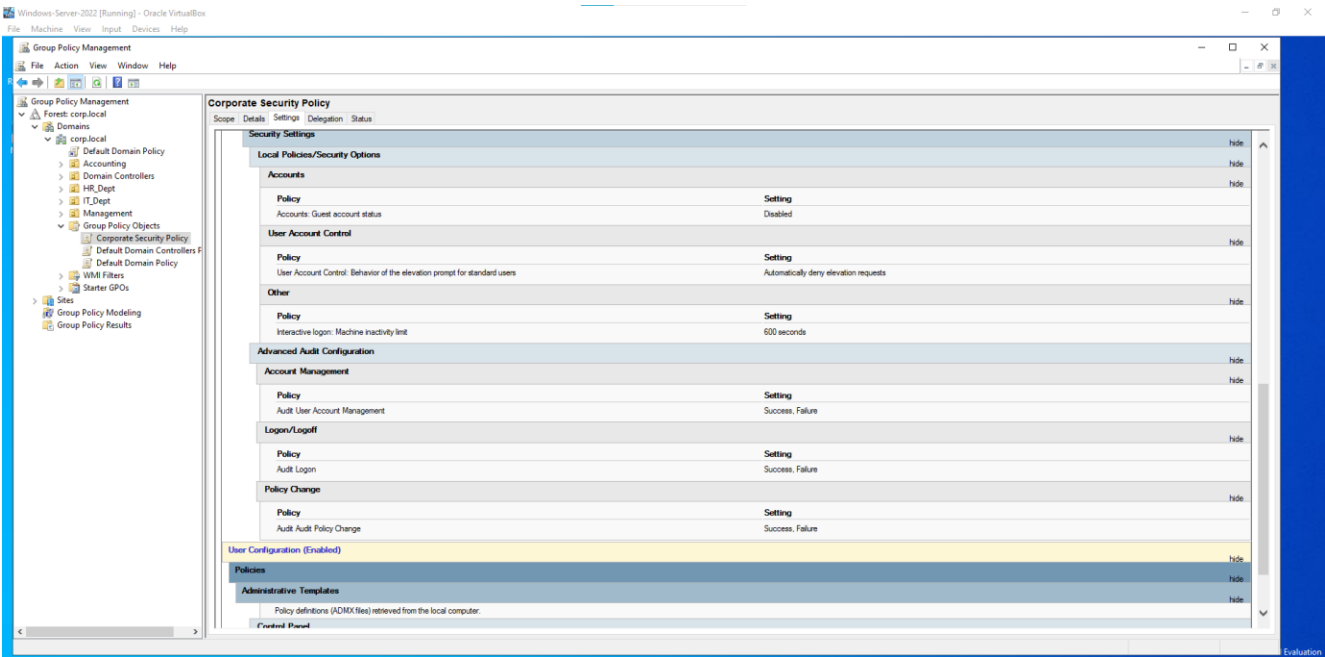


Рисунок Л.2 — Основні параметри безпеки групової політики Corporate Security Policy

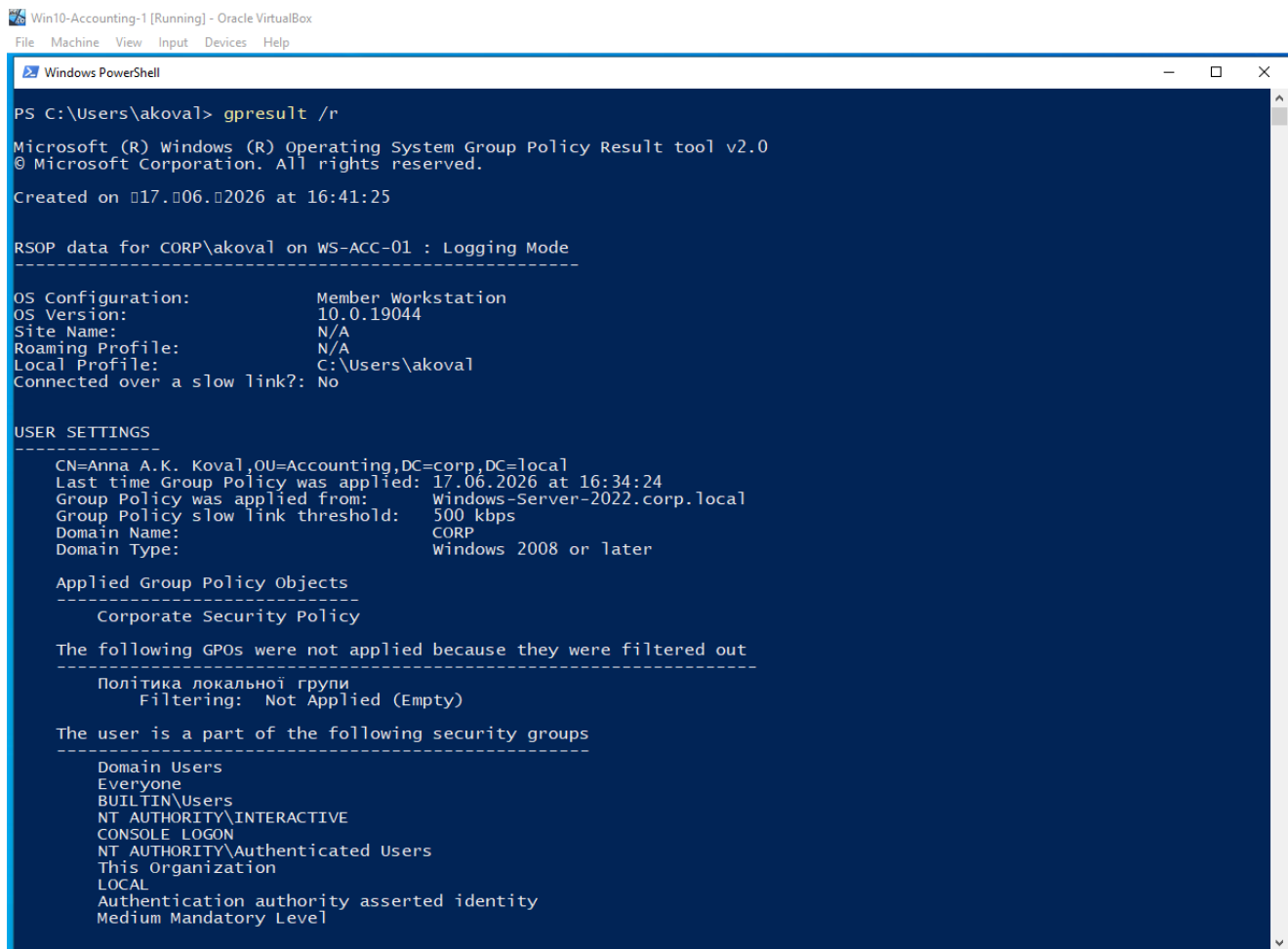


Рисунок Л.3 — Перевірка застосування Corporate Security Policy на робочій станції WS-ACC-01

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				135
Змн.	Арк.	№ докум.	Підпис	Дата		

Розгортання Icinga 2, Icinga Web 2 та Icinga Director

```
admin@icinga2-Master-Server:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for admin:
Hit:1 http://ua.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ua.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ua.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [2,067 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1,763 kB]
Get:7 http://ua.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [363 kB]
Get:8 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 components [181 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [275 kB]
Get:10 http://ua.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [17.4 kB]
Get:11 http://ua.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,698 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/main amd64 components [44.8 kB]
Get:13 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [11.5 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [1,195 kB]
Get:15 http://ua.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [331 kB]
Get:16 http://ua.archive.ubuntu.com/ubuntu noble-updates/universe amd64 components [388 kB]
Get:17 http://ua.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [34.6 kB]
Get:18 http://ua.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 components [940 B]
Get:19 http://ua.archive.ubuntu.com/ubuntu noble-backports/main amd64 components [5,772 B]
Get:20 http://security.ubuntu.com/ubuntu noble-security/universe amd64 components [76.2 kB]
Get:21 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [23.2 kB]
Get:22 http://ua.archive.ubuntu.com/ubuntu noble-backports/universe amd64 components [10.5 kB]
Fetched 8,864 kB in 15s (572 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
28 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
calculating upgrade... Done
```

Рисунок М.1 — Оновлення системних пакетів на Icinga2-Master-Server

```
admin@icinga2-Master-Server:~$ sudo apt install icinga2-ido-mysql -y
[sudo] password for admin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  dbconfig-common
Suggested packages:
  dbconfig-mysql | dbconfig-pgsql | dbconfig-sqlite3 | dbconfig-no-thanks
The following NEW packages will be installed:
  dbconfig-common icinga2-ido-mysql
0 upgraded, 2 newly installed, 0 to remove and 3 not upgraded.
Need to get 616 kB of archives.
After this operation, 1.81 kB of additional disk space will be used.
Get:1 http://ua.archive.ubuntu.com/ubuntu noble/universe amd64 dbconfig-common all 2.0.24 [596 kB]
Get:2 http://ua.archive.ubuntu.com/ubuntu noble/universe amd64 icinga2-ido-mysql amd64 2.14.2-1build2 [19.7 kB]
Fetched 616 kB in 2s (310 kB/s)
Preconfiguring packages...
Selecting previously unselected package dbconfig-common.
(Reading database ... 9090 files and directories currently installed.)
Preparing to unpack .../dbconfig-common_2.0.24_all.deb ...
Unpacking dbconfig-common (2.0.24) ...
Selecting previously unselected package icinga2-ido-mysql.
Preparing to unpack .../icinga2-ido-mysql_2.14.2-1build2_amd64.deb ...
Unpacking icinga2-ido-mysql (2.14.2-1build2) ...
Setting up dbconfig-common (2.0.24) ...
Creating config file /etc/dbconfig-common/config with new version
Setting up icinga2-ido-mysql (2.14.2-1build2) ...
dbconfig-common: writing config to /etc/dbconfig-common/icinga2-ido-mysql.conf
Creating config file /etc/dbconfig-common/icinga2-ido-mysql.conf with new version
Creating config file /etc/icinga2/features-available/ido-mysql.conf with new version
dbconfig-common: Flushing administrative password
Processing triggers for man-db (2.12.0-1build2) ...
```

Рисунок М.2 — Встановлення компонента IDO MySQL для Icinga 2

```
admin@icinga2-Master-Server:~$ sudo mysql -u root icinga < /usr/share/icinga2-ido-mysql/schema/mysql.sql
admin@icinga2-Master-Server:~$
```

Рисунок М.3 — Імпорт схеми бази даних IDO MySQL

```
admin@icinga2-Master-Server:~$ nano /etc/icinga2/features-available/ido-mysql.conf
GNU nano 7.2 /etc/icinga2/features-available/ido-mysql.conf
/*
 * The db_ido_mysql library implements IDO functionality
 * for MySQL.
 */

library "db_ido_mysql"

object IdomysqlConnection "ido-mysql" {
    user = "icinga",
    password = "icingaDBPassH67D#",
    host = "localhost",
    database = "icinga"
}
```

Рисунок М.4 — Конфігураційний файл ido-mysql.conf для підключення Icinga 2 до MariaDB

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				136
Змн.	Арк.	№ докум.	Підпис	Дата		

```
admin@icinga2-Master-Server: ~  
admin@icinga2-Master-Server:~$ sudo icinga2 feature enable ido-mysql  
Enabling feature ido-mysql. Make sure to restart Icinga 2 for these changes to take effect.  
admin@icinga2-Master-Server:~$ sudo systemctl restart icinga2  
admin@icinga2-Master-Server:~$
```

Рисунок М.5 — Увімкнення функції ido-mysql та перезапуск Icinga 2

```
admin@icinga2-Master-Server: ~  
admin@icinga2-Master-Server:~$ sudo icingacli setup token create  
The newly generated setup token is: f0eeb57611588626  
admin@icinga2-Master-Server:~$
```

Рисунок М.6 — Створення setup token для первинного налаштування Icinga Web 2

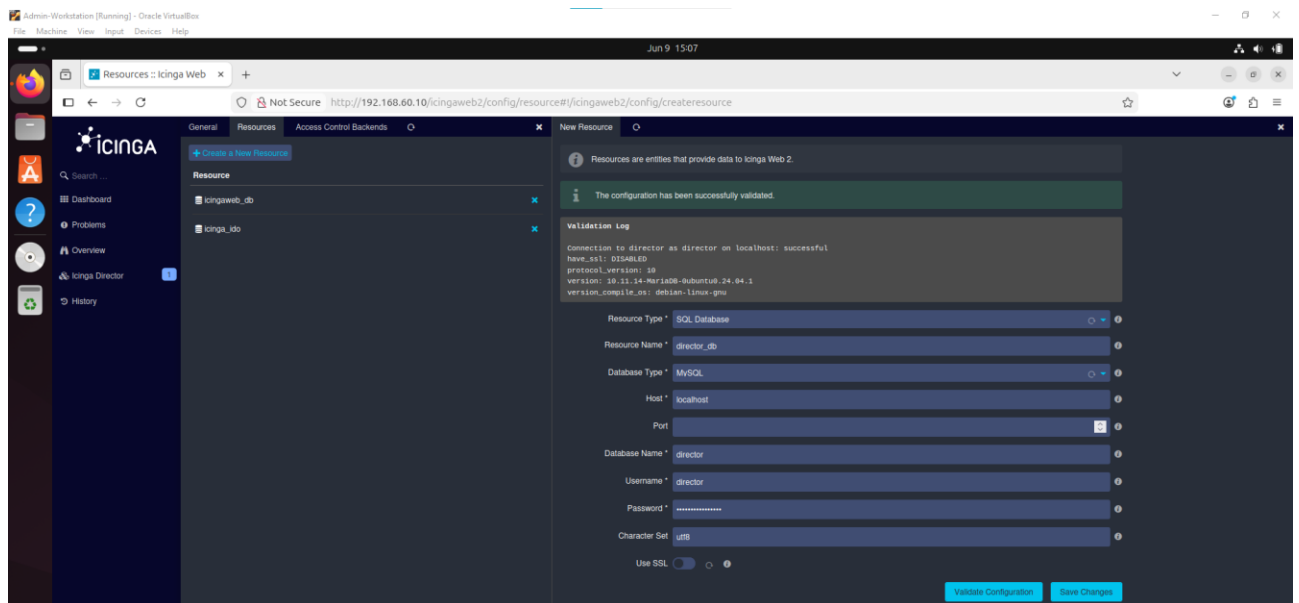


Рисунок М.7 — Підключення ресурсу бази даних Director у Icinga Web 2

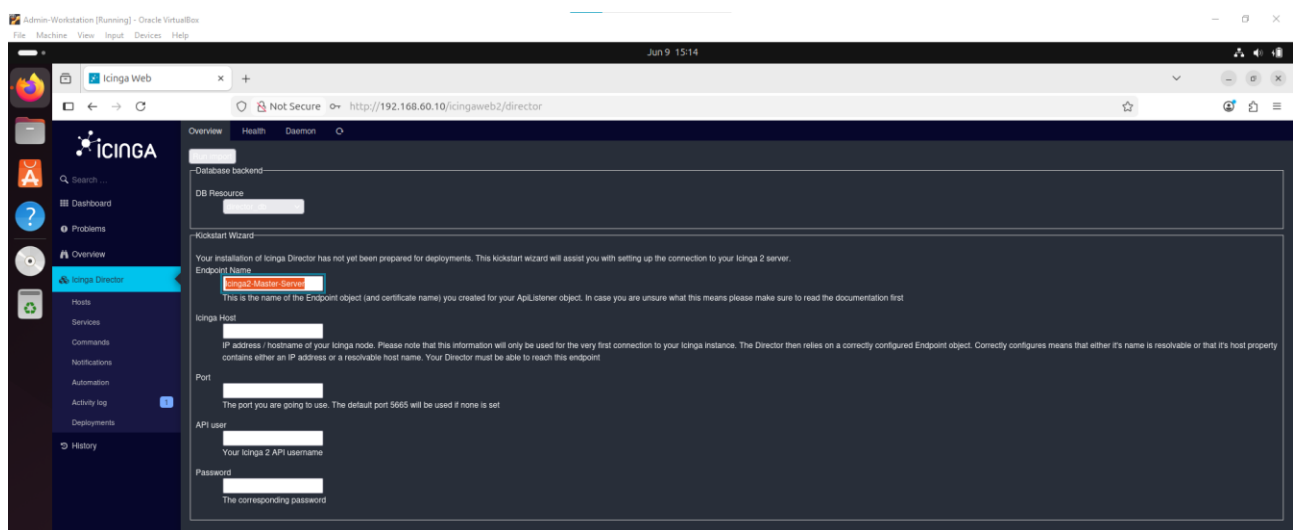


Рисунок М.8 — Kickstart Wizard для підключення Icinga Director до Icinga 2 API

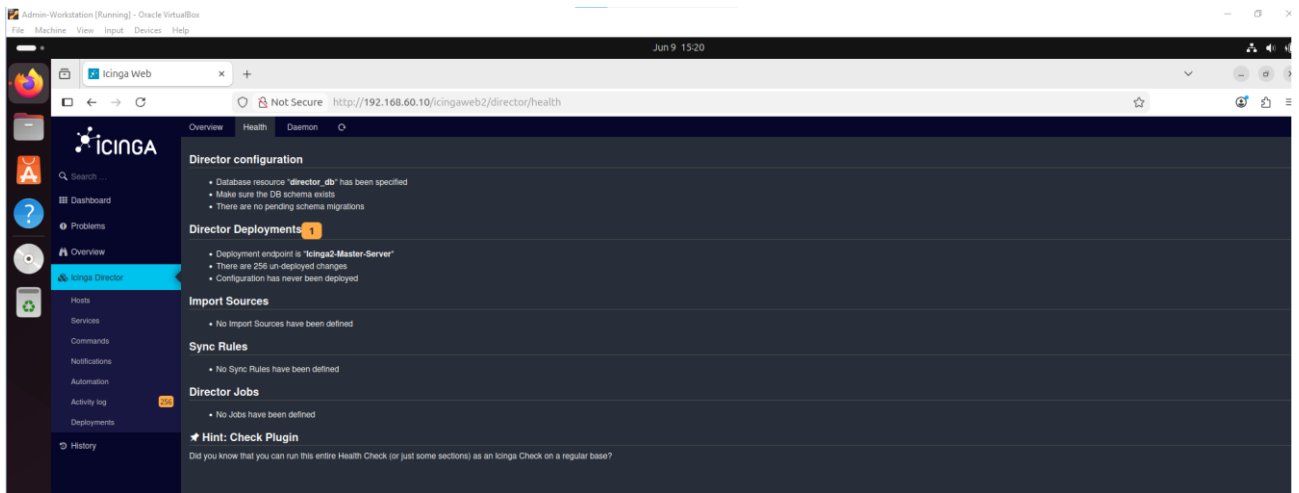


Рисунок М.9 — Сторінка стану Icinga Director після первинного підключення

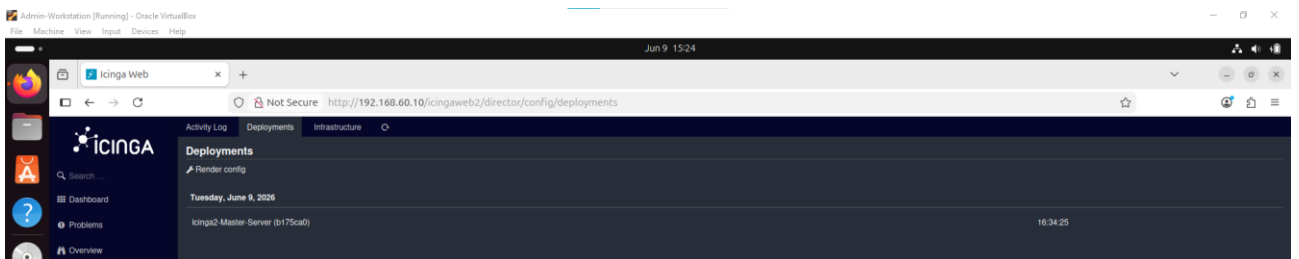


Рисунок М.10 — Історія розгортання конфігурації Icinga Director

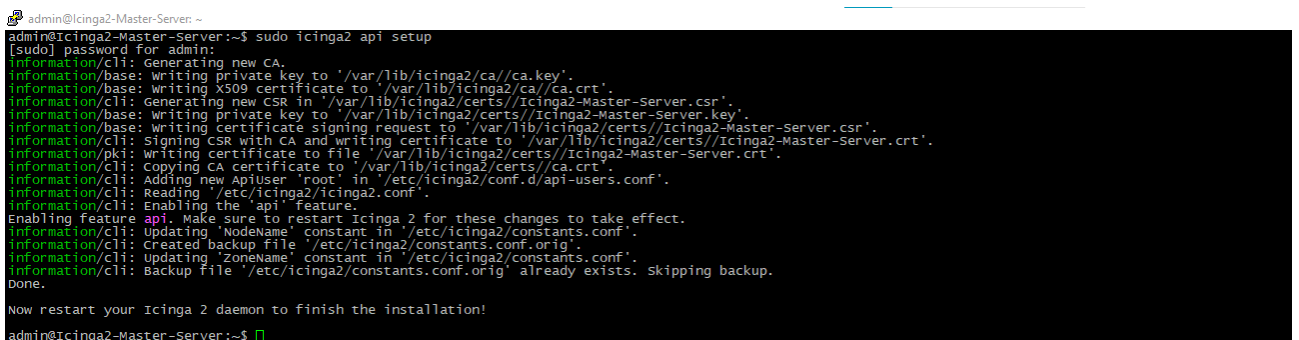


Рисунок М.11 — Ініціалізація API Icinga 2 на центральному вузлі моніторингу

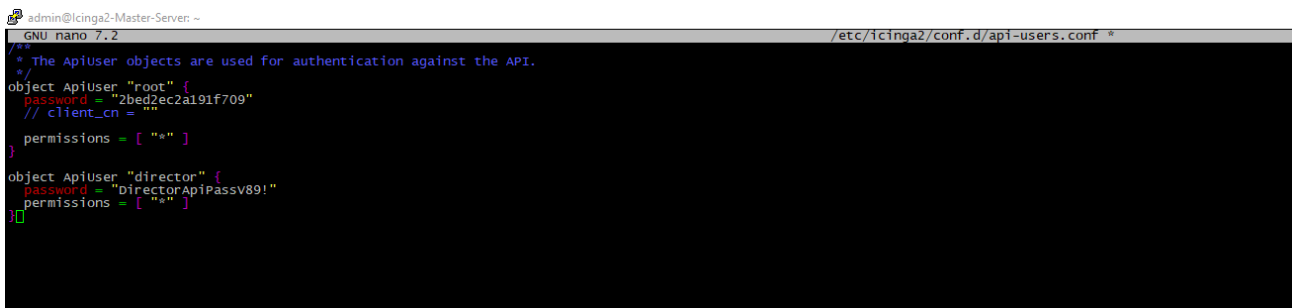


Рисунок М.12 — Конфігурація API-користувачів Icinga 2

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				138
Змн.	Арк.	№ докум.	Підпис	Дата		

```
admin@icinga2-Master-Server: ~
GNU nano 7.2 /etc/icinga2/constants.conf
/*
 * This file defines global constants which can be used in
 * the other configuration files.
 */

/* The directory which contains the plugins from the Monitoring Plugins project. */
const PluginDir = "/usr/lib/nagios/plugins"

/* The directory which contains the Manubulon plugins.
 * Check the documentation, chapter "SNMP Manubulon Plugin Check Commands", for details.
 */
const ManubulonPluginDir = "/usr/lib/nagios/plugins"

/* The directory which you use to store additional plugins which IITL provides user contributed command definitions for.
 * Check the documentation, chapter "Plugins contribution", for details.
 */
const PluginContribDir = "/usr/lib/nagios/plugins"

/* Our local instance name. By default this is the server's hostname as returned by 'hostname --fqdn'.
 * This should be the common name from the API certificate.
 */
const NodeName = "icinga2-Master-Server"

/* Our local zone name. */
const ZoneName = "icinga2-Master-Server"

/* Secret key for remote node tickets */
const TicketSalt = "DirectorTicketPass123!QwE"
```

Рисунок М.13 — Глобальні константи Icinga 2 для роботи API та агентів

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				139
Змн.	Арк.	№ докум.	Підпис	Дата		

Підключення серверів до агентного моніторингу Icinga 2

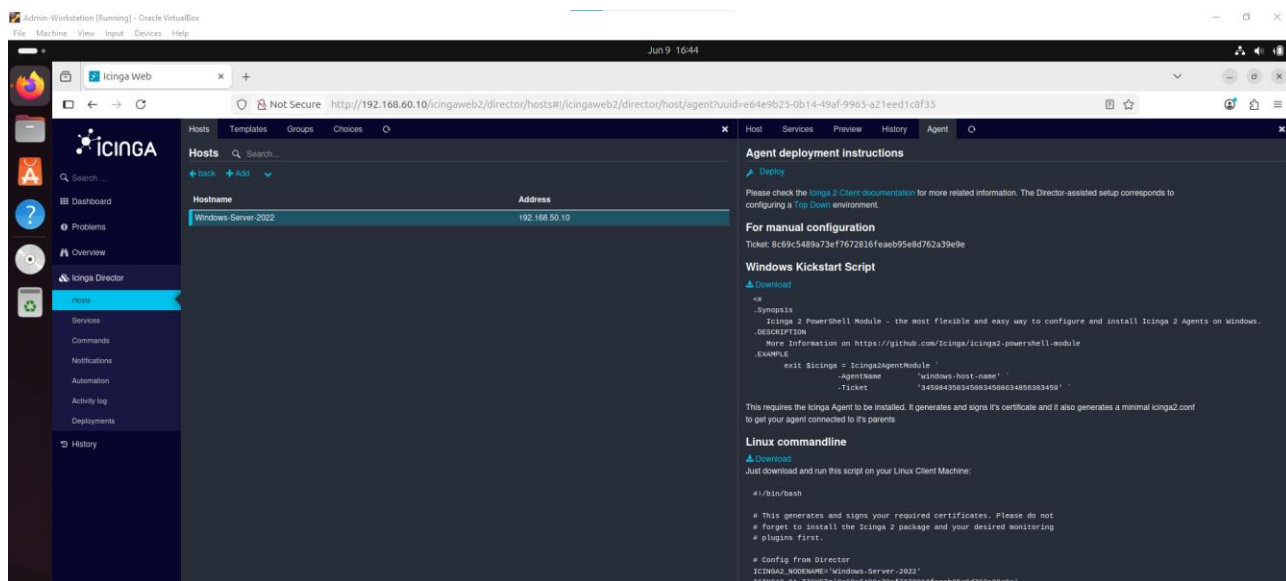


Рисунок Н.1 — Інструкція Icinga Director для розгортання агента Windows Server 2022

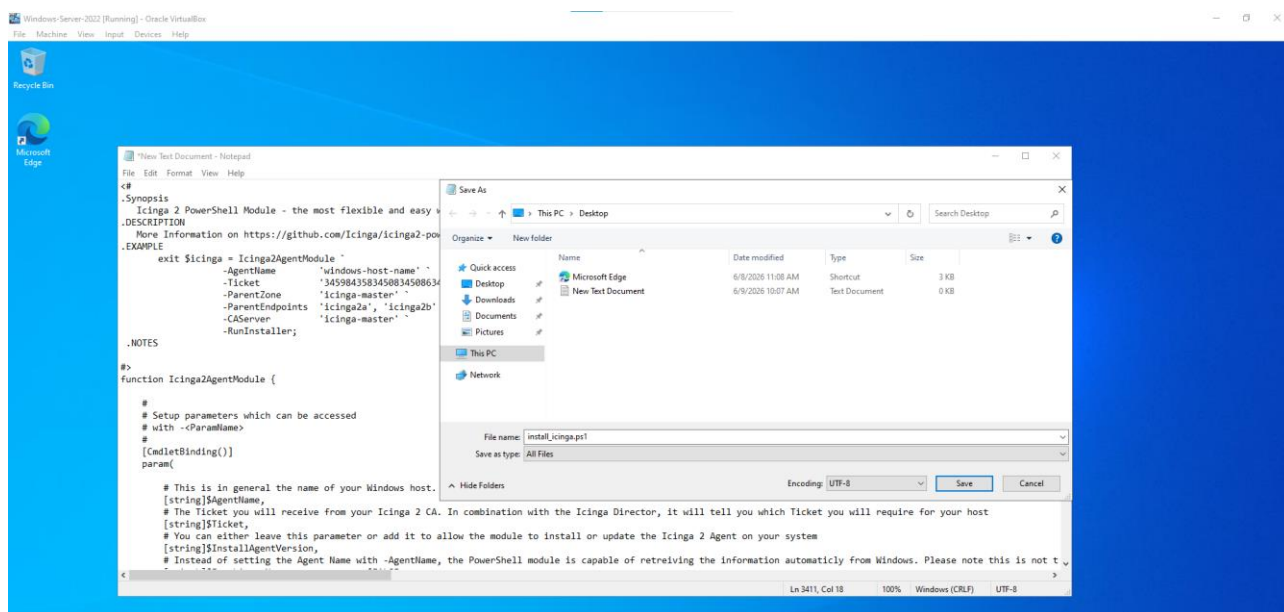


Рисунок Н.2 — Підготовка PowerShell-сценарію встановлення Icinga 2 Agent на Windows Server 2022

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				140
Змн.	Арк.	№ докум.	Підпис	Дата		

```
admin@Linux-App-Server ~$ cat install_icinga.sh
#!/bin/bash
# This generates and signs your required certificates. Please do not
# forget to install the icinga 2 package and your desired monitoring
# plugin first.

# Config from Director
ICINGA2_HOSTNAME="linux-app-server"
ICINGA2_CA_TICKET="1fabb39eeb628abb8eed3f0cc9f518890963453"
ICINGA2_PARENT_ZONE="icinga2-master-server"
ICINGA2_PARENT_ENDPOINTS="icinga2-master-server,icinga2-master-server"
ICINGA2_CA_NODE="icinga2-master-server"
ICINGA2_GLOBAL_ZONES="director-global"

# Internal defaults
IFS=$'\n'
set -e
set -o pipefail
set -x

# Helper functions
fail() {
    echo "ERROR: $1" >&2
    exit 1
}

warn() {
    echo "WARNING: $1" >&2
}

info() {
    echo "INFO: $1" >&2
}

check_command() {
    command="$@"
    if ! command >/dev/null; then
        fail "Command $command not found"
    fi
}

install_config() {
    if [ -f "$1" ]; then
        info "creating a backup at ${1}.orig"
        cp "$1" "${1}.orig"
    fi
    echo "writing config to $1"
    echo "$@" > "$1"
}

[ "$BASH_VERSION" ] || fail "This is a Bash script"

errors=()
for key in NODENAME CA_NODE CA_PORT CA_TICKET PARENT_ZONE PARENT_ENDPOINTS; do
    var="ICINGA2_${key}"
    if [ -z "${!var}" ]; then
        warn "The variable $var needs to be configured!"
        errors+=("$var")
    fi
done

if [ ${#errors[@]} -gt 0 ]; then
    fail "errors: ${errors[@]}"
fi

# Detect osfamily
if [ -n "$(dpkg-query -f='${Package}\n' -W -f='${Package} %n\n' | grep -E 'icinga2|icinga2-agent|icinga2-plugins|icinga2-tools|icinga2-remote|icinga2-wddm|icinga2-ldap|icinga2-redis|icinga2-syslog|icinga2-elasticsearch|icinga2-mysql|icinga2-postgresql|icinga2-oracle|icinga2-ldap|icinga2-redis|icinga2-syslog|icinga2-elasticsearch|icinga2-mysql|icinga2-postgresql|icinga2-oracle' | cut -d: -f1)" ]; then
    info "Assuming supplied osfamily $OS_FAMILY"
    if ! check_command rpm && ! check_command dpkg; then
        info "This should be a redhat system"
        if [ -e /etc/sysconfig/icinga2 ]; then
            # shellcheck disable=SC1091
            . /etc/sysconfig/icinga2
        fi
    fi
else
    fail "Unsupported OS family"
fi
```

Рисунок Н.3 — Сценарій install_icinga.sh для підключення Linux-App-Server до Icinga2-Master-Server

Налаштування SNMP-моніторингу pfSense

The screenshot displays the 'Services / SNMP' configuration page in pfSense. The page is divided into several sections:

- SNMP Daemon:** Includes an 'Enable' checkbox (checked) and a description: 'Enable the SNMP Daemon and its controls'.
- SNMP Daemon Settings:**
 - Polling Port:** A text input field containing '161' with a description: 'Enter the port to accept polling events on (default 161)'.
 - System Location:** An empty text input field.
 - System Contact:** An empty text input field.
 - Read Community String:** A text input field containing 'k9aJ3mP9zvLq2' with a description: 'The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.'
- SNMP Traps:** Includes an 'Enable' checkbox (unchecked) and a description: 'Enable the SNMP Trap and its controls'.
- SNMP Modules:** A list of modules with checkboxes:
 - MibII (checked)
 - Netgraph (checked)
 - PF (checked)
 - Host Resources (checked)
 - UCD (checked)
 - Regex (checked)
- Interface Binding:**
 - Internet Protocol:** A dropdown menu set to 'IPv4'.
 - Bind Interfaces:** A list box containing 'All', 'WAN', 'LAN', and 'Localhost', with 'All' selected.

A 'Save' button is located at the bottom of the form.

Рисунок П.1 — Налаштування SNMP-сервісу на pfSense для моніторингу інтерфейсів, ресурсів і Suricata

Шаблони хостів у Icinga Director

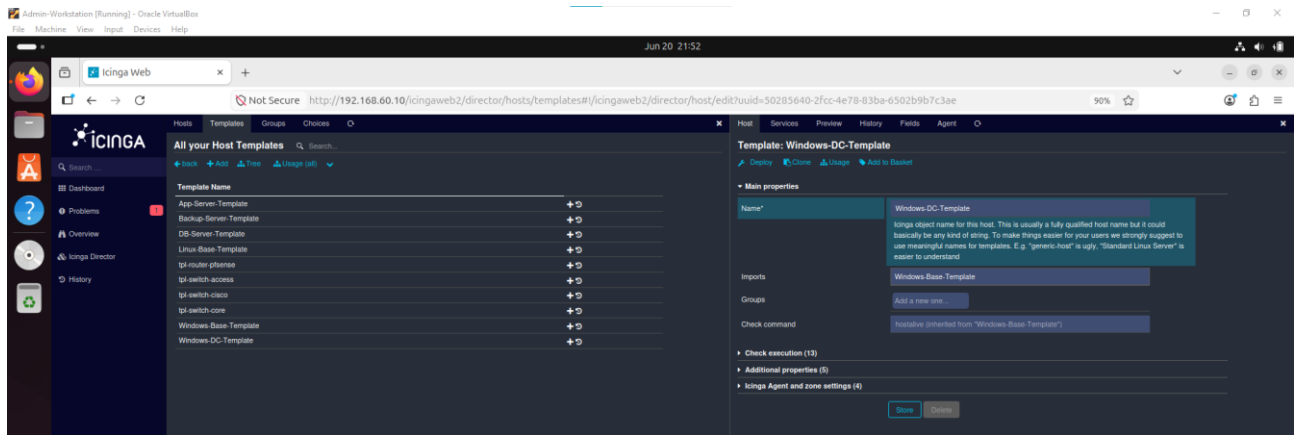


Рисунок Р.1 — Шаблон Windows-DC-Template для контролера домену Windows Server 2022

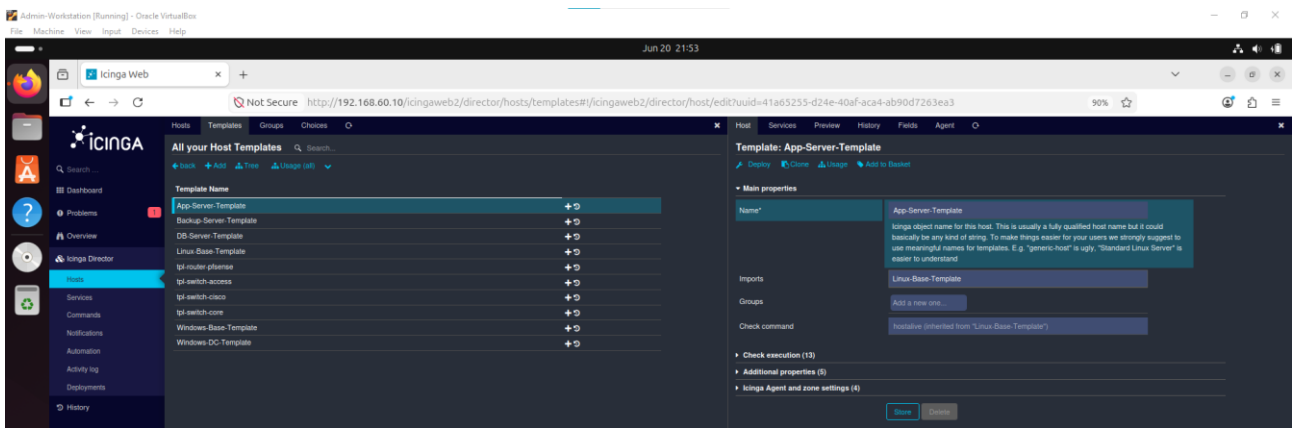


Рисунок Р.2 — Рольовий шаблон App-Server-Template для Linux-App-Server

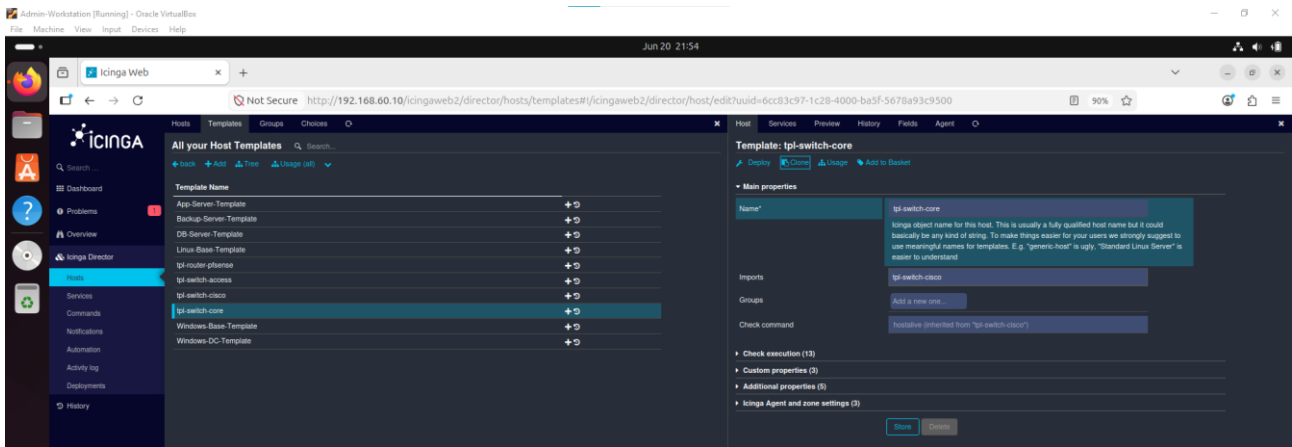


Рисунок Р.3 — Шаблон tpl-switch-core для Cisco Core-L3-Switch

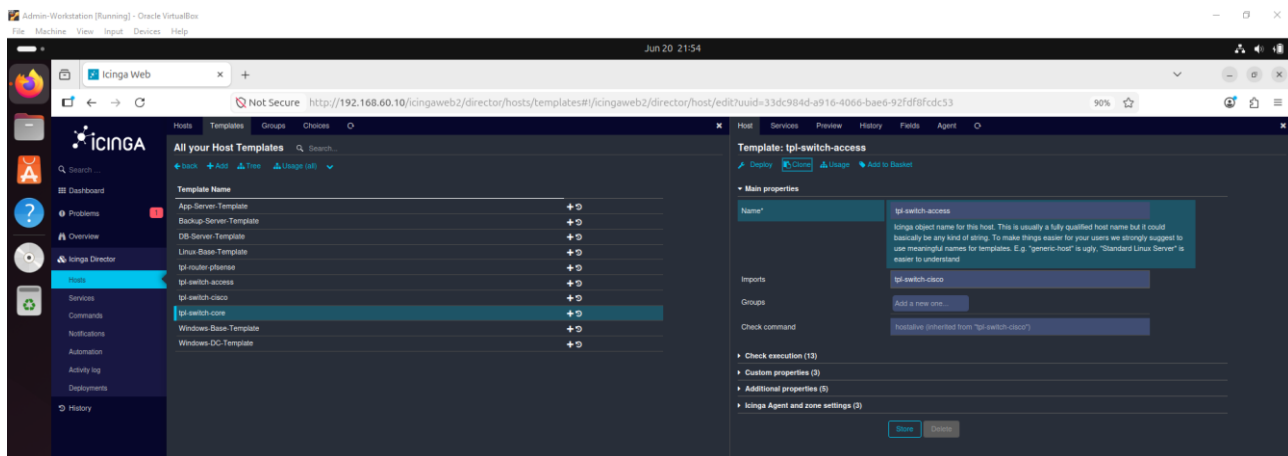


Рисунок Р.4 — Шаблон tpl-switch-access для комутаторів доступу

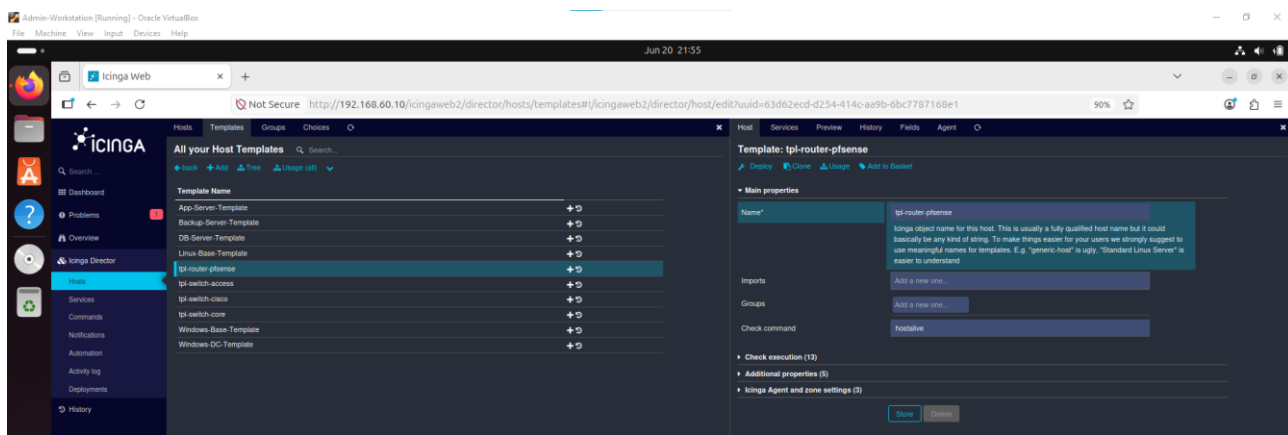


Рисунок Р.5 — Шаблон tpl-router-pfsense для граничного маршрутизатора pfSense

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				144
Змн.	Арк.	№ докум.	Підпис	Дата		

Сервісні шаблони та сервісні набори Icinga Director

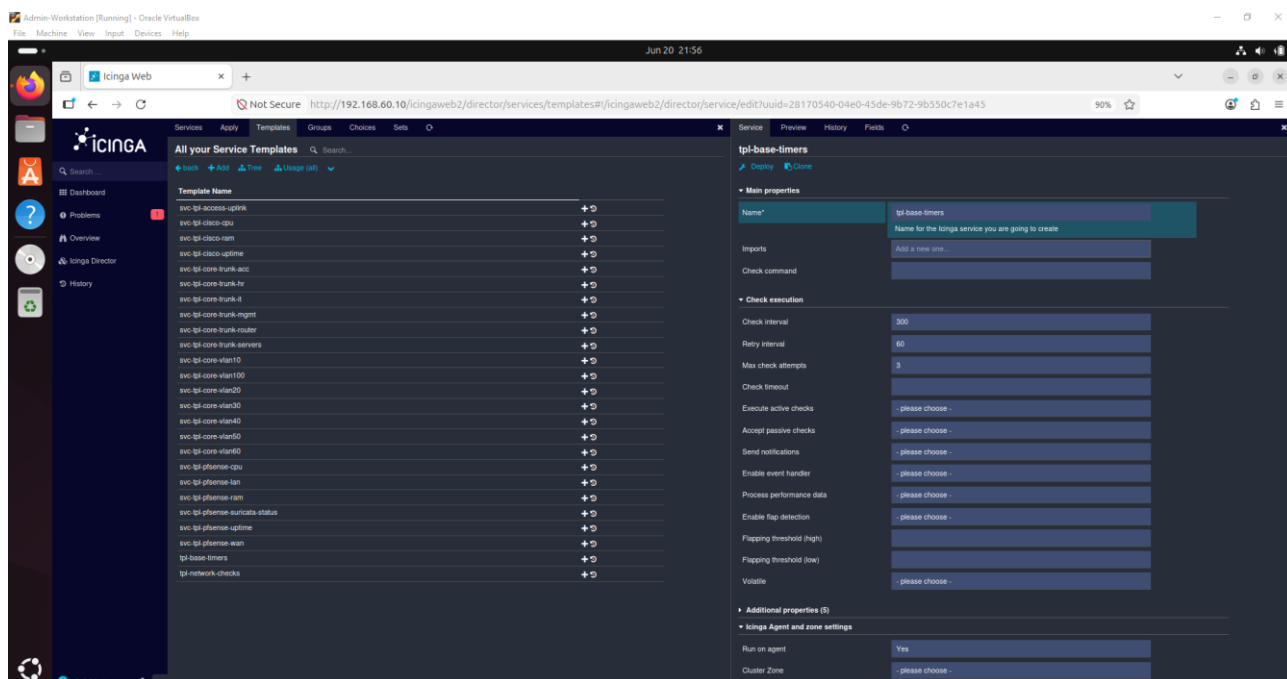


Рисунок С.1 — Базовий сервісний шаблон tpl-base-timers

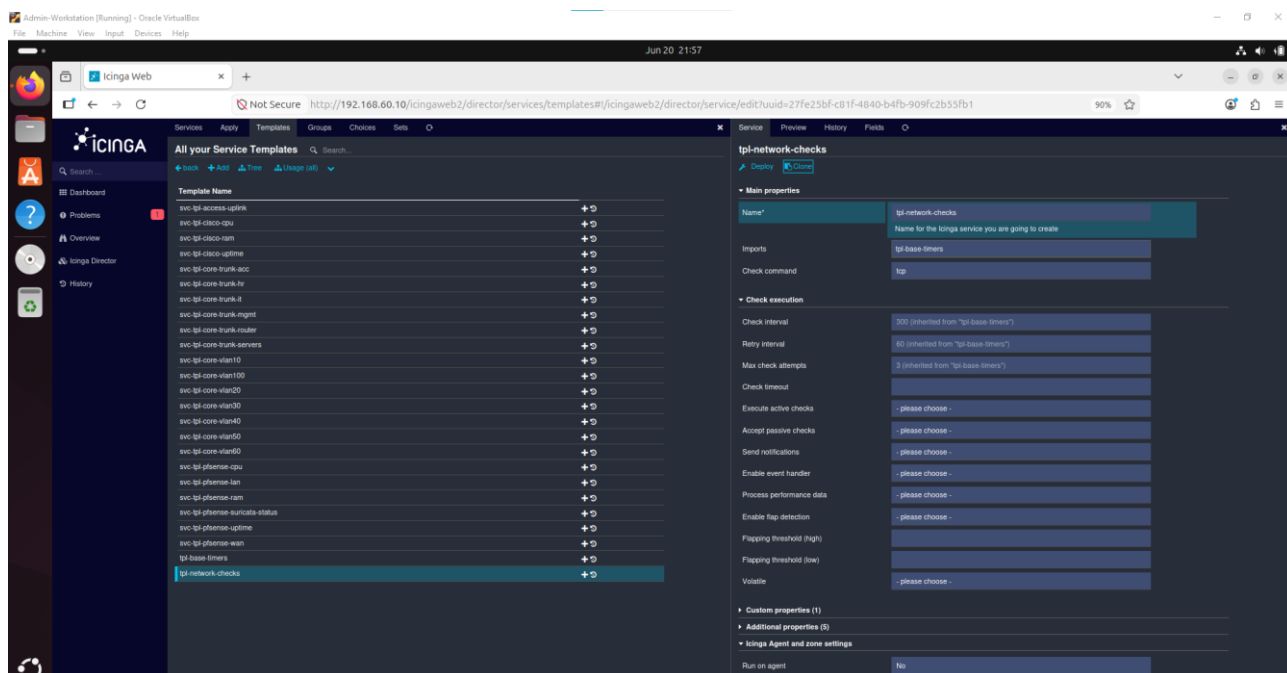


Рисунок С.2 — Сервісний шаблон tpl-network-checks для мережових перевірок

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський П.Г.				145
Змн.	Арк.	№ докум.	Підпис	Дата		

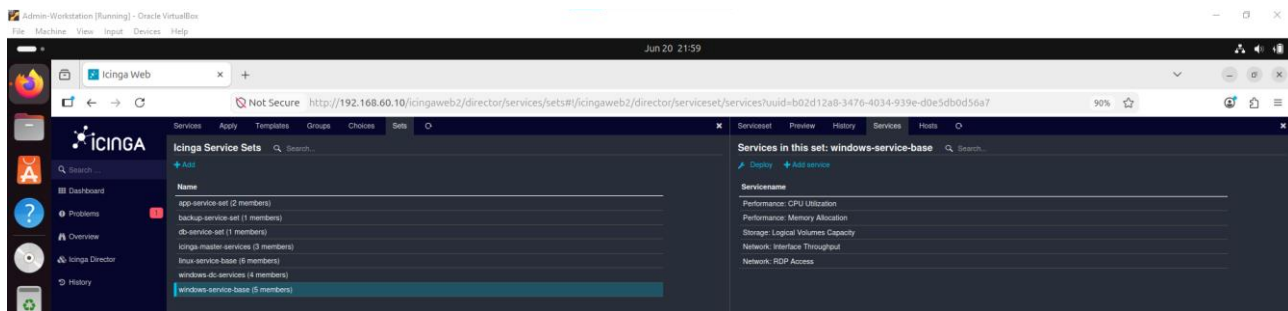


Рисунок С.3 — Базовий сервісний набір windows-service-base для Windows-серверів

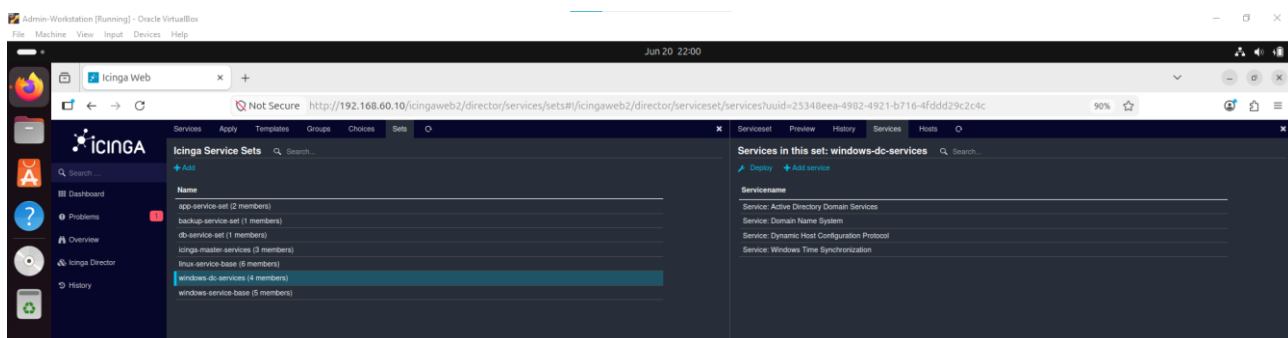


Рисунок С.4 — Сервісний набір windows-dc-services для служб контролера домену

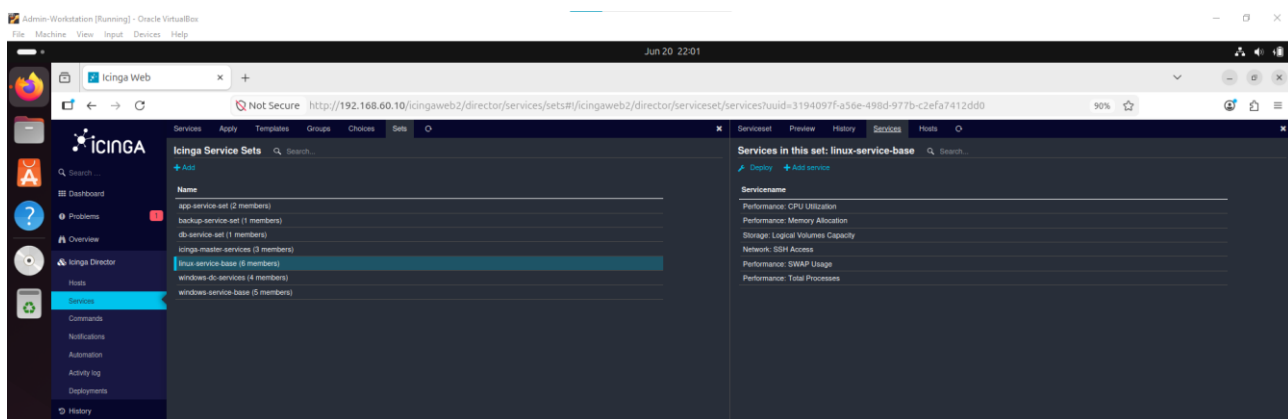


Рисунок С.5 — Базовий сервісний набір linux-service-base для Linux-серверів

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				146
Змн.	Арк.	№ докум.	Підпис	Дата		

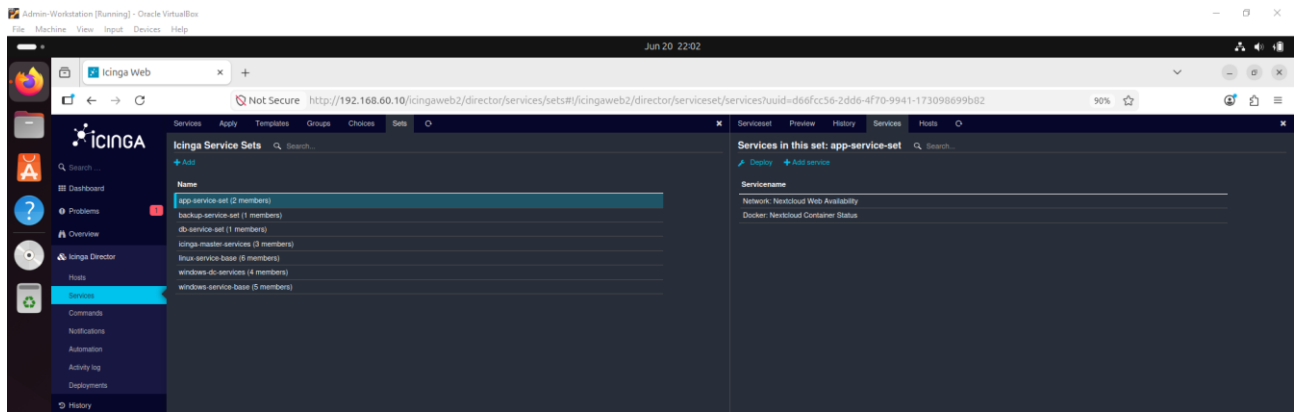


Рисунок С.6 — Сервісний набір app-service-set для контролю Nextcloud і Docker-контейнера

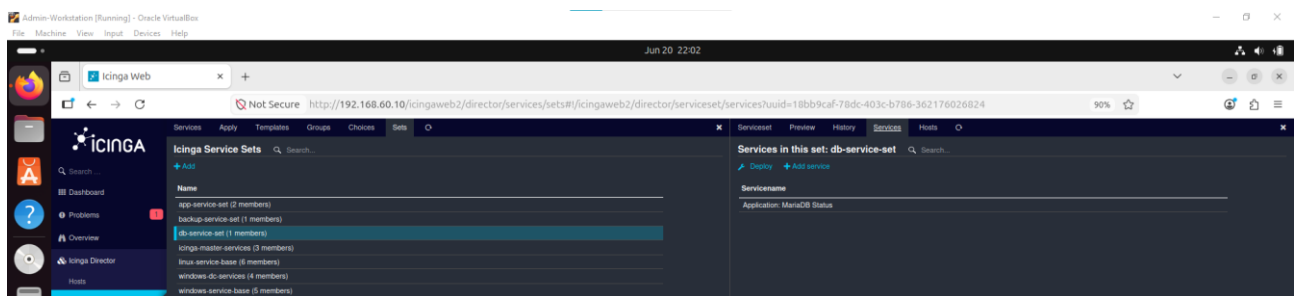


Рисунок С.7 — Сервісний набір db-service-set для контролю MariaDB

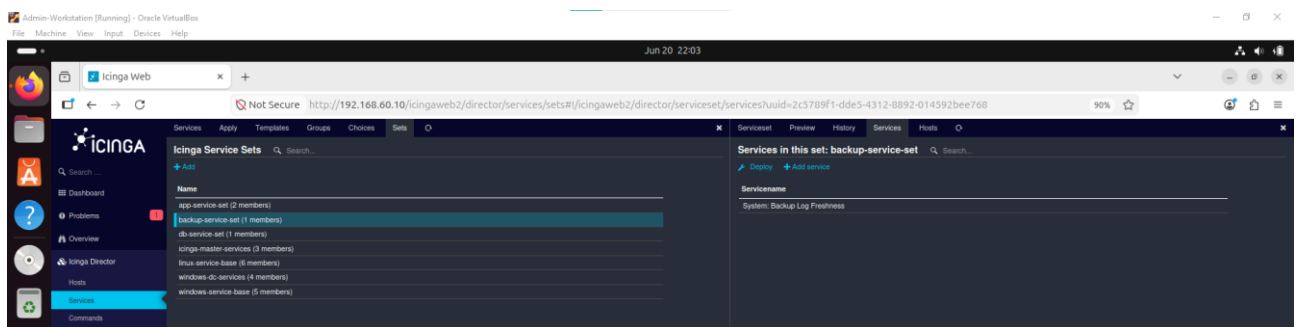


Рисунок С.8 — Сервісний набір backup-service-set для контролю актуальності журналу резервного копіювання

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				147
Змн.	Арк.	№ докум.	Підпис	Дата		

Правила автоматичного призначення перевірок Apply Rules

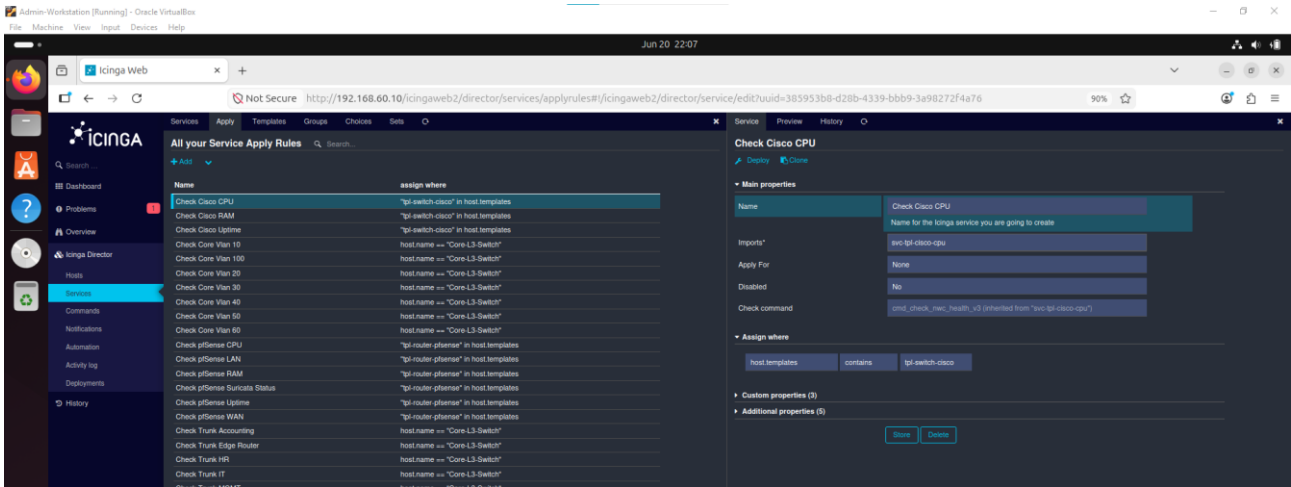


Рисунок Т.1 — Apply Rule для базової перевірки CPU Cisco-комутаторів

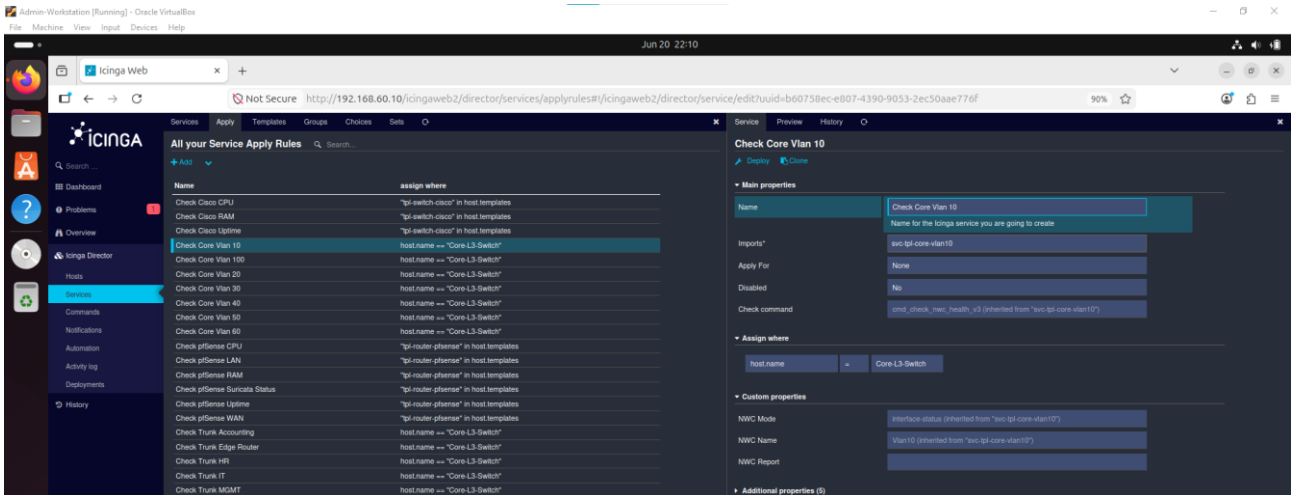


Рисунок Т.2 — Apply Rule для перевірки VLAN-інтерфейсу Core-L3-Switch

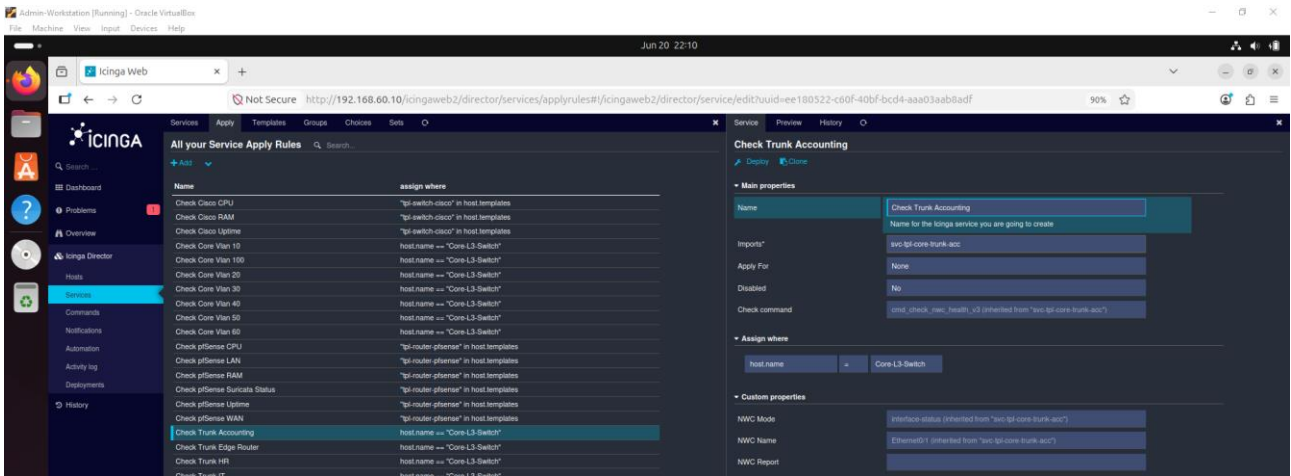


Рисунок Т.3 — Apply Rule для перевірки trunk-з'єднання Core-L3-Switch

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський П.Г.				148
Змн.	Арк.	№ докум.	Підпис	Дата		

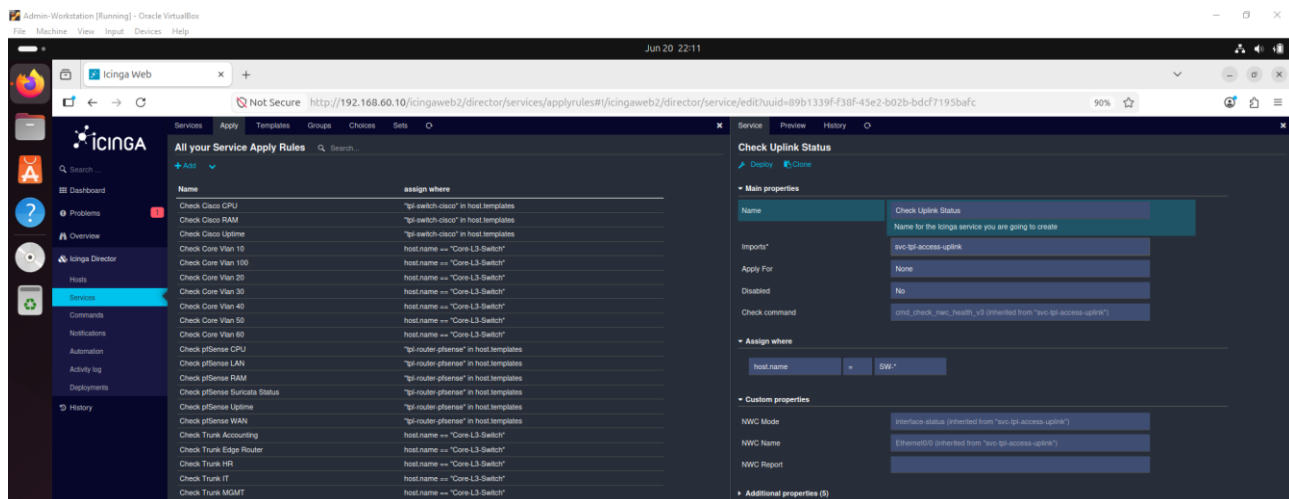


Рисунок Т.4 — Apply Rule для перевірки uplink-портів комутаторів доступу

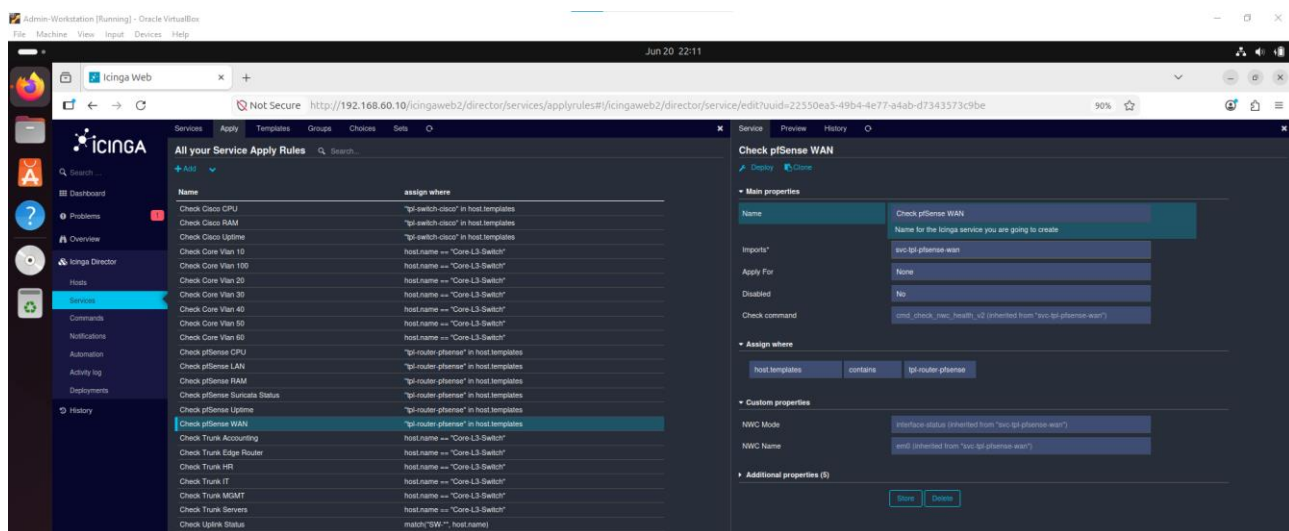


Рисунок Т.5 — Apply Rule для перевірки WAN-інтерфейсу pfsense

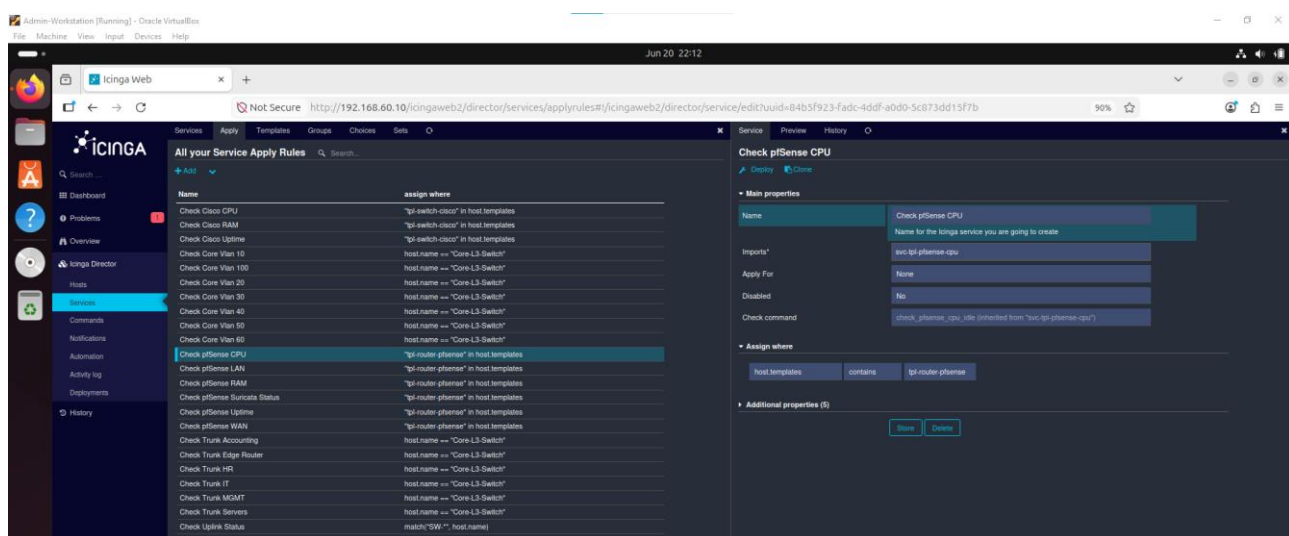


Рисунок Т.6 — Apply Rule для перевірки використання процесора pfsense

		Берковський І.Ю.				Арк.
		Фальковський ІГ.				149
Змн.	Арк.	№ докум.	Підпис	Дата	ККІКБ.КР.Б – 125 – 03 – ПЗ	

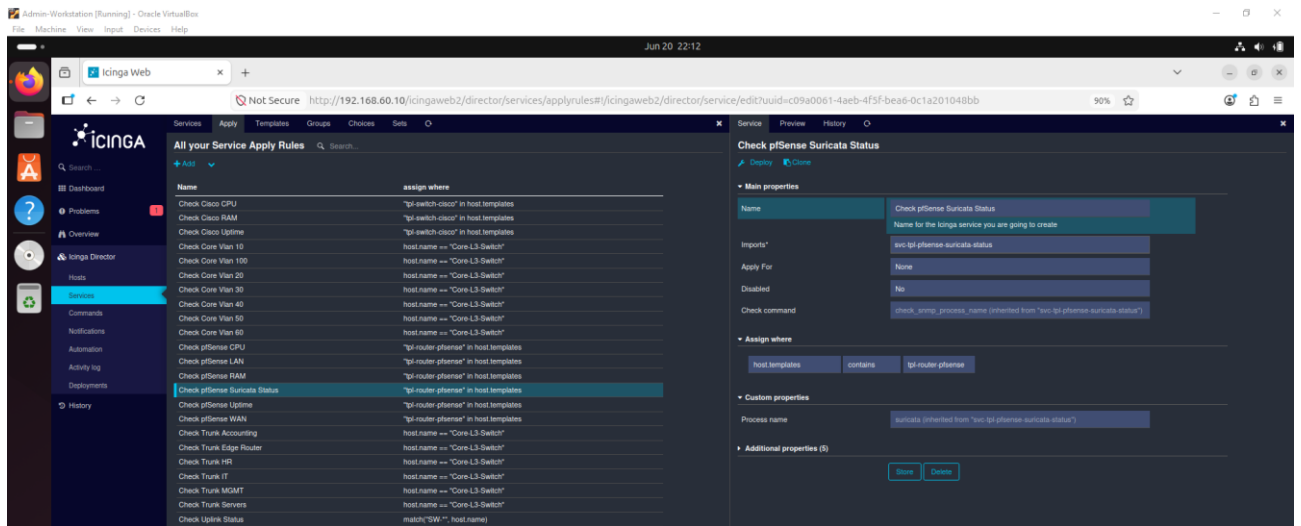


Рисунок Т.7 — Apply Rule для перевірки процесу Suricata на pfSense

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				150
Змн.	Арк.	№ докум.	Підпис	Дата		

Data Fields та CheckCommands у Icinga Director

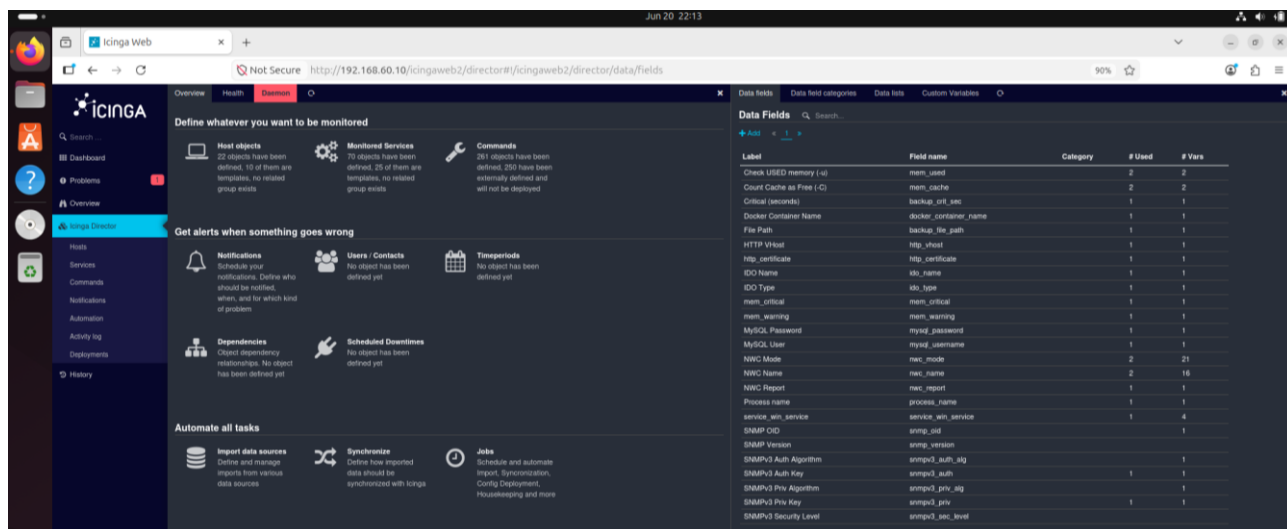


Рисунок У.1 — Огляд Data Fields, створених в Icinga Director

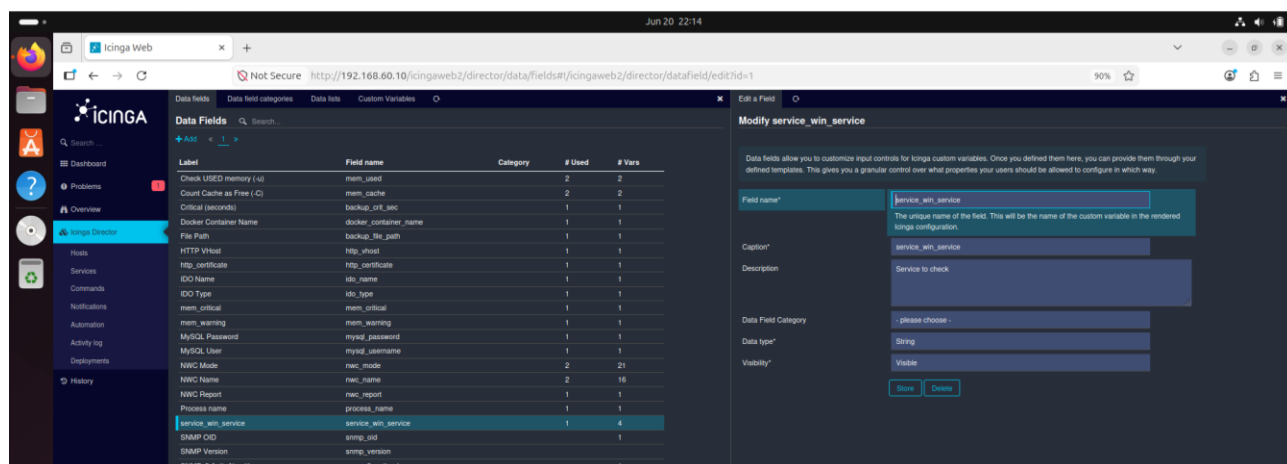


Рисунок У.2 — Data Field service_win_service для перевірки служб Windows Server

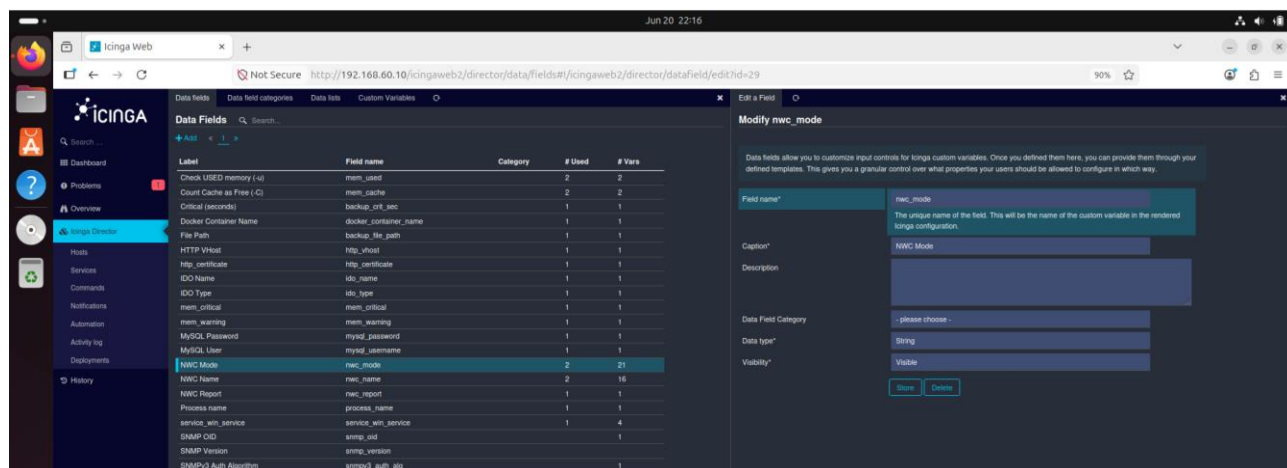


Рисунок У.3 — Data Field nwc_mode для SNMP-перевірок мережевого обладнання

		Берковський І.Ю.							Арк.
		Фальковський ІГ.							151
Змн.	Арк.	№ докум.	Підпис	Дата					

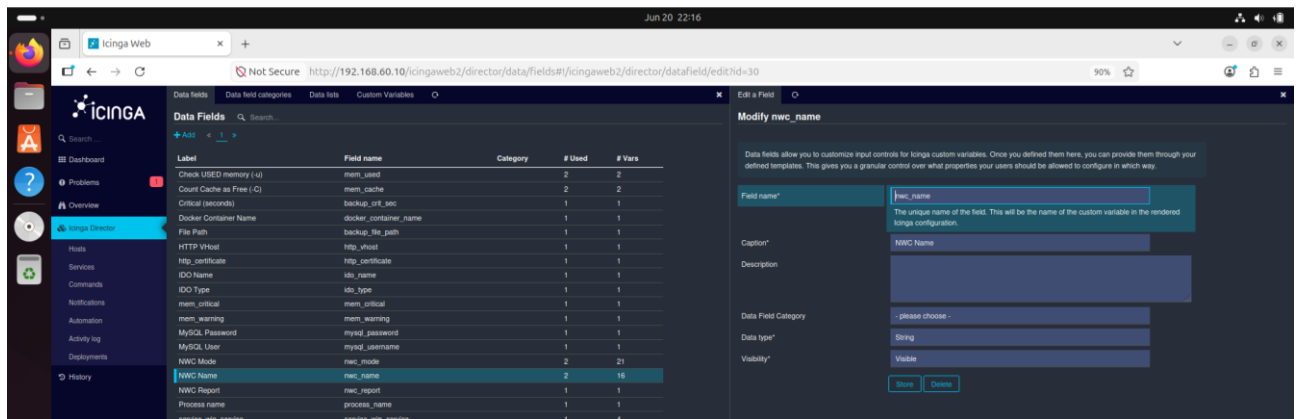


Рисунок У.4 — Data Field nwc_name для визначення інтерфейсу або об'єкта SNMP-перевірки

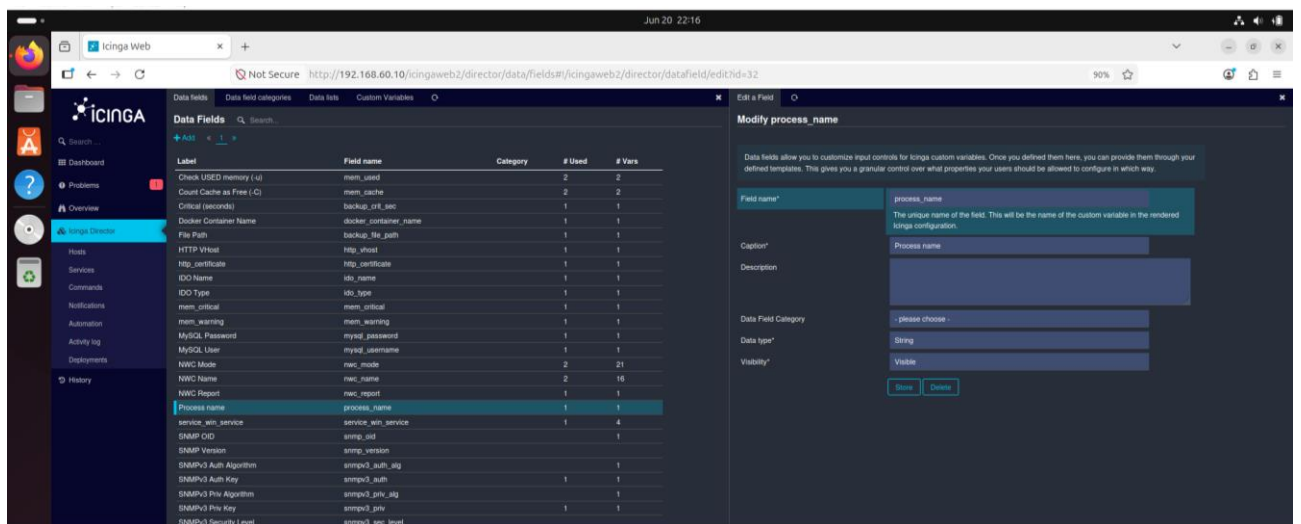


Рисунок У.5 — Data Field process_name для перевірки процесу Suricata

Critical (seconds)	backup_crit_sec	1	1
Docker Container Name	docker_container_name	1	1
File Path	backup_file_path	1	1

Рисунок У.6 — Data Field backup_file_path для перевірки журналу резервного копіювання

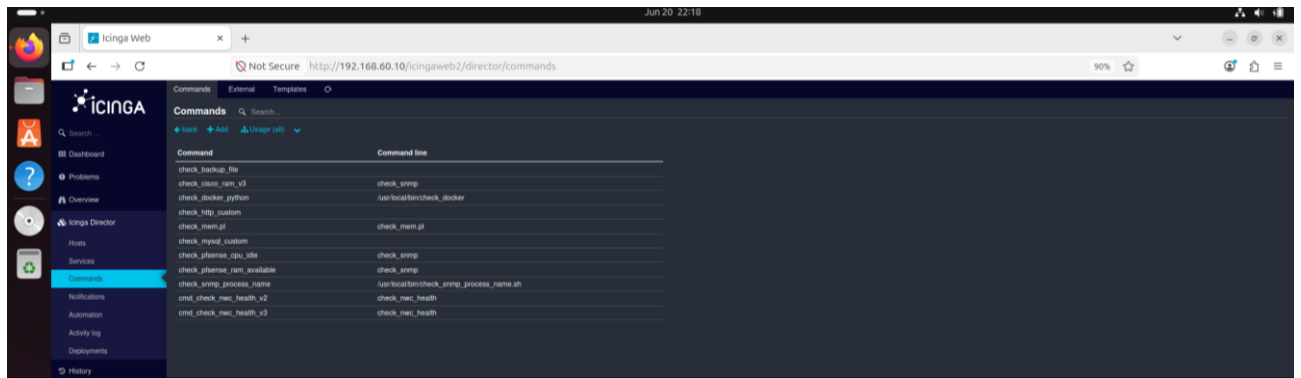


Рисунок У.7 — Перелік CheckCommands, використаних у системі моніторингу

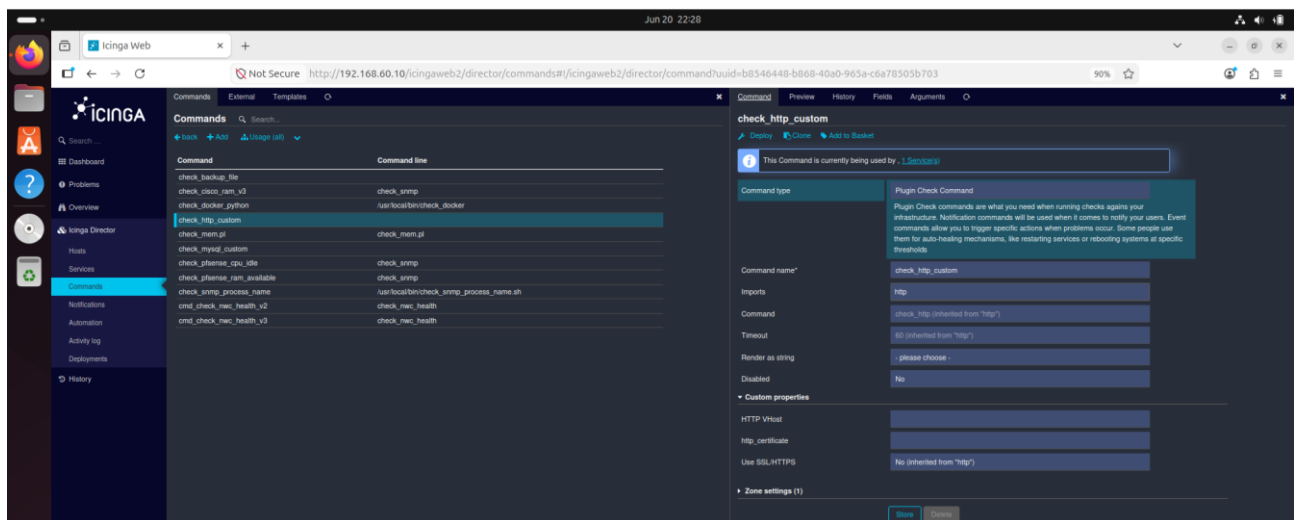


Рисунок У.8 — CheckCommand check_http_custom для перевірки доступності Nextcloud

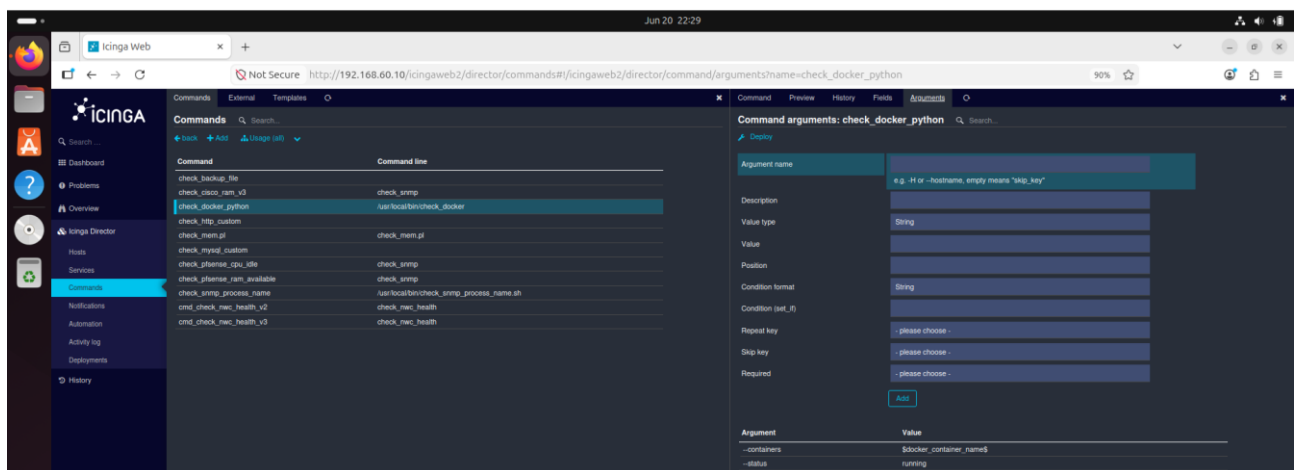


Рисунок У.9 — Аргументи CheckCommand check_docker_python для перевірки Docker-контейнера

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				153
Змн.	Арк.	№ докум.	Підпис	Дата		

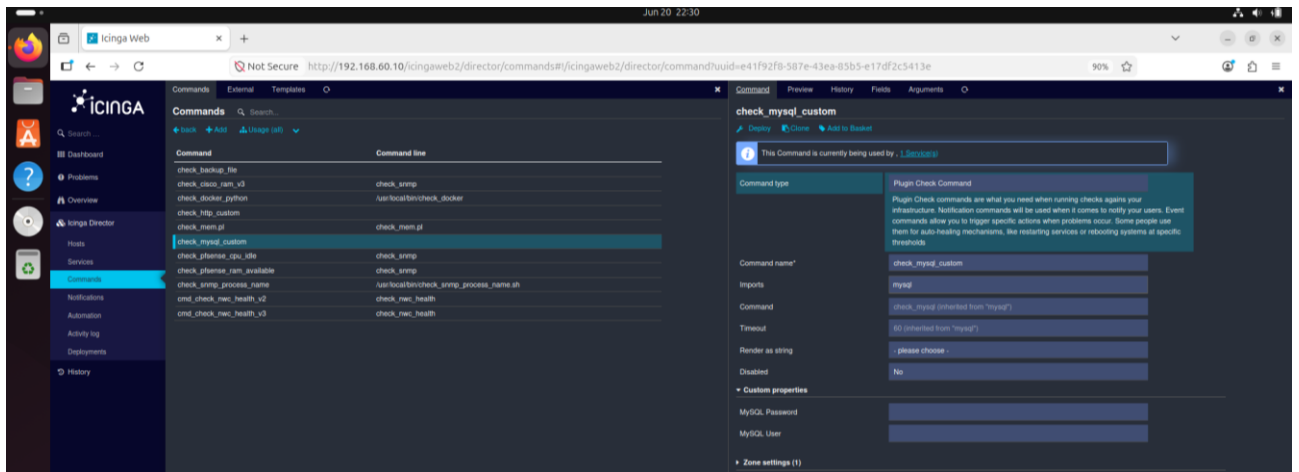


Рисунок У.10 — CheckCommand check_mysql_custom для перевірки MariaDB

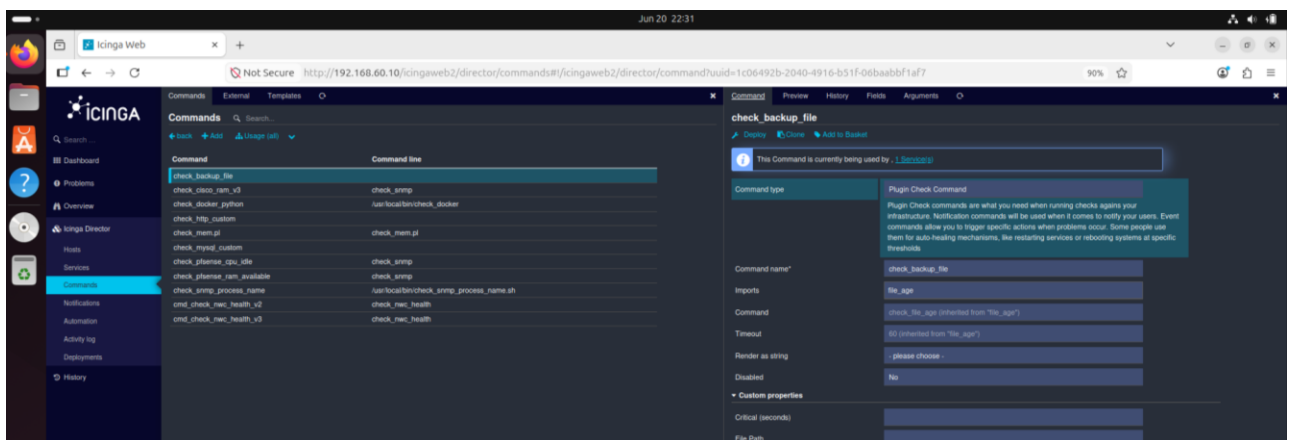


Рисунок У.11 — CheckCommand check_backup_file для перевірки актуальності журналу резервного копіювання

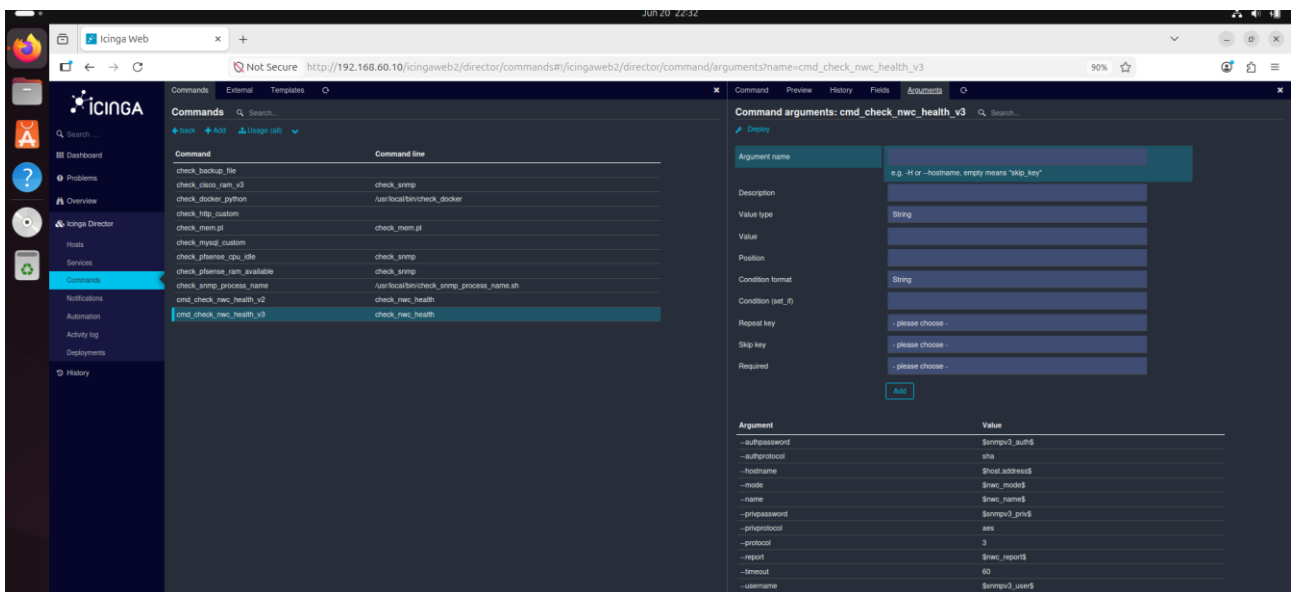


Рисунок У.12 — Аргументи CheckCommand cmd_check_nwc_health_v3 для SNMPv3-моніторингу Cisco-комутаторів

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський ІГ.				154
Змн.	Арк.	№ докум.	Підпис	Дата		

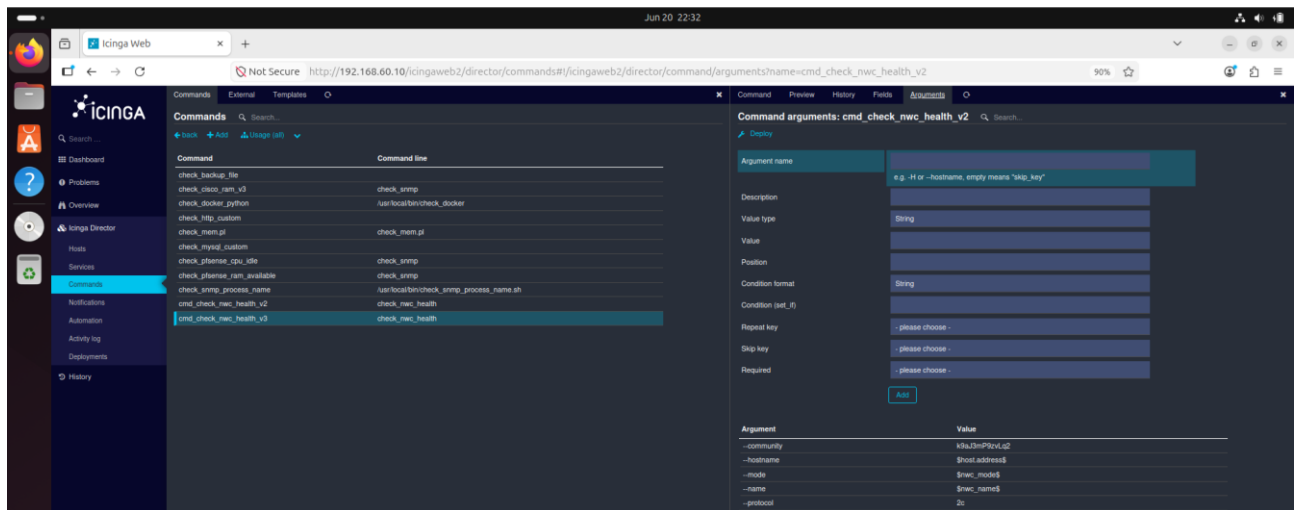


Рисунок У.13 — Аргументи CheckCommand cmd_check_nwc_health_v2 для SNMP-моніторингу pfSense

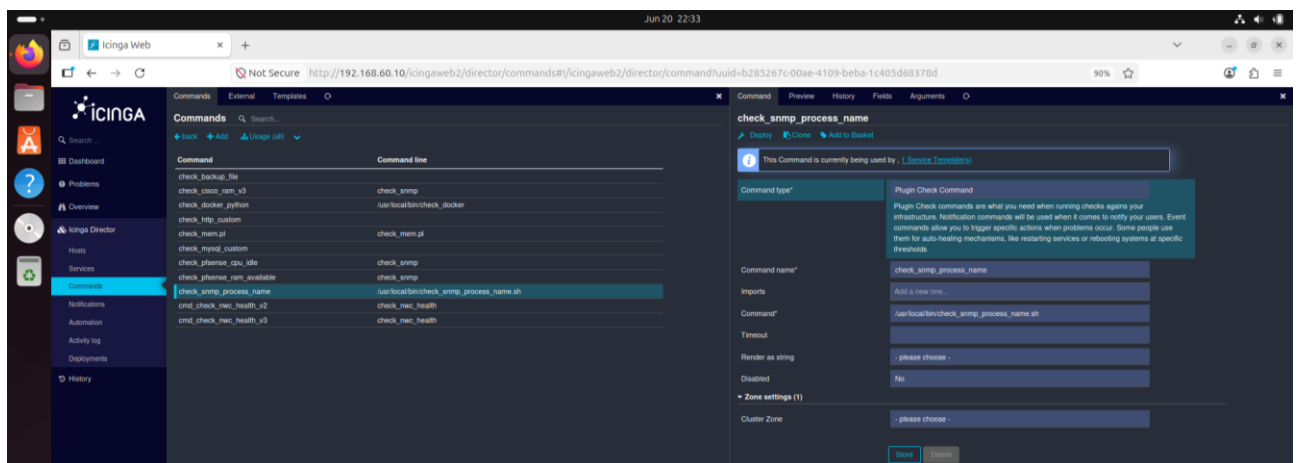


Рисунок У.14 — CheckCommand check_snmp_process_name для перевірки процесу Suricata

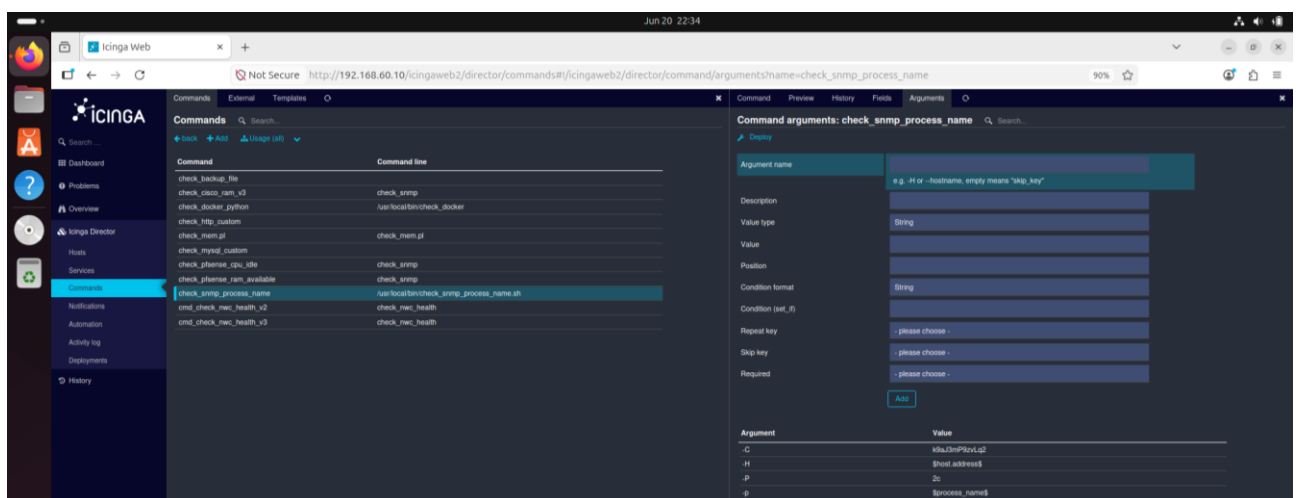


Рисунок У.15 — Аргументи CheckCommand check_snmp_process_name

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				155
Змн.	Арк.	№ докум.	Підпис	Дата		

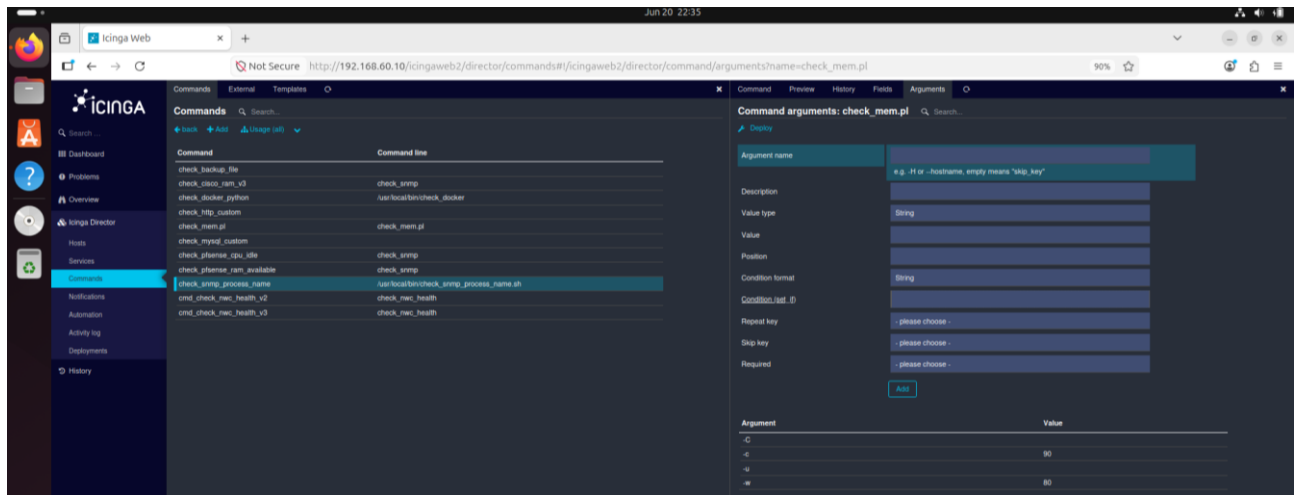


Рисунок У.16 — Аргументи CheckCommand check_mem.pl для перевірки оперативної пам'яті Linux-серверів

		Берковський І.Ю.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Фальковський І.Г.				156
Змн.	Арк.	№ докум.	Підпис	Дата		