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: «Проєкт підсистеми безпекового моніторингу доменної інфраструктури Microsoft Active Directory із застосуванням Graylog»

Виконав: студент 4-го курсу групи КБ-22-3
спеціальності 125 «Кіберберзпека»
_____ Іван Огороднійчук
Керівник: старший викладач кафедри КІ та КБ
_____ Ігор Фальковський
Рецензент: к.пед.н.,доцент кафедри КІ та КБ
_____ Олена Головня

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 випускну кваліфікаційну роботу бакалавра

Студент: Огороднійчук Іван Анатолійович

Тема роботи: «Проєкт підсистеми безпекового моніторингу доменної інфраструктури Microsoft Active Directory із застосуванням Graylog»

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

Термін здачі студентом закінченої роботи 26 червня 2026 р.

Вихідні дані роботи :

Необхідність побудови та дослідження системи безпекового моніторингу в мінімальній доменній інфраструктурі Microsoft Active Directory із забезпеченням централізованого збору журналів подій, виявлення невдалих спроб автентифікації, змін облікових записів, ескалації привілеїв, підозрілих входів до системи та тестових файлових загроз.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання та аналіз предметної області	01.04.26	Виконав
2	Проєктування архітектури мінімальної доменної інфраструктури та вибір програмного забезпечення	10.04.26	Виконав
3	Розгортання віртуального середовища VirtualBox і налаштування мережевої взаємодії	10.04.26	Виконав
4	Налаштування доменної інфраструктури Microsoft Active Directory (контролери домену, DNS, робоча станція)	15.04.26	Виконав
5	Розгортання та налаштування системи моніторингу Graylog, організація централізованого збору журналів подій	25.04.26	Виконав
6	Тестування системи моніторингу, моделювання інцидентів безпеки та оцінка ефективності роботи	12.05.26	Виконав
7	Оформлення пояснювальної записки, підготовка до захисту та захист роботи	05.06.26	Виконав

Студент _____ Іван Огороднійчук

Керівник _____ Ігор Фальковський

Обладнання та програмне забезпечення:

1. Апаратне забезпечення: ноутбук ASUS TUF Gaming A15 (AMD Ryzen 7, 16 ГБ RAM).
2. Система віртуалізації: Oracle VM VirtualBox 7.1.x.
3. Операційні системи та програмне забезпечення:

- Microsoft Windows Server 2022 (Standard Evaluation; Серверна операційна система, яка виступає в ролі головного контролера домену) [21]
- Microsoft Windows 10 Pro; (Клієнтська операційна система) [21]
- Ubuntu Server 24.04 LTS; (Серверна операційна система на базі Linux з тривалим терміном підтримки) [21]
- Graylog 6.x; (Централізована система управління логами) [9,10]
- Elasticsearch 8.x; (Високопродуктивний пошуковий та аналітичний рушій) [13]
- MongoDB Community Server 7.x; (NoSQL база даних) [14]
- Winlogbeat 8.x; (Легковажний агент-збирач) [11]
- NXLog Community Edition 3.x. (Універсальний та гнучкий агент для збору й пересилання логів) [12]

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ігор Фальковський	1 квітня 2026	1 квітня 2026
2	Ігор Фальковський	3 квітня 2026	3 квітня 2026
3	Ігор Фальковський	6 травня 2026	6 травня 2026

Студент _____ Іван Огороднійчук

Керівник _____ Ігор Фальковський

АНОТАЦІЯ

Мета кваліфікаційної роботи бакалавра полягає у дослідженні підходів до побудови підсистеми безпекового моніторингу доменної інфраструктури Microsoft Active Directory та реалізації централізованої системи збору й аналізу журналів подій на базі Graylog. Завданням роботи є проєктування, розгортання та налаштування системи моніторингу подій безпеки, що забезпечує контроль активності користувачів, аудит змін у доменному середовищі та виявлення типових інцидентів інформаційної безпеки.

Кваліфікаційна робота бакалавра на тему «Проєкт підсистеми безпекового моніторингу доменної інфраструктури Microsoft Active Directory із застосуванням Graylog» складається з теоретичної, проєктної та практичної частин і пояснювальної записки.

У роботі проаналізовано особливості функціонування Microsoft Active Directory, механізми аудиту подій безпеки та сучасні засоби централізованого моніторингу. Спроєктовано лабораторне середовище на базі Oracle VirtualBox, розгорнуто доменну інфраструктуру Microsoft Active Directory та сервер моніторингу Graylog. Налаштовано служби DNS, реплікацію між контролерами домену, а також агенти Winlogbeat і NXLog для передавання журналів подій.

Реалізовано механізми моніторингу автентифікації користувачів, аудиту змін у домені, контролю привілейованої активності та виявлення інцидентів безпеки на основі правил кореляції подій і пошуку індикаторів компрометації. Проведено тестування працездатності створеної системи шляхом моделювання типових загроз інформаційній безпеці.

Пояснювальна записка до кваліфікаційної роботи містить 61 сторінки, 46 рисунків та 2 таблиці. Список використаних джерел налічує 21 найменування.

КЛЮЧОВІ СЛОВА: MICROSOFT ACTIVE DIRECTORY, GRAYLOG, WINLOGBEAT, NXLOG, БЕЗПЕКОВИЙ МОНІТОРИНГ, ДОМЕННА ІНФРАСТРУКТУРА, ЖУРНАЛИ ПОДІЙ, АУДИТ БЕЗПЕКИ, WINDOWS SERVER, ІНФОРМАЦІЙНА БЕЗПЕКА.

					ККІКБ.КР.Б –125 – 08 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Огороднійчук.І.А		18.06.26	Проєкт підсистеми безпекового моніторингу доменної інфраструктури Microsoft Directory із застосуванням Graylog	Літ.	Арк. 4 / Аркушів 61
Керівник		Фальковський.І.Г		18.06			
Реценз.		Головня О.С.		18.06.26		ФІКТ, Гр. КБ-22-3	
Н. контр.		Фальковський.І.Г		18.06			
Затверд.		Єфіменко А.А.		20.06.26			

ANNOTATION

The purpose of the bachelor's qualification work is to study approaches to building a security monitoring subsystem for a Microsoft Active Directory domain infrastructure and to implement a centralized log collection and analysis system based on Graylog. The objective of the work is to design, deploy, and configure a security event monitoring system that provides user activity control, auditing of changes within the domain environment, and detection of typical information security incidents.

The bachelor's qualification work entitled “Project of a Security Monitoring Subsystem for Microsoft Active Directory Domain Infrastructure Using Graylog” consists of theoretical, design, and practical parts, as well as an explanatory report.

The work analyzes the features of Microsoft Active Directory operation, security event auditing mechanisms, and modern centralized monitoring solutions. A laboratory environment based on Oracle VirtualBox was designed, a Microsoft Active Directory domain infrastructure and a Graylog monitoring server were deployed. DNS services, replication between domain controllers, and Winlogbeat and NXLog agents for event log forwarding were configured.

Mechanisms for monitoring user authentication, auditing domain changes, controlling privileged activity, and detecting security incidents based on event correlation rules and indicators of compromise (IOC) searches were implemented. The functionality of the developed system was tested by simulating typical information security threats.

The explanatory report contains 61 pages, 46 figures, and 2 tables. The list of references includes 21 sources.

KEYWORDS: MICROSOFT ACTIVE DIRECTORY, GRAYLOG, WINLOGBEAT, NXLOG, SECURITY MONITORING, DOMAIN INFRASTRUCTURE, EVENT LOGS, SECURITY AUDITING, WINDOWS SERVER, INFORMATION SECURITY.

ЗМІСТ

Перелік умовних позначень 7

Вступ 9

РОЗДІЛ 1 Теоретичні основи організації безпекового моніторингу в доменних інфраструктурах Microsoft Active Directory 11

1.1 Архітектура та принципи роботи Microsoft Active Directory 11
1.2 Основні компоненти Active Directory 12
1.3 Домени, дерева та ліси Active Directory 13
1.4 Роль DNS у функціонуванні Active Directory 14
1.5 Контролери домену 15
1.6 Реплікація Active Directory 16
1.7 Механізми Kerberos та LDAP 16
1.8 Group Policy та централізоване адміністрування 17
1.9 Роль Active Directory у забезпеченні інформаційної безпеки 17
Висновки до розділу 1 18

РОЗДІЛ 2 Проєктування та розгортання системи безпекового моніторингу 19

2.1 Проєктування архітектури лабораторної інфраструктури 19
2.2 Вибір програмного забезпечення та середовища віртуалізації 20
2.3 Розгортання доменної інфраструктури Microsoft Active Directory 21
2.4 Розгортання системи централізованого моніторингу Graylog 22
Висновки до розділу 2 24

РОЗДІЛ 3 Налаштування та тестування системи безпекового моніторингу 25

3.1 Підготовка серверної інфраструктури до моніторингу 25
3.2 Налаштування сервера централізованого збору логів Graylog 30
3.3 Налаштування збору журналів подій Windows 34
3.4 Налаштування аудиту Active Directory 37
3.5 Реалізація сценаріїв виявлення інцидентів безпеки 41
3.6 Формування інформаційних панелей моніторингу 41
3.7 Аналіз отриманих результатів 42
Висновки до розділу 3 43

РОЗДІЛ 4 Реалізація механізмів виявлення інцидентів та оцінка ефективності системи 45

4.1 Реалізація правил виявлення та кореляції подій безпеки 45
4.2 Налаштування пошуку індикаторів компрометації (IOC) 46
4.3 Оцінка ефективності функціонування системи 47
Висновки до розділу 4 48

Висновки 49

Список використаної літератури 51

ДОДАТКИ 53

Перелік умовних позначень

AD – Active Directory

AD DS – Active Directory Domain Services

DNS – Domain Name System

GPO – Group Policy Object

LDAP – Lightweight Directory Access Protocol

DC – Domain Controller

OU – Organizational Unit

SIEM – Security Information and Event Management

IP – Internet Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

GUI – Graphical User Interface

VM – Virtual Machine

NAT – Network Address Translation

OS – Operating System

RAM – Random Access Memory

CPU – Central Processing Unit

VMs – Virtual Machines

NXLog – агент збору та передачі журналів подій

Winlogbeat – агент збору журналів подій Windows

Graylog – система централізованого збору та аналізу журналів подій

MongoDB – система керування базами даних

EICAR – European Institute for Computer Antivirus Research Test File

Kerberos – протокол мережевої автентифікації

Syslog – протокол передачі журналів подій

Event ID – унікальний ідентифікатор події Windows

Windows Defender – вбудована антивірусна система Microsoft Windows

Вступ

Актуальність теми. Сучасні корпоративні інформаційні системи активно використовують доменні інфраструктури на базі Microsoft Active Directory для централізованого керування обліковими записами, автентифікацією користувачів, політиками безпеки та доступом до мережевих ресурсів. Разом із розширенням функціональності доменних середовищ зростає і кількість потенційних кіберзагроз, серед яких особливу небезпеку становлять несанкціоновані спроби доступу, атаки типу brute-force, ескалація привілеїв, компрометація облікових записів та несанкціоновані зміни конфігурації домену.

Однією з важливих задач забезпечення інформаційної безпеки є своєчасне виявлення підозрілої активності та інцидентів безпеки шляхом централізованого моніторингу журналів подій. Використання систем централізованого збору та аналізу логів дозволяє автоматизувати процес виявлення аномалій, підвищити рівень контролю над станом доменної інфраструктури та скоротити час реагування на інциденти.

Актуальність теми кваліфікаційної роботи обумовлена необхідністю побудови доступного, ефективного та масштабованого рішення для безпекового моніторингу в мінімальній доменній інфраструктурі Microsoft Active Directory, що дозволяє реалізувати механізми централізованого логування, аналізу подій та виявлення потенційних загроз інформаційній безпеці.

Метою кваліфікаційної роботи є розробка та організація системи безпекового моніторингу в мінімальній доменній інфраструктурі на базі Microsoft Active Directory із забезпеченням централізованого збору журналів подій, виявлення підозрілої активності та інцидентів інформаційної безпеки.

Визначена мета обумовлює наступні завдання:

- провести аналіз сучасних підходів і засобів безпекового моніторингу доменних інфраструктур;

- спроєктувати мінімальну доменну інфраструктуру на базі Microsoft Active Directory;
- виконати розгортання доменного середовища із двома контролерами домену та клієнтською робочою станцією;
- реалізувати систему централізованого збору та аналізу журналів подій із використанням Graylog;
- налаштувати аудит подій безпеки та централізоване логування;
- реалізувати механізми виявлення інцидентів інформаційної безпеки, зокрема brute-force атак, ескалації привілеїв, підозрілих входів у систему та змін у Active Directory;
- провести тестування працездатності системи моніторингу та оцінити ефективність виявлення загроз.

Об'єктом дослідження є процес забезпечення безпеки та моніторингу подій у доменній інфраструктурі корпоративної інформаційної системи на базі Microsoft Active Directory.

Предметом дослідження є методи, засоби та технології централізованого збору журналів подій, моніторингу безпеки, аналізу подій та виявлення інцидентів інформаційної безпеки в доменному середовищі Microsoft Active Directory з використанням Graylog.

У процесі виконання кваліфікаційної роботи було розроблено проект мінімальної системи безпекового моніторингу доменної інфраструктури Microsoft Active Directory, реалізованої у віртуальному середовищі VirtualBox. Проєкт передбачає централізований збір журналів подій, моніторинг дій користувачів та адміністраторів, а також виявлення типових інцидентів інформаційної безпеки.

РОЗДІЛ 1 Теоретичні основи організації безпекового моніторингу в доменних інфраструктурах Microsoft Active Directory

1.1 Архітектура та принципи роботи Microsoft Active Directory

У сучасних корпоративних інформаційних системах одним із ключових компонентів централізованого адміністрування мережевої інфраструктури є служба каталогів Microsoft Active Directory (AD). Вона використовується для централізованого управління користувачами, комп'ютерами, мережевими ресурсами, групами безпеки, політиками доступу та механізмами автентифікації в корпоративному середовищі. Active Directory є фундаментальною складовою екосистеми операційних систем Microsoft Windows Server та широко застосовується в організаціях різного масштабу — від невеликих локальних мереж до глобальних корпоративних інфраструктур. Поява Active Directory була обумовлена необхідністю спрощення управління великою кількістю користувачів та комп'ютерів у корпоративних мережах. До впровадження AD адміністрування здійснювалось локально на кожному окремому комп'ютері, що значно ускладнювало контроль доступу та управління обліковими записами. Active Directory дозволила реалізувати централізований підхід, у межах якого всі об'єкти інфраструктури зберігаються в єдиній логічній структурі та можуть управлятися з одного адміністративного середовища.

Служба Active Directory являє собою каталогову систему, яка функціонує за принципом ієрархічної бази даних, де зберігаються відомості про мережеві об'єкти. До таких об'єктів належать користувачі, сервери, робочі станції, групи безпеки, принтери, політики безпеки та інші ресурси організації. Кожен об'єкт у каталозі має набір атрибутів, що описують його властивості, наприклад ім'я користувача, пароль, членство у групах або параметри доступу.

Основними перевагами використання Active Directory є централізоване управління, масштабованість, гнучка система делегування прав доступу, автоматизоване застосування політик безпеки та підтримка механізмів єдиної автентифікації (Single Sign-On). Це дозволяє адміністраторам істотно знизити витрати

часу на обслуговування інфраструктури та підвищити рівень інформаційної безпеки організації.

1.2 Основні компоненти Active Directory

Архітектура Microsoft Active Directory складається з декількох взаємопов'язаних компонентів, які забезпечують її функціонування. Основними логічними елементами є домени, дерева доменів, ліси, організаційні одиниці, контролери домену та служба DNS .

Домен (Domain) є базовою логічною одиницею Active Directory. Він являє собою адміністративну область, у межах якої зберігаються облікові записи користувачів, груп, комп'ютерів та інші об'єкти. Усі ресурси, що належать домену, використовують спільну базу автентифікації та централізовані правила безпеки.

Наприклад, у межах даної кваліфікаційної роботи використовується домен **corp.local**, який виступає центральною логічною одиницею тестової інфраструктури. Усі контролери домену та робочі станції входять до цього доменного середовища.

Організаційні одиниці (Organizational Units, OU) використовуються для логічного групування об'єктів домену. Вони дозволяють впорядковувати користувачів, комп'ютери та сервери відповідно до структури організації або функціонального призначення . Наприклад, можуть бути створені окремі OU для користувачів, адміністраторів, серверів та робочих станцій.

Використання організаційних одиниць забезпечує можливість делегування адміністративних прав та застосування окремих групових політик до конкретних підрозділів домену.



Рис 1.1 – Ієрархічна структура Active Directory

1.3 Домени, дерева та ліси Active Directory

Однією з ключових особливостей Active Directory є підтримка багаторівневої структури доменів.

Дерево доменів (Tree) являє собою сукупність декількох взаємопов’язаних доменів, які мають спільний простір імен DNS. Наприклад:

corp.local
it.corp.local
security.corp.local

У такому випадку дочірні домени успадковують загальну структуру іменування та довірчі відносини із батьківським доменом.

Ліс (Forest) є найвищим рівнем логічної структури Active Directory. Він об’єднує одне або декілька дерев доменів та виступає глобальною адміністративною межею безпеки . У межах одного лісу всі домени можуть довіряти один одному, а користувачі отримують можливість доступу до ресурсів згідно з наданими правами.

Для невеликих організацій, а також у межах даної кваліфікаційної роботи, використовується мінімальна структура, яка складається з одного домену в

одному лісі. Такий підхід дозволяє спростити адміністрування та мінімізувати складність конфігурації.

1.4 Роль DNS у функціонуванні Active Directory

Однією з найважливіших складових Active Directory є служба DNS (Domain Name System). Без DNS повноцінне функціонування Active Directory є практично неможливим.

DNS використовується для:

- пошуку контролерів домену;
- маршрутизації автентифікаційних запитів;
- локалізації мережевих ресурсів;
- підтримки механізмів реплікації між контролерами домену.

Коли користувач намагається увійти до домену, робоча станція звертається до DNS-сервера для визначення місцезнаходження доступного контролера домену. Після цього відбувається процес автентифікації користувача.

У більшості випадків DNS-сервер встановлюється разом із роллю Active Directory Domain Services на контролері домену. Це дозволяє інтегрувати записи Active Directory із DNS-зоною та автоматично оновлювати записи ресурсів.

Неправильна конфігурація DNS є однією з найпоширеніших причин проблем із функціонуванням домену. Зокрема можуть виникати помилки автентифікації, відсутність реплікації або неможливість входу користувачів у доменне середовище.

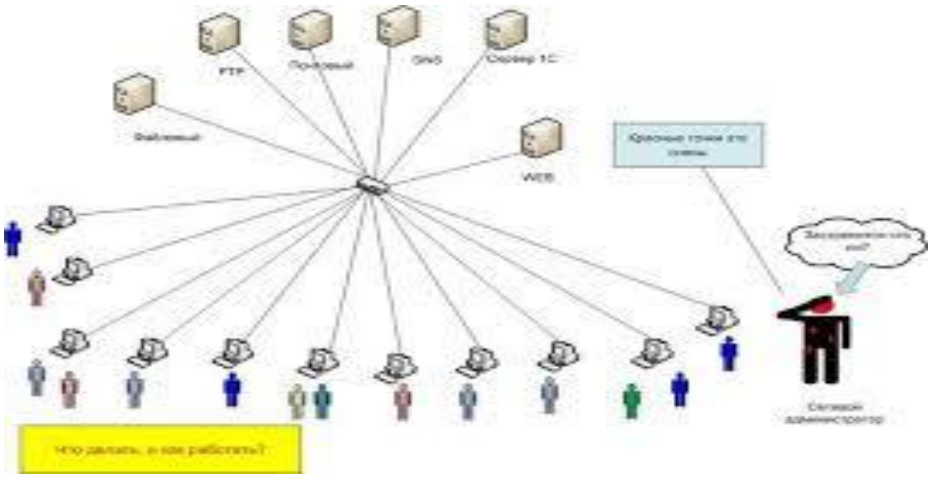


Рис 1.2 – Взаємодія DNS та Active Directory під час автентифікації користувача

1.5 Контролери домену

Контролер домену (Domain Controller, DC) — це сервер, на якому встановлена роль Active Directory Domain Services. Він відповідає за автентифікацію користувачів, авторизацію доступу, застосування політик безпеки та зберігання бази даних Active Directory .

Контролери домену є критично важливими компонентами інфраструктури, оскільки саме через них проходить більшість процесів керування доступом.

До основних функцій контролера домену належать:

- автентифікація користувачів;
- централізоване зберігання облікових записів;
- обробка запитів Kerberos;
- застосування Group Policy;
- підтримка DNS;
- реплікація інформації між контролерами.

Для забезпечення відмовостійкості рекомендується використовувати декілька контролерів домену. У межах даної роботи використовується конфігурація із двох контролерів домену, що дозволяє забезпечити резервування та реплікацію даних.

1.6 Реплікація Active Directory

Реплікація є процесом синхронізації даних між контролерами домену . Вона необхідна для забезпечення цілісності інформації в межах доменної інфраструктури.

Наприклад, якщо на одному контролері домену було створено нового користувача або змінено пароль, відповідні зміни автоматично передаються на інші контролери.

Реплікація може здійснюватися:

- внутрішньосайтово (Intrasite replication);
- міжсайтово (Intersite replication).

У невеликих мережах зазвичай використовується внутрішньосайтова реплікація, яка виконується автоматично та має мінімальні затримки.

Наявність декількох контролерів домену дозволяє мінімізувати ризики відмови окремого сервера та забезпечує високу доступність доменної інфраструктури.

1.7 Механізми Kerberos та LDAP

Одним із ключових елементів Active Directory є використання протоколу Kerberos для автентифікації користувачів.

Kerberos базується на використанні квитків (tickets), які дозволяють реалізувати безпечну автентифікацію без постійної передачі пароля мережею.

Під час входу користувача до домену відбувається наступна послідовність дій:

1. користувач вводить облікові дані;
2. клієнт звертається до контролера домену;
3. видається Ticket Granting Ticket (TGT);
4. користувач отримує доступ до ресурсів.

Такий механізм дозволяє зменшити ризики компрометації паролів та реалізувати централізовану модель доступу.

Іншим важливим протоколом є LDAP (Lightweight Directory Access Protocol), який використовується для взаємодії із каталогом Active Directory. LDAP дозволяє здійснювати пошук об’єктів, зміну атрибутів користувачів, отримання інформації про групи та інші операції.

1.8 Group Policy та централізоване адміністрування

Group Policy (GPO) є одним із найбільш потужних інструментів Active Directory. Вона дозволяє централізовано застосовувати правила конфігурації до користувачів і комп’ютерів.

За допомогою GPO можна:

- налаштовувати параметри безпеки;
- обмежувати доступ користувачів;
- встановлювати програмне забезпечення;
- конфігурувати журнали аудиту;
- керувати політиками паролів.

У межах даної роботи механізм Group Policy використовується для активації журналювання подій безпеки, необхідних для централізованого моніторингу та подальшого аналізу в системі Graylog.

1.9 Роль Active Directory у забезпеченні інформаційної безпеки

Microsoft Active Directory відіграє критично важливу роль у забезпеченні інформаційної безпеки корпоративної мережі. Саме через AD здійснюється контроль доступу до ресурсів, керування обліковими записами та застосування політик безпеки.

Разом із тим Active Directory є однією з найбільш привабливих цілей для кіберзловмисників. У разі компрометації доменного середовища зловмисник може отримати контроль над значною частиною корпоративної інфраструктури.

Тому особливої важливості набуває централізований моніторинг подій безпеки, аудит дій користувачів та своєчасне виявлення аномальної активності. Саме ці завдання реалізуються у межах даної кваліфікаційної роботи шляхом побудови системи безпекового моніторингу на базі Microsoft Active Directory та Graylog.

Висновки до розділу 1

У даному розділі було розглянуто архітектуру лабораторної доменної інфраструктури, побудованої на базі Microsoft Active Directory, визначено основні загрози інформаційній безпеці, характерні для подібних середовищ, та проаналізовано підходи до централізованого збору і аналізу журналів подій. Також було обґрунтовано вибір Graylog як інструменту моніторингу. Отримані результати формують основу для подальшої практичної реалізації системи безпекового моніторингу.

РОЗДІЛ 2 Проєктування та розгортання системи безпекового моніторингу

2.1 Проєктування архітектури лабораторної інфраструктури

У межах даної кваліфікаційної роботи було спроєктовано мінімальне лабораторне середовище, призначене для реалізації системи безпекового моніторингу на базі Microsoft Active Directory. Під час проєктування основною вимогою була можливість моделювання типових процесів корпоративної мережі, а також реалізація сценаріїв виявлення інцидентів інформаційної безпеки.

Для побудови лабораторного середовища було прийнято рішення використовувати платформу віртуалізації Oracle VirtualBox, що дозволяє створювати ізольовані мережеві середовища без необхідності використання додаткового фізичного обладнання.

Розроблена архітектура включає такі компоненти:

- **Serv-Ohrdn-1** – основний контролер домену;
- **Serv-Ohrdn-2** – резервний контролер домену;
- **WS-1-Ohrdn** – клієнтська робоча станція;
- **Ohorodniuchuk-ubunt** – сервер централізованого збору журналів подій.

Для забезпечення взаємодії між вузлами використовується окрема NAT Network у VirtualBox з адресним простором **192.168.100.0/24**.

Таблиця 2.1 – IP-адресація лабораторного середовища

Назва	IP-адреса	Роль в схемі
Serv-Ohrdn-1	192.168.100.10	Основний контролер домену
Serv-Ohrdn-2	192.168.100.11	Резервний контролер домену
WS-1-Ohrdn	192.168.100.20	Робоча станція
Ohorodniuchuk-ubunt	192.168.100.30	Сервер для збору логів

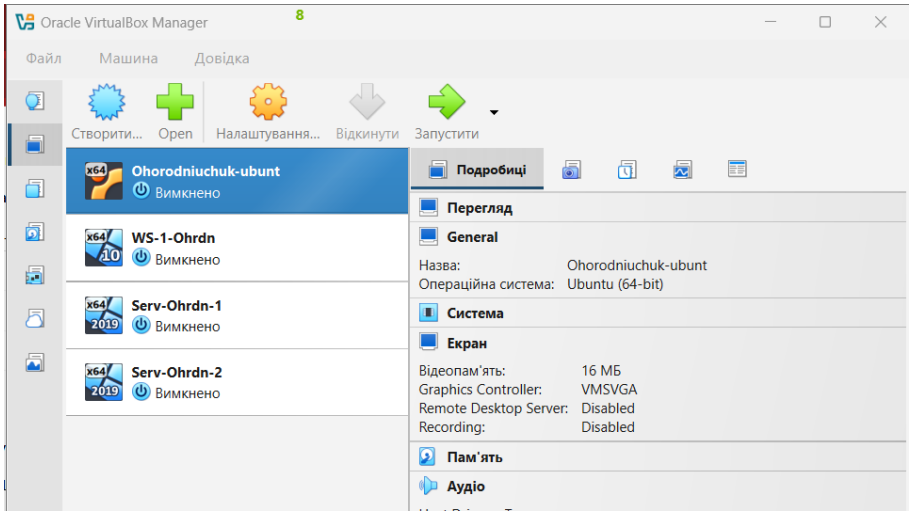


Рис 2.1 – Архітектура лабораторної мережі

2.2 Вибір програмного забезпечення та середовища віртуалізації

Для реалізації доменного середовища було обрано операційну систему Windows Server 2022 з образом готового серверу, оскільки вона містить сучасні механізми керування доменом, підтримує Active Directory Domain Services та забезпечує необхідний функціонал для аудиту подій безпеки.

На клієнтській робочій станції використовується Windows 10 , що дозволяє моделювати типовий користувацький вузол корпоративної мережі.

Для реалізації централізованого моніторингу обрано Ubuntu Server 22.04 LTS, на базі якої розгортається Graylog. Використання Linux-сервера дозволяє зменшити споживання ресурсів та забезпечити стабільну роботу системи збору логів.

Перевагами використання Graylog у межах роботи є:

- підтримка syslog;
- централізований збір журналів;
- зручний веб-інтерфейс;
- можливість побудови правил виявлення інцидентів;
- підтримка інформаційних панелей (dashboards).

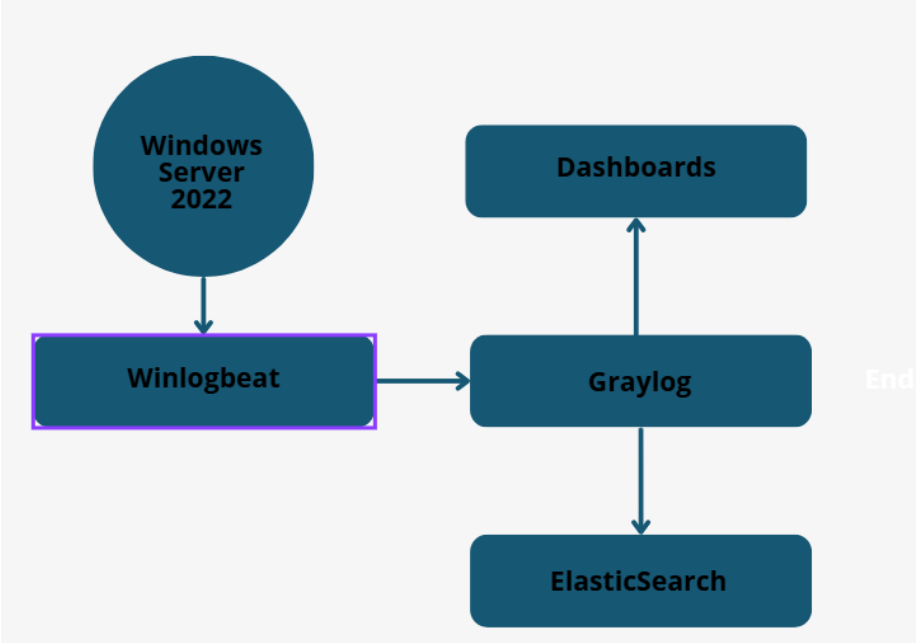


Рис.2.2 Схема архітектури збору логів

Для передачі подій із Windows-вузлів використовується агент NXLog та Winlogbeat, який виконує функції експорту журналів Windows Event Logs до сервера Graylog.

2.3 Розгортання доменної інфраструктури Microsoft Active Directory

Після створення віртуального середовища було виконано налаштування доменної інфраструктури.

На сервері **Serv-Ohrdn-1** було встановлено роль **Active Directory Domain Services (AD DS)** та створено домен **corp.local**. Додатково встановлено DNS-сервер, який використовується для локалізації контролерів домену та підтримки функціонування Active Directory.

На сервері **Serv-Ohrdn-2** виконано підключення до існуючого домену та встановлено роль додаткового контролера домену. Така конфігурація забезпечує:

- реплікацію бази Active Directory;
- резервування механізмів автентифікації;
- підвищення відмовостійкості середовища.

Клієнтська робоча станція **WS-1-Ohrdn** була приєднана до домену для моделювання типової поведінки користувача в корпоративній мережі.

Після розгортання домену було створено:

- тестові облікові записи користувачів;
- групи безпеки;
- організаційні одиниці (OU);
- політики доменної безпеки.

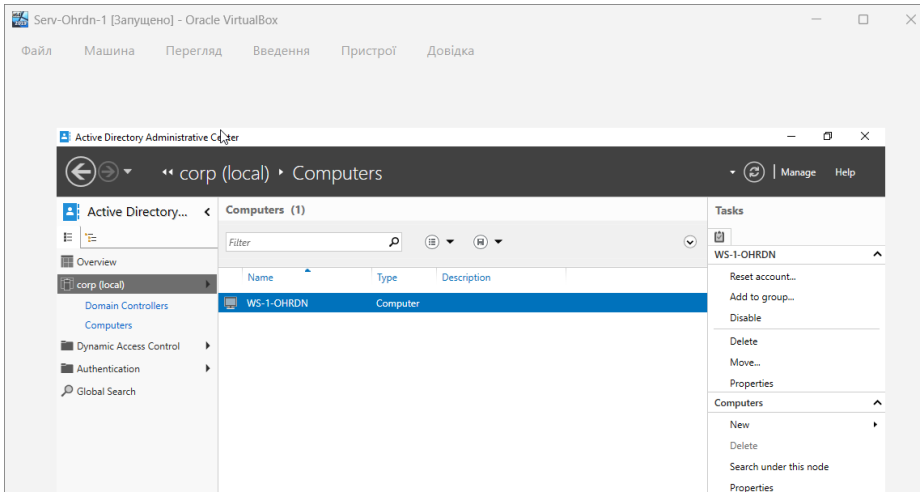


Рис 2.3 – Структура домену corp.local компютери

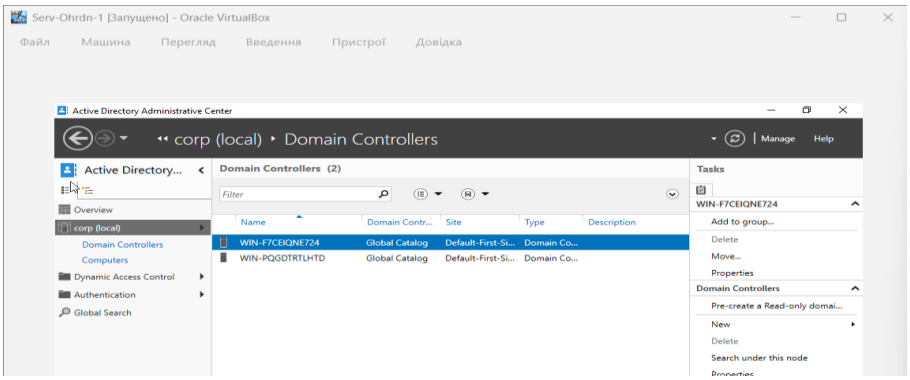


Рис 2.4 – Структура домену corp.local контролери домену

2.4 Розгортання системи централізованого моніторингу Graylog

Для реалізації централізованого збору журналів подій було розгорнуто сервер Graylog на базі Ubuntu Server.

Архітектура рішення включає:

- Graylog Server — система обробки логів;
- OpenSearch — механізм індексації даних;
- MongoDB — сховище конфігурацій Graylog.

На Windows-вузлах встановлено агент NXLog та Winlogbeat, який виконує передачу журналів подій Windows до Graylog.

У межах роботи налаштовано збір наступних категорій подій:

- успішні входи в систему (Event ID 4624);
- невдалі входи (Event ID 4625);
- зміни користувачів (4720, 4726);
- зміни привілеїв (4728);
- адміністративні входи (4672).

Додатково реалізовано механізми виявлення:

- brute-force атак;
- privilege escalation;
- підозрілих входів;
- тестових файлових загроз (EICAR).

Після завершення конфігурації було створено інформаційні панелі моніторингу для відображення активності доменного середовища.

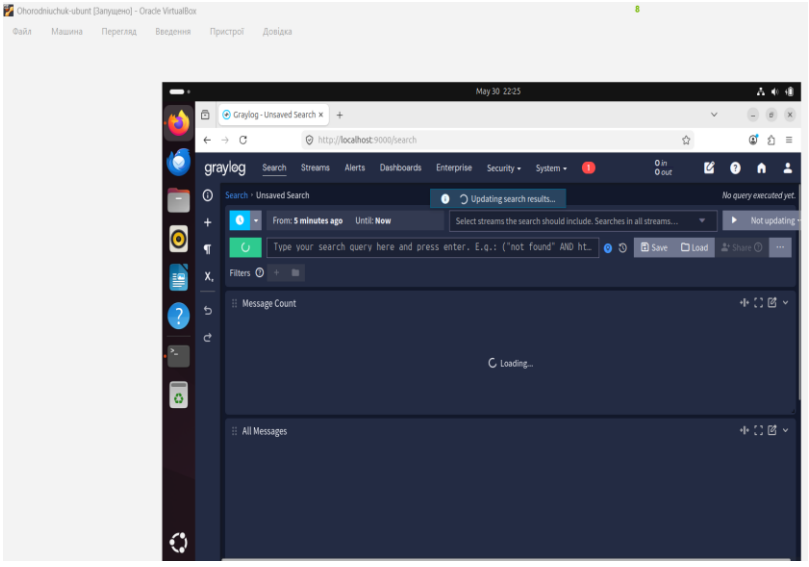


Рис 2.5 – Інтерфейс системи Graylog

Висновки до розділу 2

У другому розділі було виконано проєктування та реалізацію лабораторного середовища для побудови системи безпекового моніторингу. Обґрунтовано вибір програмного забезпечення та платформи віртуалізації, розгорнуто доменну інфраструктуру Microsoft Active Directory та реалізовано систему централізованого збору журналів подій на базі Graylog. Отримане середовище дозволяє перейти до практичного етапу тестування механізмів виявлення інцидентів інформаційної безпеки.

3.1 Підготовка серверної інфраструктури до моніторингу

Після завершення розгортання доменної інфраструктури було виконано підготовку серверів до інтеграції із системою централізованого моніторингу. На цьому етапі основною задачею було забезпечення стабільної мережевої взаємодії між усіма компонентами лабораторного середовища та перевірка коректності роботи служб Active Directory.

На кожній віртуальній машині було налаштовано статичні IP-адреси відповідно до розробленої схеми адресації. Використання статичних адрес є обов'язковою умовою для коректної роботи доменної інфраструктури, оскільки зміна мережевих параметрів може призвести до порушення роботи DNS та механізмів автентифікації.

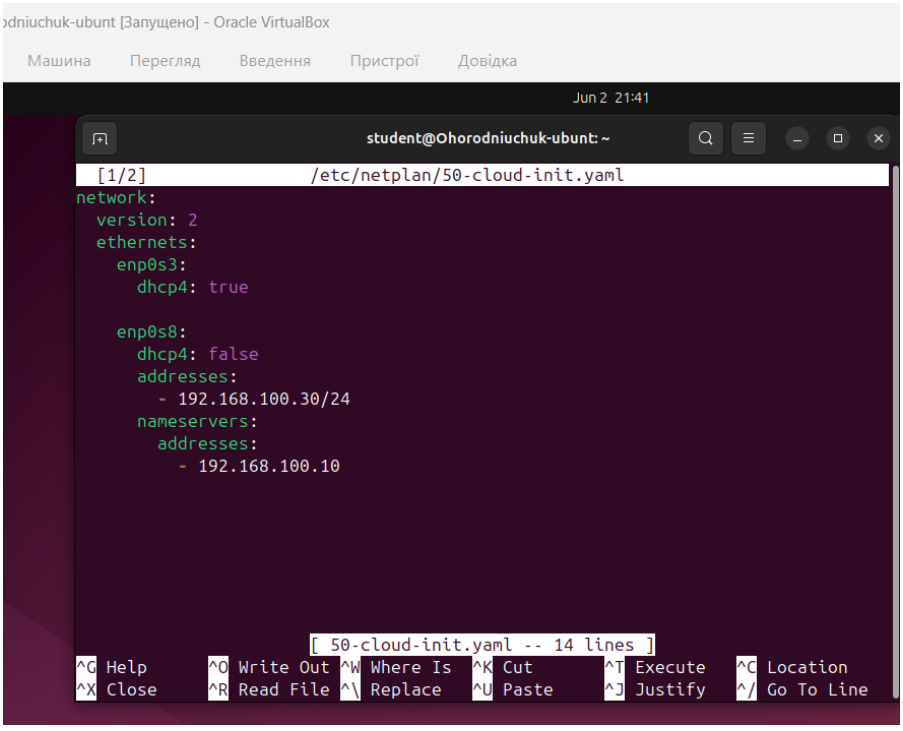


Рис.3.1. Налаштування мережі Ubuntu-Server(Ohorodniuchuk-ubunt)

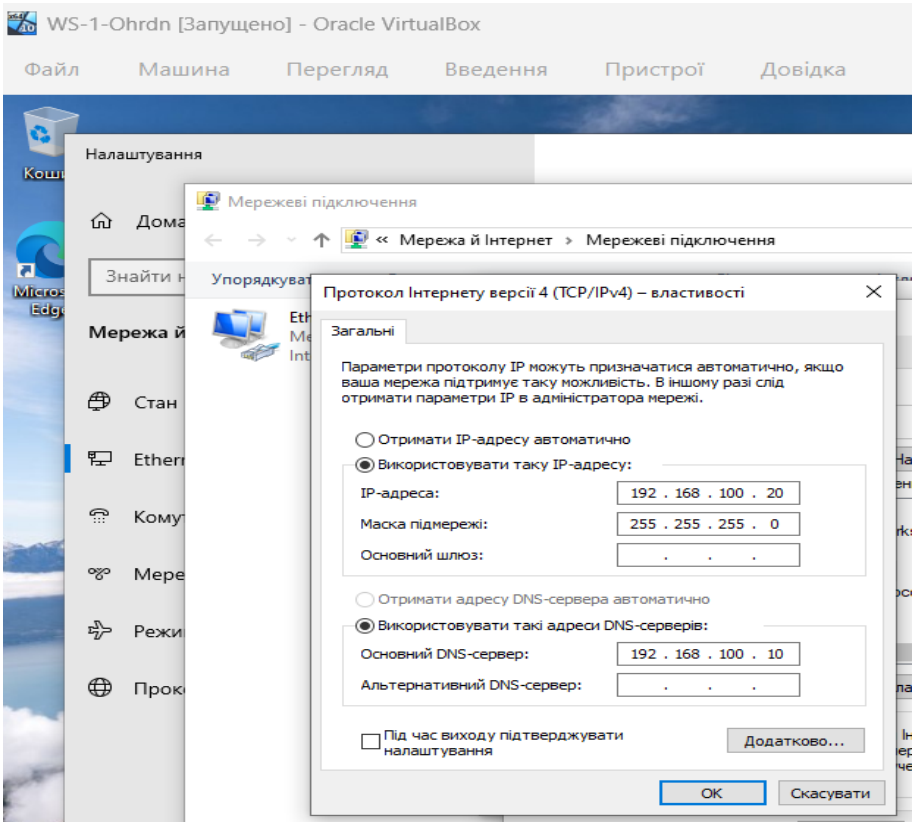


Рис.3.2.Налаштування мережі робочої станції (WS-1-Ohrdn)

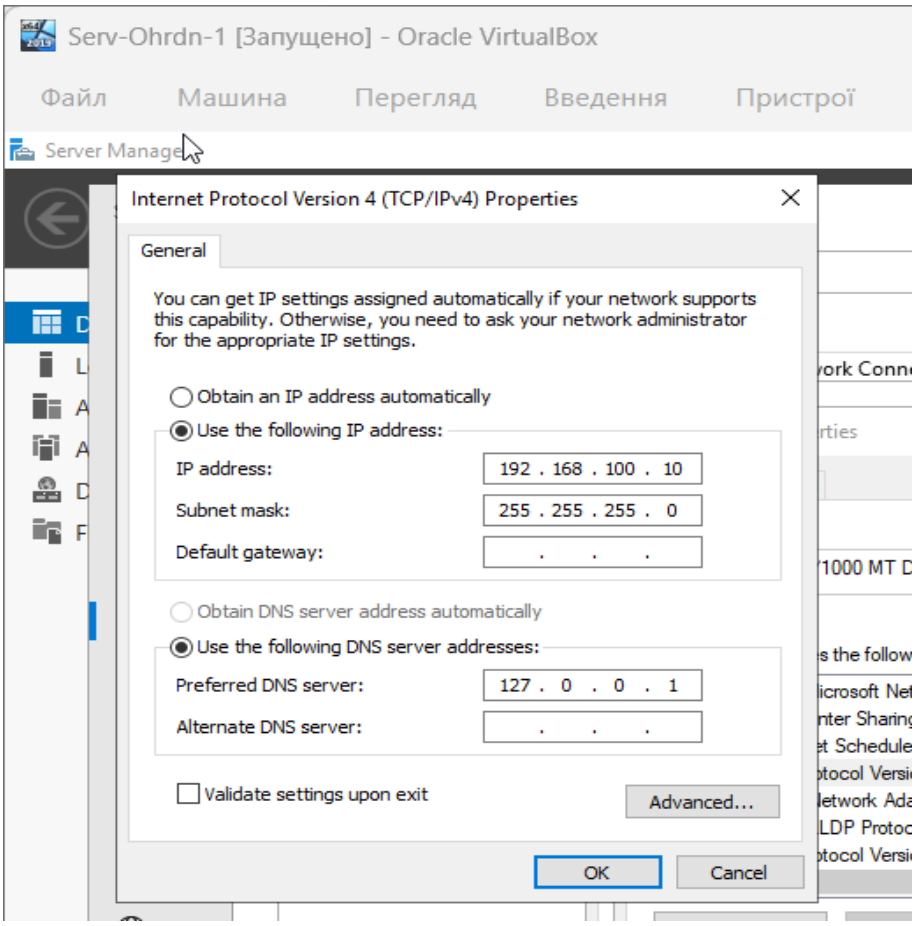


Рис.3.3.Налаштування мережі контролера домену (Serv-Ohrdn-1)

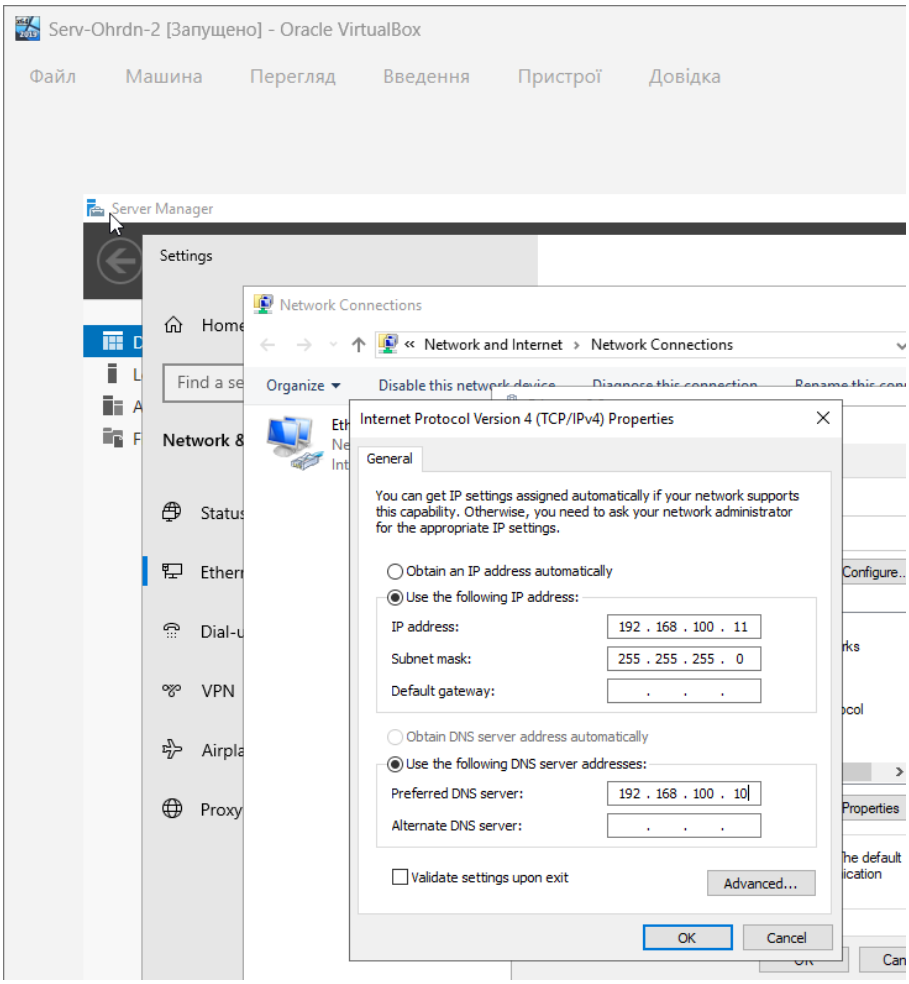


Рис.3.4.Налаштування мережі резервного контролера домену (Serv-Ohrdn-2)

Після налаштування мережі було виконано перевірку доступності вузлів за допомогою утиліти ping. Усі сервери успішно відповідали на ICMP-запити, що підтвердило працездатність мережевої взаємодії між компонентами інфраструктури.

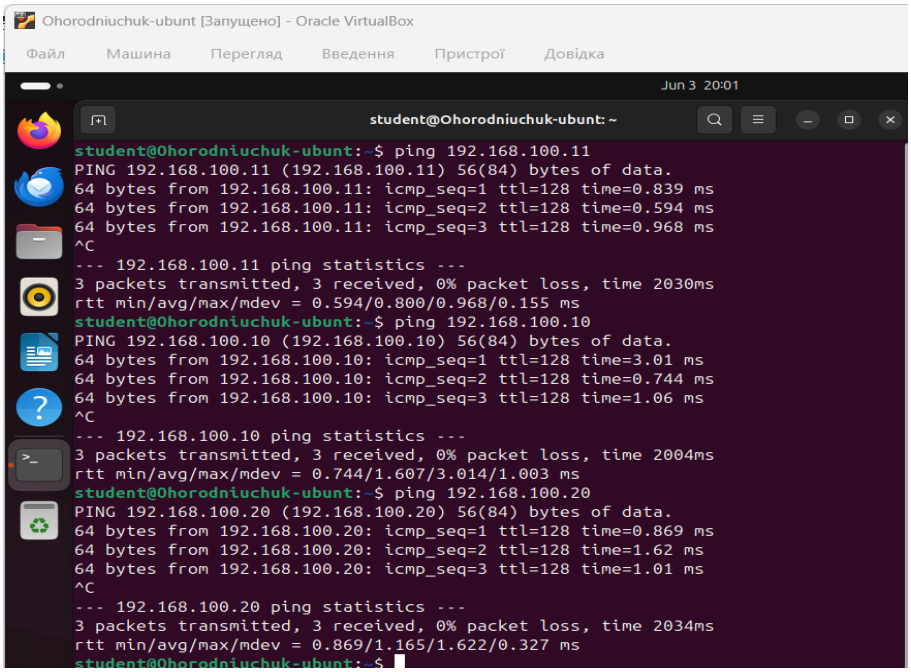


Рис.3.5 Перевірка звязку між контролерами домену сервера ubuntu

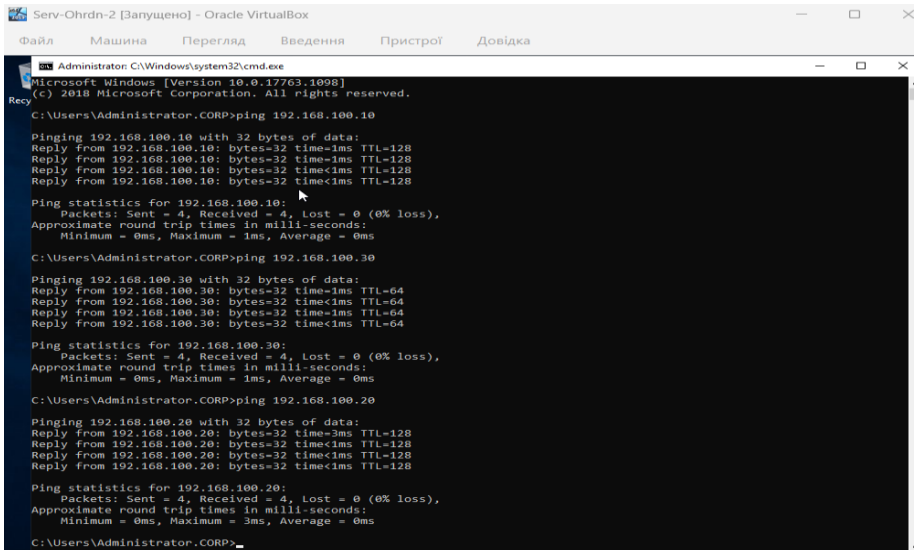


Рис.3.6 Перевірка звязку між пристроями домену з резервного контролеру

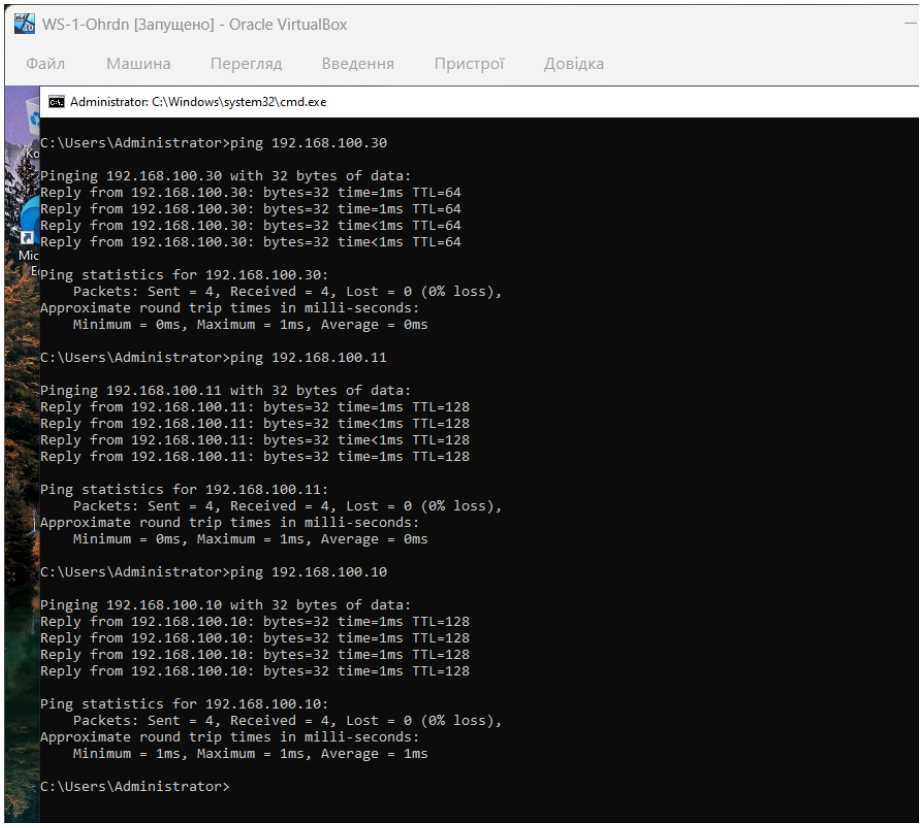


Рис.3.7 Перевірка звязку між пристроями домену з робочої станції

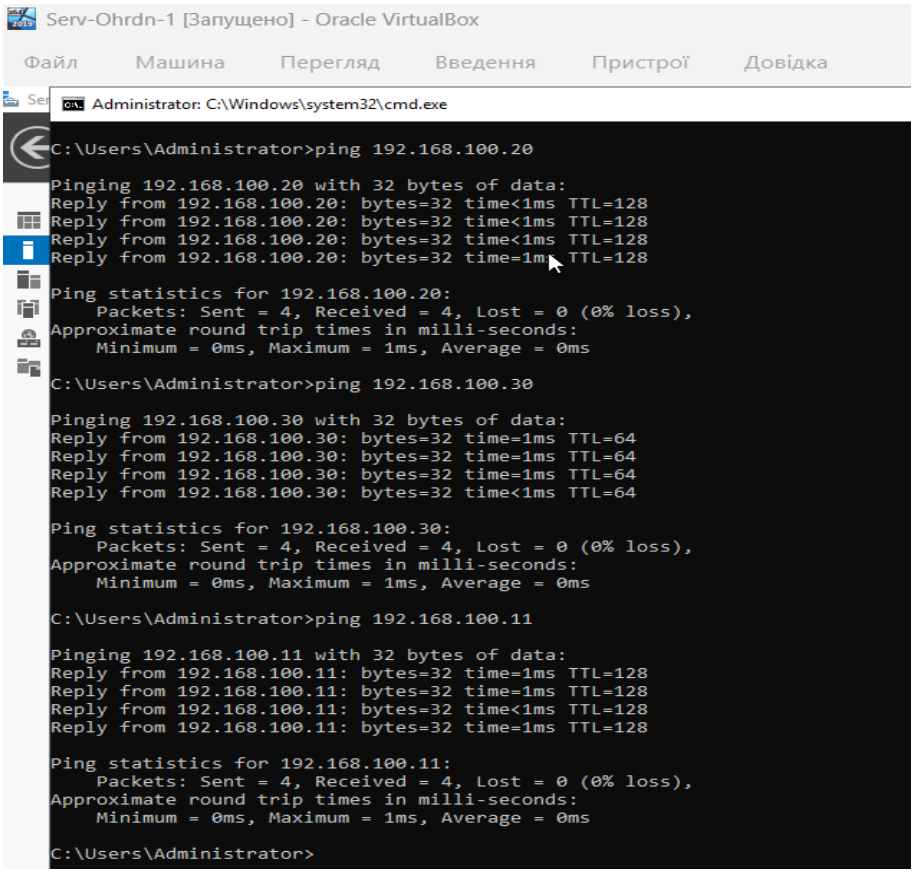


Рис.3.8 Перевірка звязку між пристроями домену з головного контролеру

Додатково було перевірено:

- коректність DNS-резолюції;
- доступність контролерів домену;
- синхронізацію часу;
- реплікацію між WS-1-Ohrdn та WS-2-Ohrdn.

Синхронізація часу є особливо важливою для роботи Kerberos, оскільки відхилення системного часу може призвести до помилок автентифікації.

3.2 Налаштування сервера централізованого збору логів Graylog

Для реалізації функцій моніторингу був використаний окремий сервер Ubuntu Server 22.04 LTS, на якому розгорнуто Graylog.

На початковому етапі було виконано оновлення системи та встановлення необхідних залежностей. Після цього були встановлені компоненти MongoDB та elasticSearch, які використовуються Graylog для зберігання конфігураційних даних та індексації журналів подій.

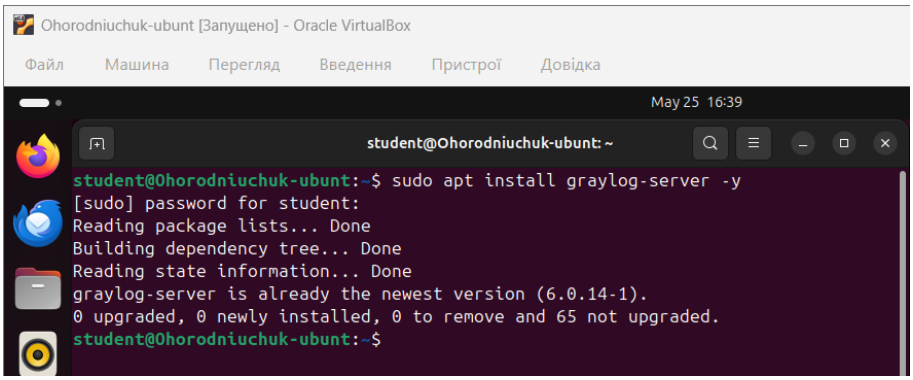


Рис.3..9 Встановлення Graylog

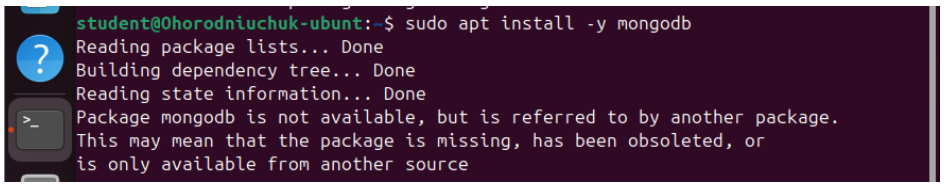


Рис.3..10 Встановлення Mongodb

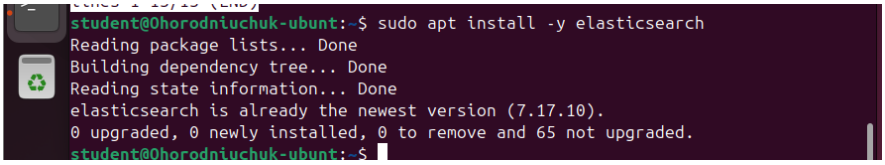


Рис.3..11 Встановлення ElasticSearch

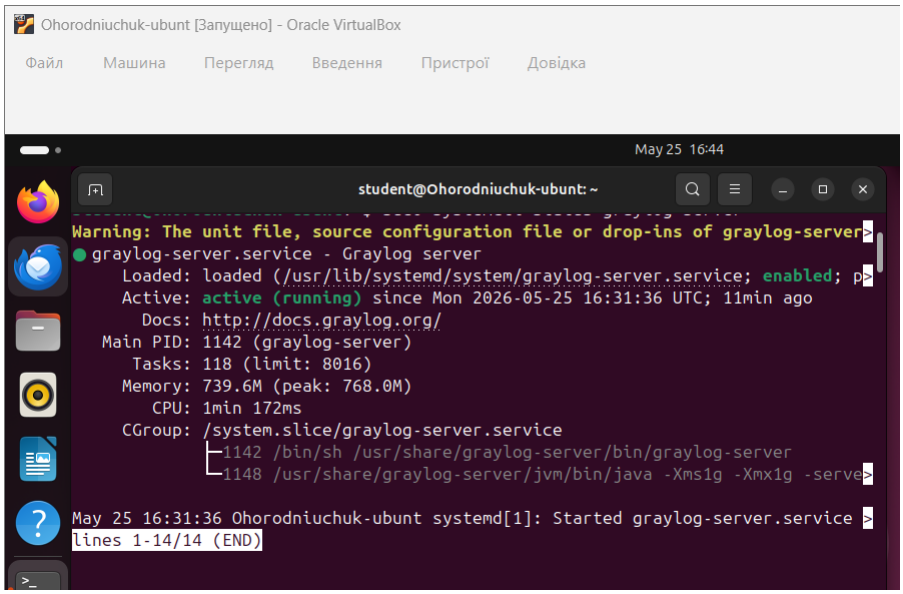


Рис.3..12 Перевірка статусу Graylog

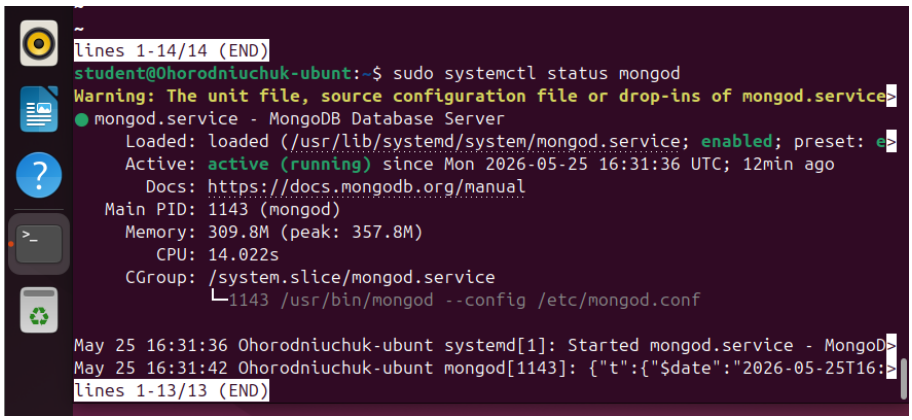


Рис.3..13 Перевірка статусу Mongodb

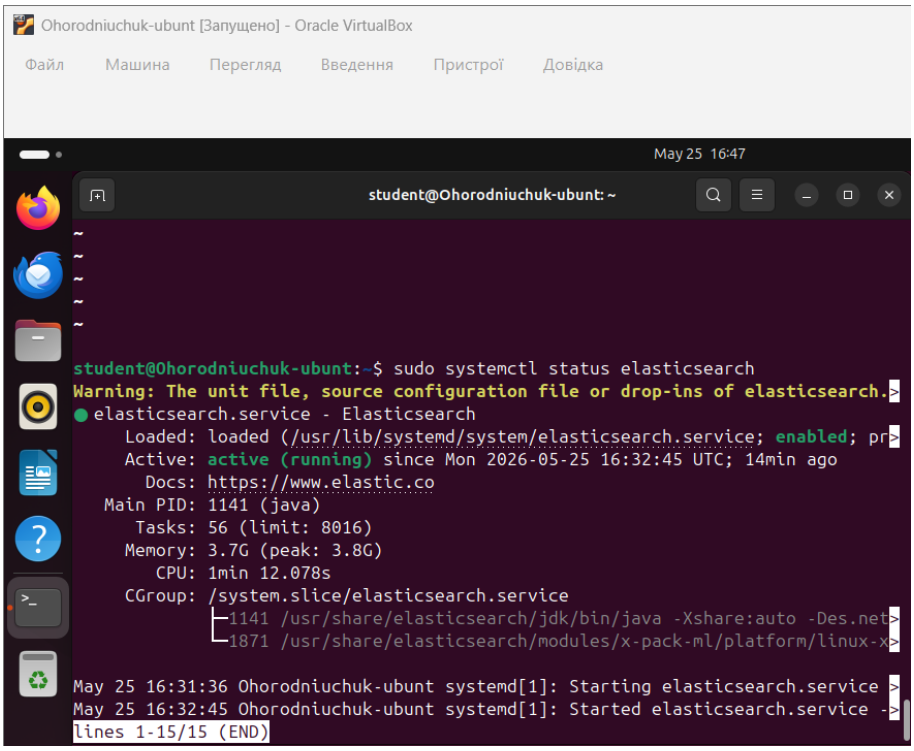


Рис.3..13 Перевірка статусу ElasticSearch

Після завершення інсталяції було налаштовано веб-інтерфейс Graylog та перевірено доступність сервера через браузер.

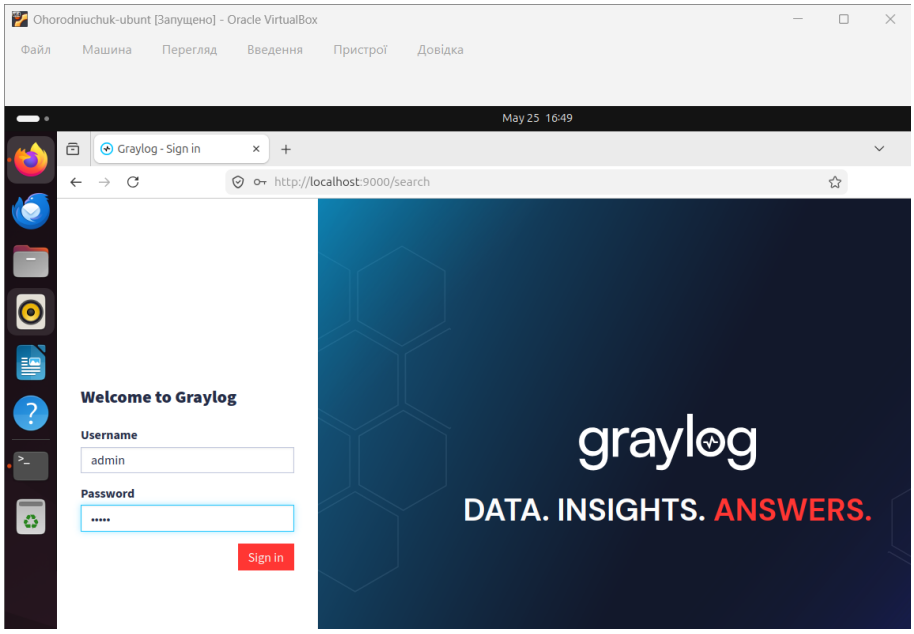


Рис.3.14. Перевірка роботи Graylog

Для прийому повідомлень від агентів збору логів було створено Windows Input. Даний механізм забезпечує прийом повідомлень від усіх вузлів лабораторного середовища.

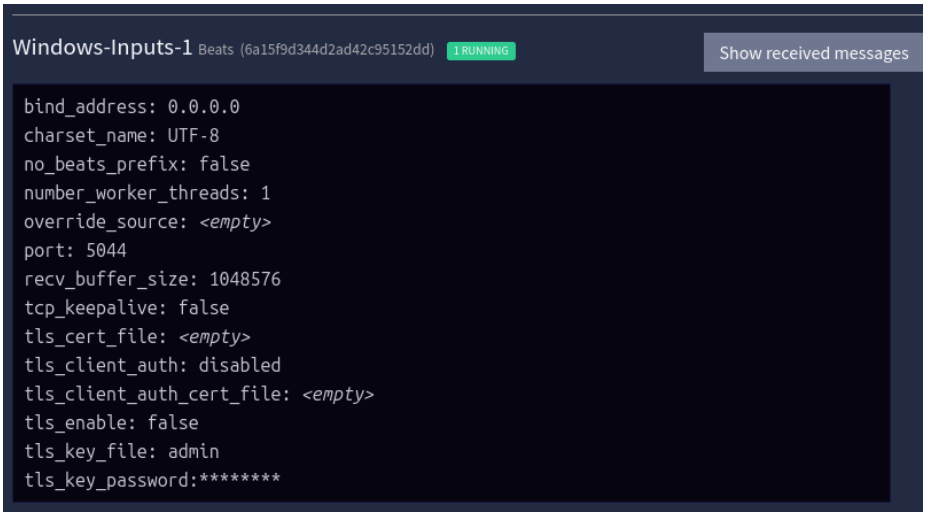


Рис.3.15. Налаштування Windows Input

На цьому ж етапі було налаштовано:

- часовий пояс;
- індекси зберігання логів;
- правила ротації журналів;
- обмеження на обсяг збережених даних.

Після завершення налаштування виконано тестову відправку повідомлень для перевірки працездатності системи.

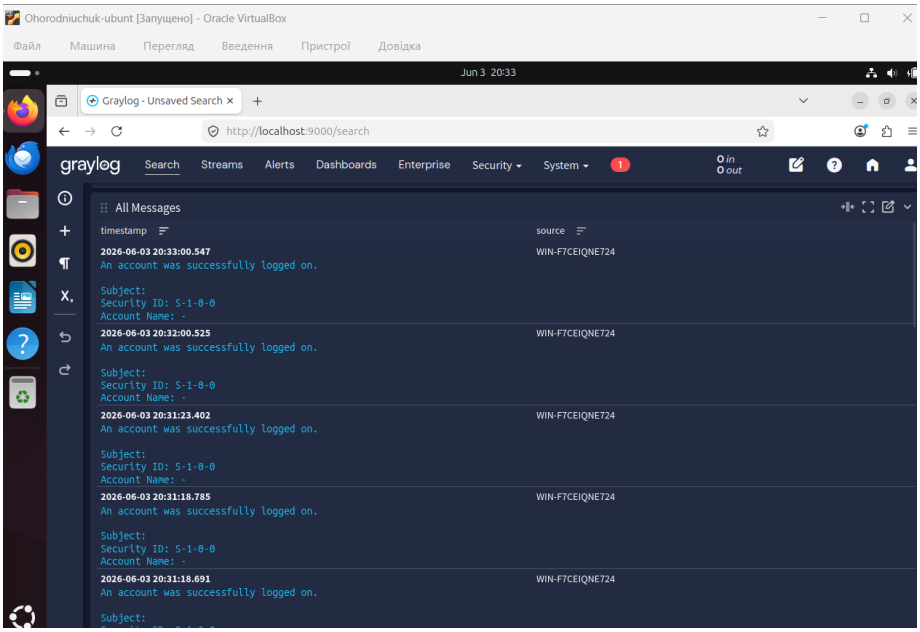


Рис.3.16. Перевірка працездатності системи

3.3 Налаштування збору журналів подій Windows

Для забезпечення централізованого збору журналів подій було реалізовано передачу логів з усіх вузлів доменної інфраструктури до сервера Graylog. У процесі побудови системи використовувалися різні агенти збору подій залежно від призначення вузла.

На контролерах домену Serv-Ohrdn-1 та Serv-Ohrdn-2 було встановлено агент **Winlogbeat**, який призначений для отримання подій із журналів Windows Event Log та їх подальшої передачі на сервер моніторингу. Використання Winlogbeat дозволяє гнучко налаштовувати перелік журналів та типів подій, що передаються до системи аналізу.

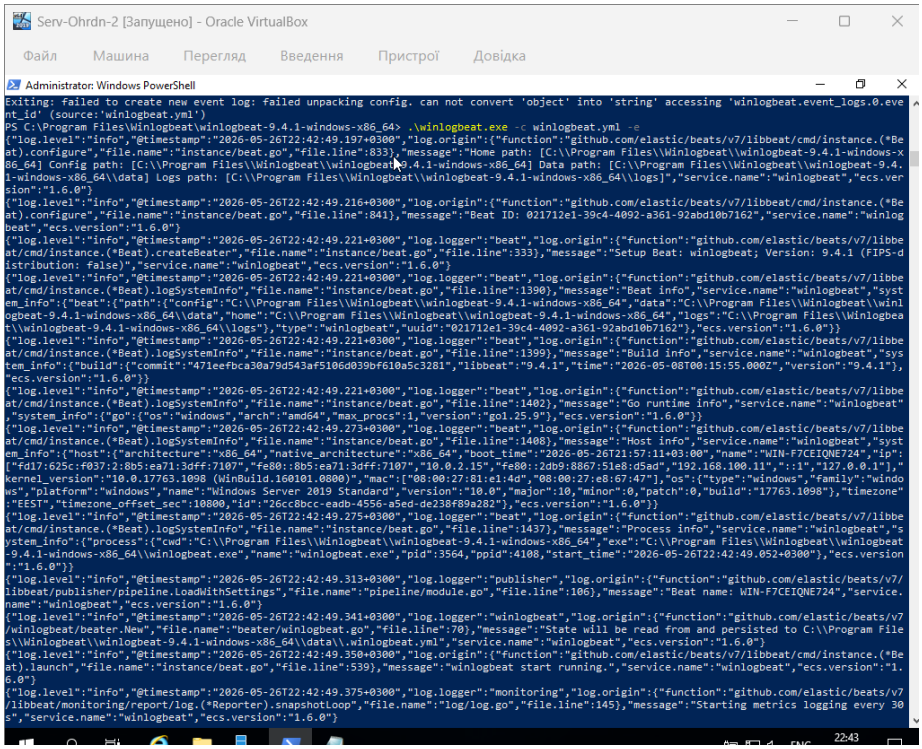


Рис.3.17 Налаштування winlogbeat на Serv-Ohrdn-2

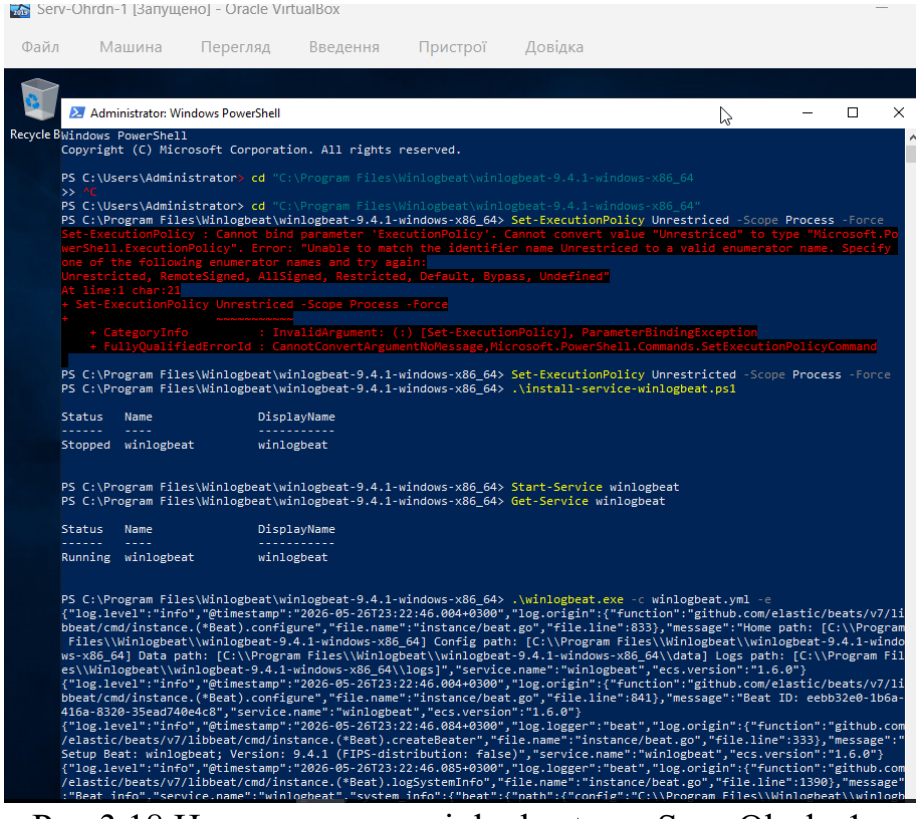


Рис.3.18 Налаштування winlogbeat на Serv-Ohrdn-1

На клієнтській робочій станції WS-1-Ohrdn було використано агент **NXLog**, який забезпечує збір подій із журналів операційної системи Windows та їх надсилання до Graylog через протокол Syslog.

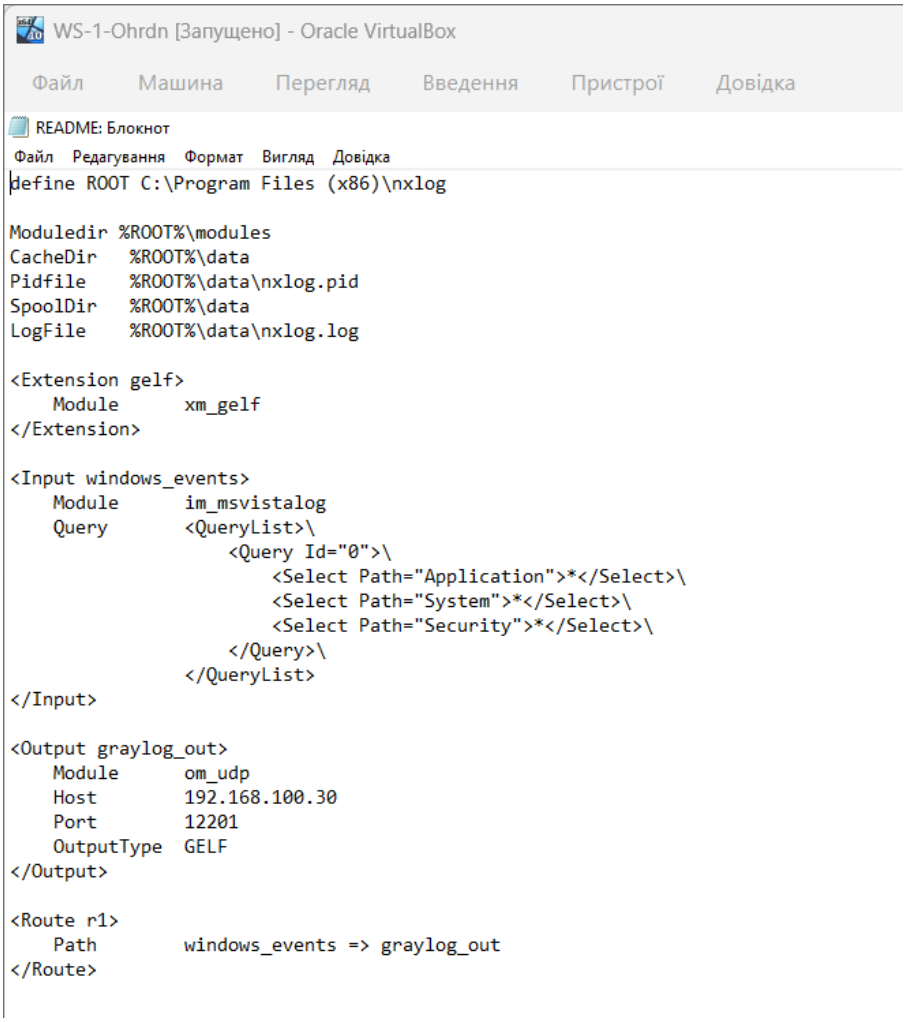


Рис.3.19 Налаштування Nxlog на робочій станції

Перед початком передачі журналів було створено відповідні Inputs на сервері Graylog для приймання повідомлень від агентів збору логів. Після цього виконано налаштування конфігураційних файлів агентів.

Для моніторингу були обрані такі журнали Windows:

- Security;
- System;
- Application;
- Microsoft-Windows-Windows Defender/Operational.

Основна увага приділялася журналу **Security**, оскільки саме він містить інформацію про події автентифікації, зміни облікових записів та використання привілейованих прав доступу.

Для перевірки працездатності системи було виконано генерацію тестових подій на всіх вузлах домену. Під час перевірки створювалися невдалі спроби входу до системи, зміни параметрів облікових записів та адміністративні операції.

Після надходження повідомлень до Graylog було виконано аналіз отриманих даних. У результаті встановлено, що журнали з контролерів домену та клієнтської станції успішно передаються на сервер моніторингу та доступні для подальшої обробки.

Для додаткової перевірки було здійснено пошук за ідентифікаторами подій безпеки Windows. Система коректно відобразила події:

- Event ID 4624 (успішний вхід);
- Event ID 4625 (невдалий вхід);
- Event ID 4672 (вхід із привілейованими правами);
- Event ID 4720 (створення користувача);
- Event ID 4728 (додавання користувача до групи).

Отримані результати підтвердили працездатність реалізованої системи централізованого збору журналів подій та готовність інфраструктури до подальшого тестування механізмів виявлення інцидентів інформаційної безпеки.

3.4 Налаштування аудиту Active Directory

Для забезпечення збору максимальної кількості подій безпеки було виконано налаштування політик аудиту через Group Policy Management.

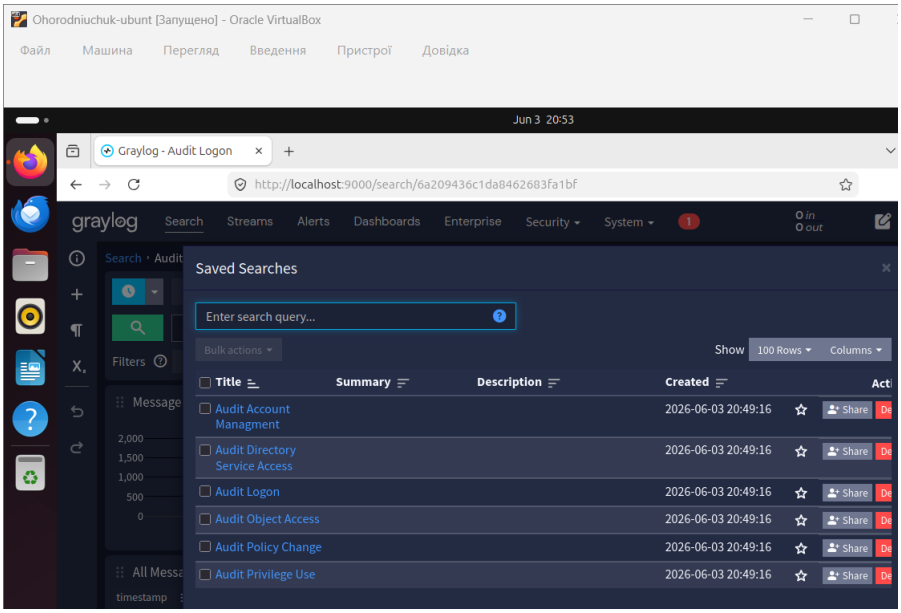


Рис.3.20 Налаштування політик аудиту через Group Policy Management

У межах домену було активовано аудит таких категорій:

- Audit Logon;
- Audit Account Management;
- Audit Policy Change;
- Audit Privilege Use;
- Audit Object Access;
- Audit Directory Service Access.

Після застосування політик на всіх вузлах домену було виконано примусове оновлення налаштувань.

З метою перевірки коректності роботи аудиту були виконані тестові операції:

- створення нового користувача;

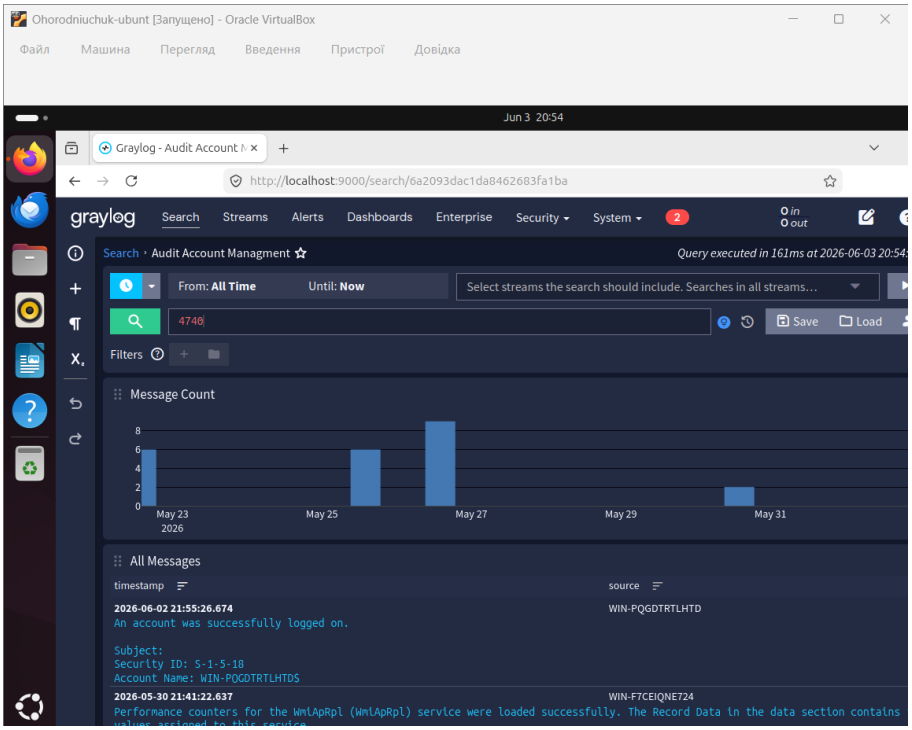


Рис.3.21 Тестова операція створення нового користувача

- зміна пароля;

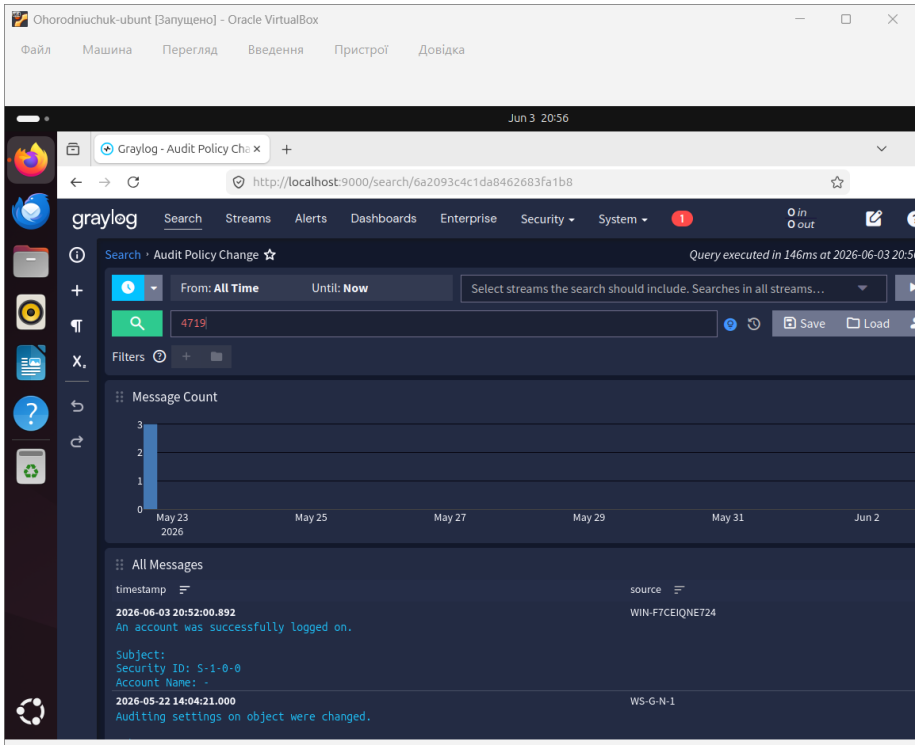


Рис.3.22 Тестова операція зміна пароля

- блокування облікового запису;

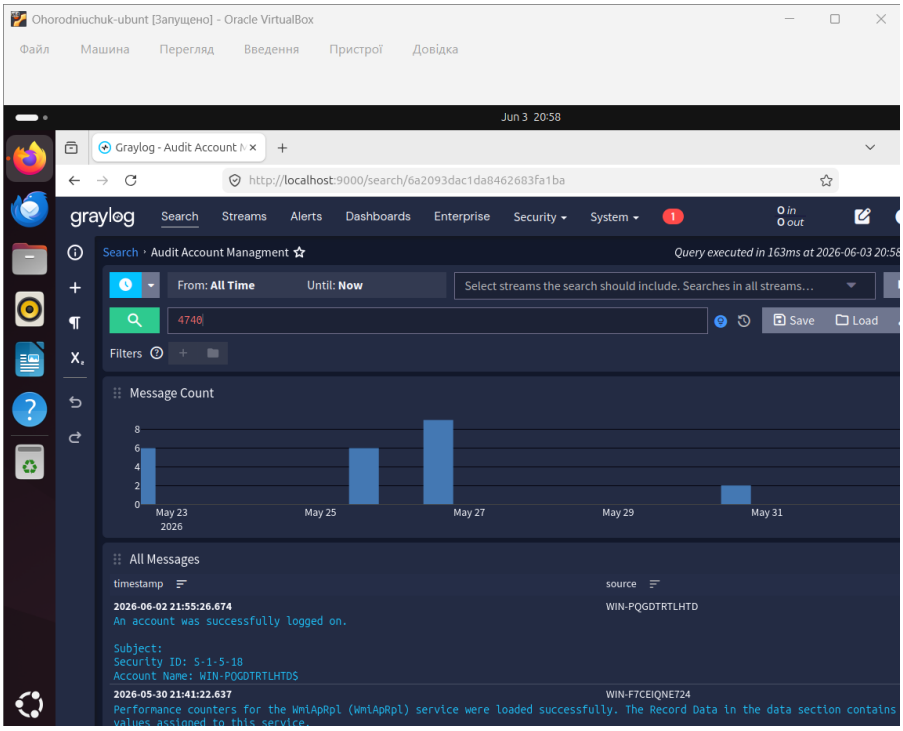


Рис.3.23 Тестова операція блокування облікового запису

- додавання до групи Domain Admins.

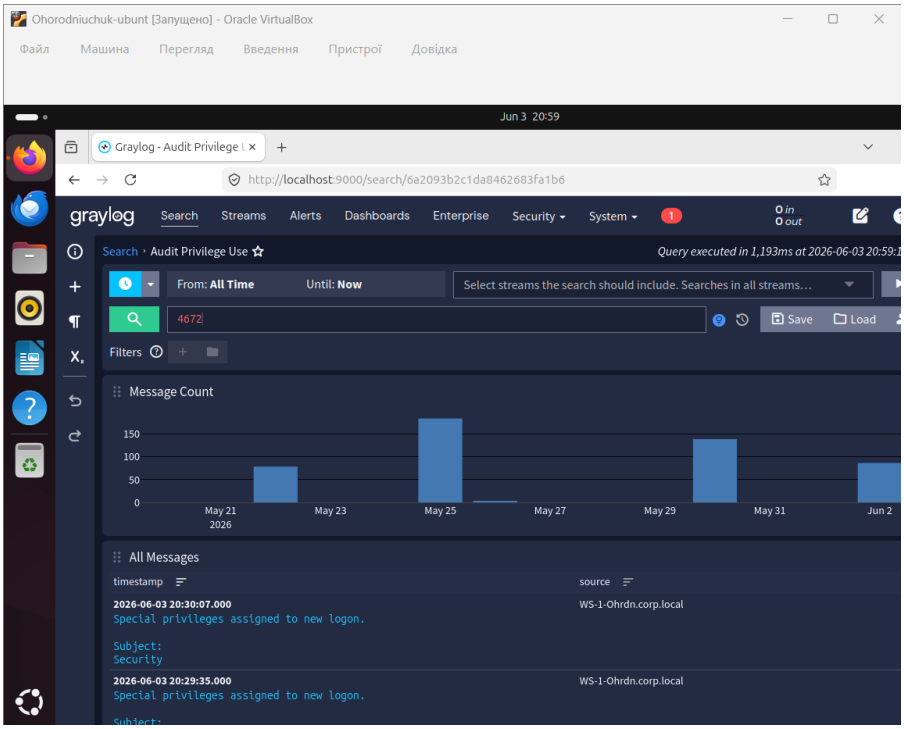


Рис.3.21 Тестова операція додавання до групи Domain Admins

Кожна з виконаних операцій успішно відобразилась у журналі Security та була передана до Graylog.

3.5 Реалізація сценаріїв виявлення інцидентів безпеки

Після завершення налаштування збору журналів було реалізовано набір правил для виявлення типових інцидентів інформаційної безпеки.

Виявлення brute-force атак

Для моделювання атаки було виконано серію невдалих спроб входу під тестовим обліковим записом.

У результаті в журналі Security були сформовані події Event ID 4625.

Graylog успішно зафіксував появу великої кількості однакових подій за короткий проміжок часу, що дозволило визначити можливу атаку перебору пароля.

Контроль привілейованих входів

Для моніторингу адміністративної активності використовувалися події Event ID 4672.

Після входу під обліковим записом адміністратора відповідні записи були отримані сервером моніторингу та відображені на інформаційній панелі.

Контроль змін у домені

Додатково реалізовано моніторинг подій створення та модифікації облікових записів.

Було перевірено:

- створення користувача;
- видалення користувача;
- зміну властивостей облікового запису;
- зміну членства в групах.

Усі події були успішно зафіксовані.

3.6 Формування інформаційних панелей моніторингу

Для підвищення зручності аналізу було створено декілька інформаційних панелей (Dashboards).

На панелях відображалися:

- кількість успішних входів;
- кількість невдалих входів;
- події створення користувачів;
- адміністративна активність;
- події Windows Defender.

Використання панелей дозволило оперативно оцінювати поточний стан безпеки доменного середовища та швидко виявляти аномалії.

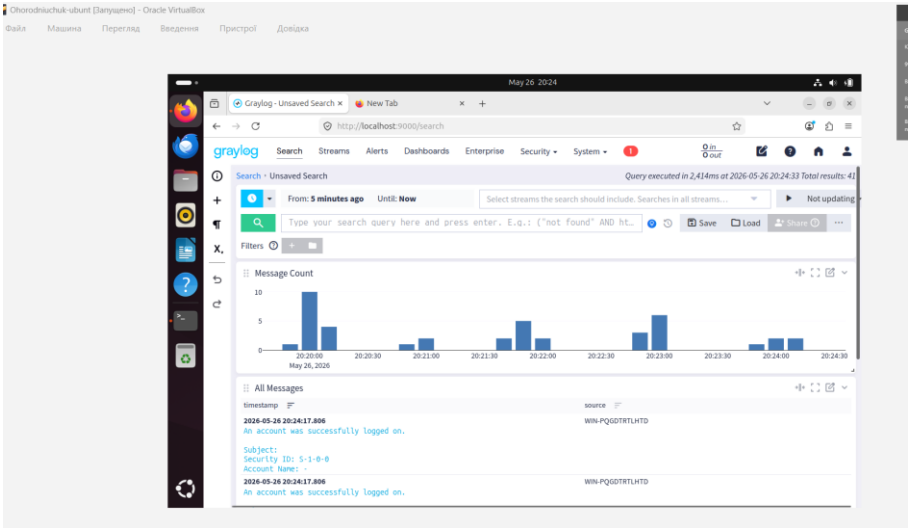


Рис.3.22 Оцінка поточного стану безпеки

3.7 Аналіз отриманих результатів

У ході тестування було підтверджено коректну роботу всіх компонентів створеної системи.

Результати показали, що розроблена інфраструктура забезпечує:

- централізований збір логів;
- збереження подій безпеки;
- контроль автентифікації;
- виявлення змін у домені;
- моніторинг діяльності адміністраторів;
- контроль подій антивірусного захисту.

Отримані дані підтверджують ефективність використання Graylog як інструменту моніторингу в невеликих доменних інфраструктурах.

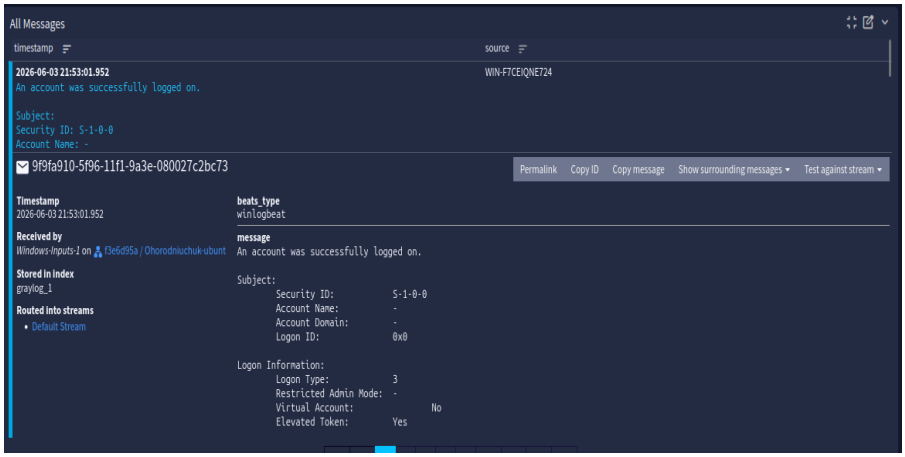


Рис.3.23 Дані про успішний вхід



Рис.3.24 Дані про невдалий вхід

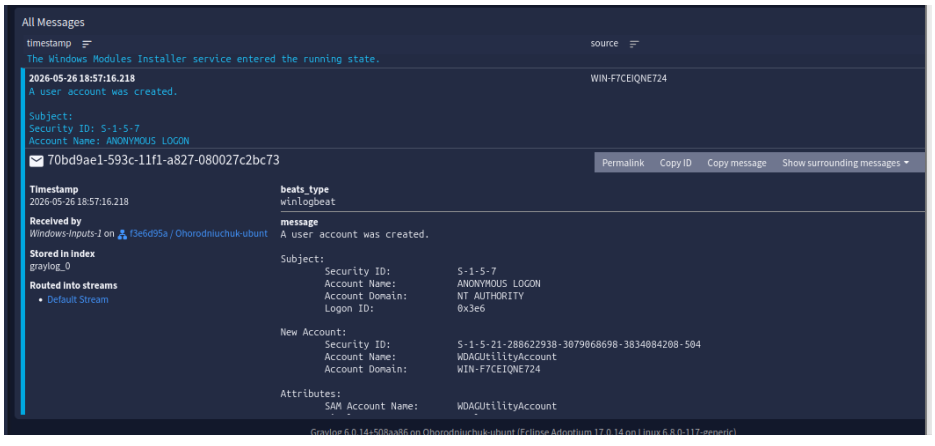


Рис.3.25 Дані про створення користувача

Висновки до розділу 3

У третьому розділі було виконано повний цикл налаштування та тестування системи безпекового моніторингу. Налаштовано сервер Graylog, агенти збору

логів NXLog, політики аудиту Active Directory та механізми виявлення інцидентів. Проведене тестування підтвердило можливість ефективного контролю подій безпеки в доменному середовищі та своєчасного виявлення типових загроз інформаційній безпеці.

РОЗДІЛ 4 Реалізація механізмів виявлення інцидентів та оцінка ефективності системи

4.1 Реалізація правил виявлення та кореляції подій безпеки

Для моніторингу спроб підбору паролів у системі Graylog налаштовано правило оповіщення на основі подій журналу безпеки Windows Event ID 4625 (невдалий вхід). Якщо протягом 5 хвилин фіксується понад 10 таких подій від одного джерела, система автоматично генерує сповіщення про brute-force атаку.

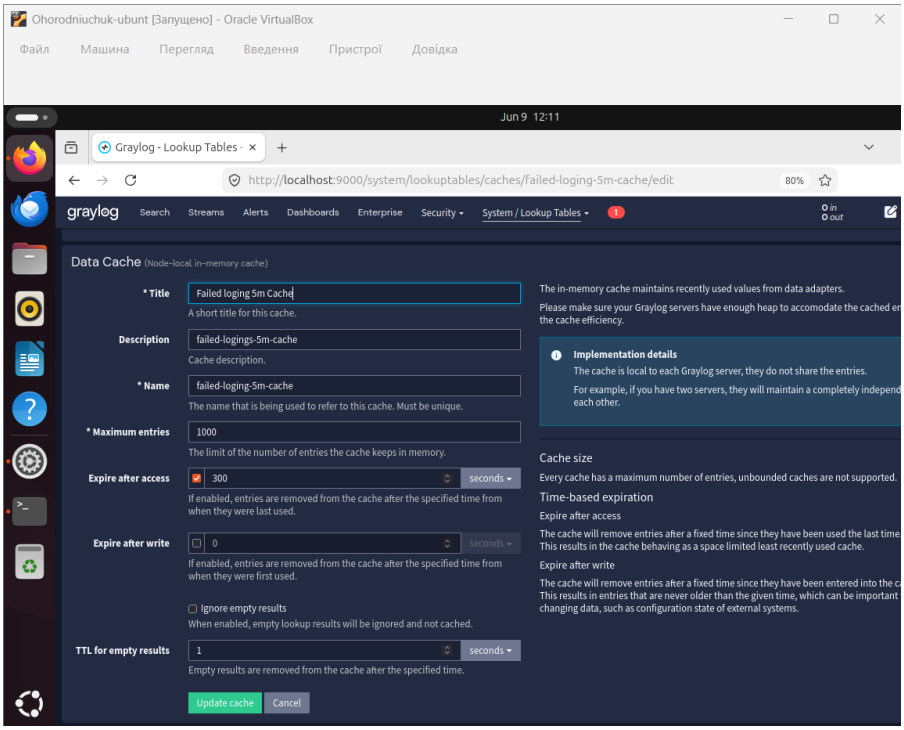


Рис.4.1 Налаштування правила

Для мінімізації хибних спрацьовувань реалізовано кореляційне правило, яке відстежує паттерн успішного входу після серії невдач: 4625 → 4625 → 4625 → 4624 (де Event ID 4624 — успішна автентифікація). Така послідовність сигналізує про ймовірну компрометацію облікового запису. Працездатність обох механізмів успішно підтверджена під час практичного тестування за допомогою симуляції відповідних загрозових сценаріїв.

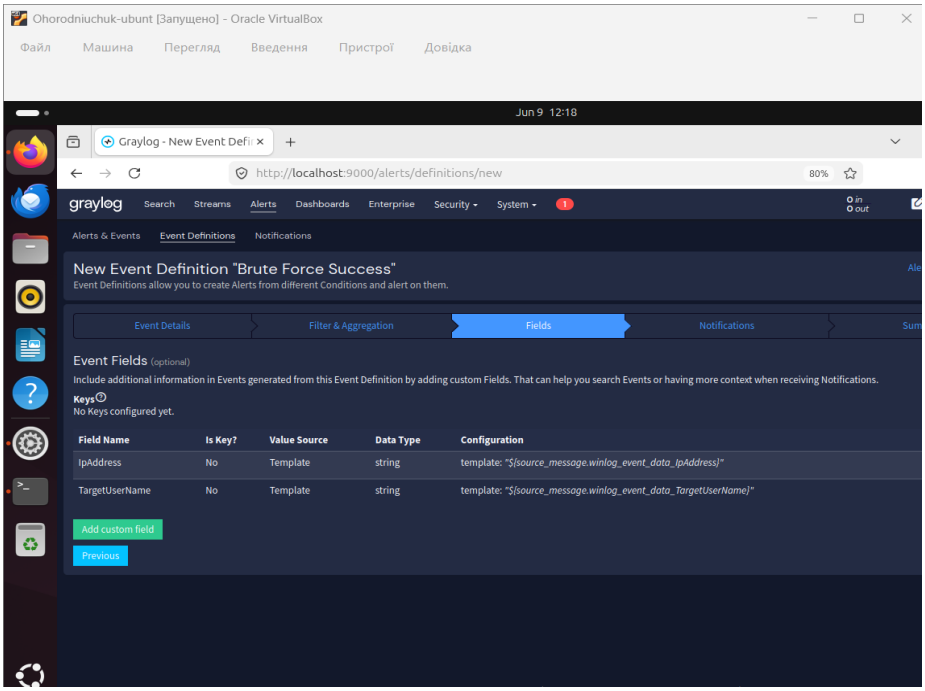


Рис.4.2 Створенно кореляційне правило

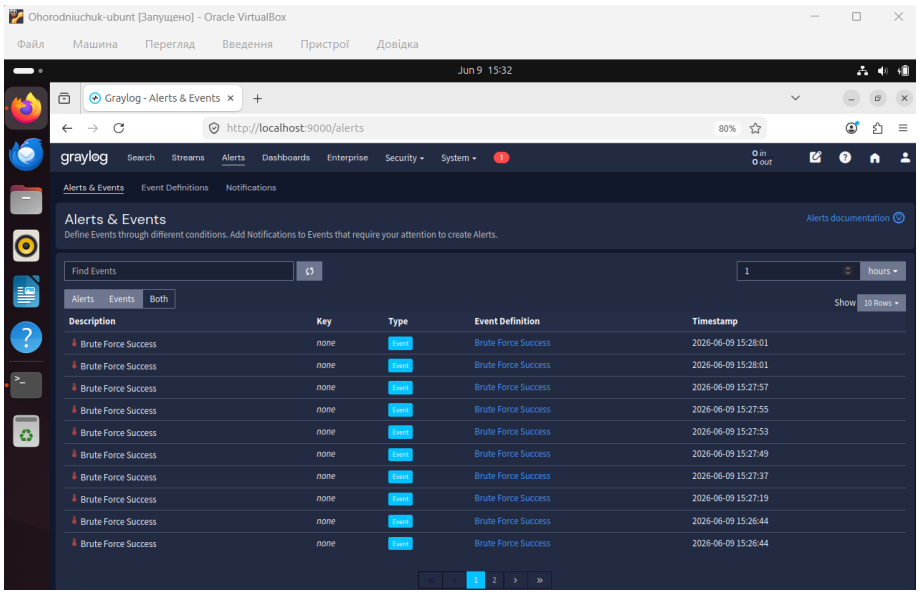


Рис.4.3 тестування перевірки на brute-force атаку

4.2 Налаштування пошуку індикаторів компрометації (IOC)

З метою оперативного розслідування інцидентів у Graylog оптимізовано механізм пошуку за ключовими індикаторами компрометації (IOC). Пошукові запити та фільтри налаштовано за такими параметрами:

- Ім'я користувача (наприклад, аналіз активності облікового запису Administrator);
- IP-адреса джерела (наприклад, фільтрація подій з хоста 192.168.100.20);
- Тип та точний час виникнення події.

Цей інструментарій дозволяє аналітику безпеки в реальному часі локалізувати джерело підозрілої активності та реконструювати хронологію дій зловмисника.

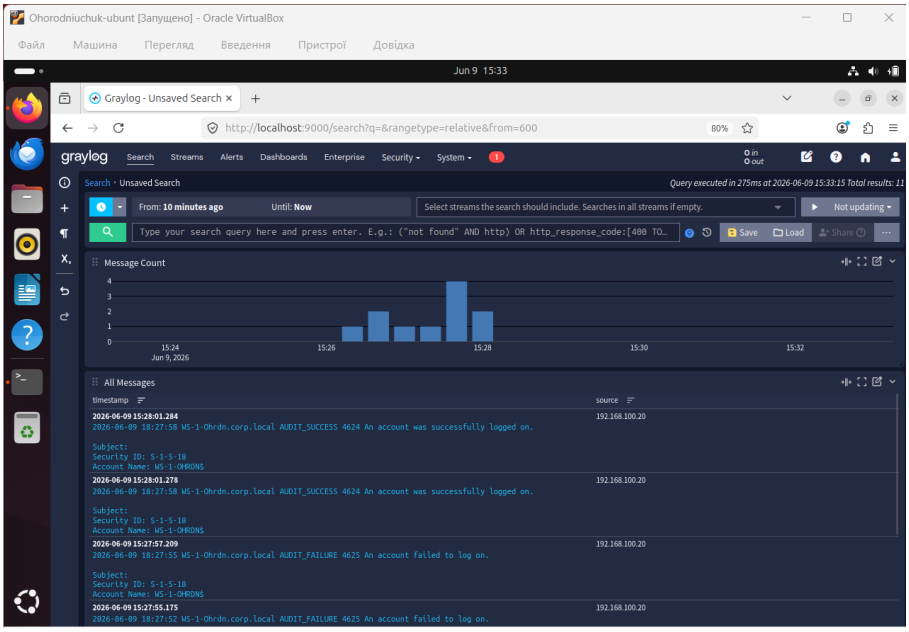


Рис.4.4 Аналітика безпеки в реальному часі

4.3 Оцінка ефективності функціонування системи

Комплексне тестування розгорнутого рішення в середовищі невеликої доменної інфраструктури підтвердило його ефективність за такими ключовими напрямками:

Таблиця 2.1

Напрямок моніторингу	Результат тестування
Збір та аналіз логів	Забезпечено централізоване агрегування журналів подій Windows та Active Directory.
Контроль автентифікації	Успішно фіксуються аномальні сплески невдалих спроб входу та факти компрометації.

Аудит дій адміністраторів	Реалізовано повний трекінг критичних змін у домені та активності привілейованих користувачів.

Згенеровані системою автоматичні сповіщення продемонстрували високу точність та мінімальну затримку, що доводить готовність рішення забезпечувати базовий рівень інформаційної безпеки підприємства.

Висновки до розділу 4

У межах четвертого розділу було успішно проведено практичну реалізацію та тестування механізмів виявлення інцидентів безпеки в системі Graylog. Результати тестування розроблених правил аналізу подій невдалого входу здатність у реальному часі ідентифікувати brute-force атаки й факти компрометації облікових записів із мінімальною затримкою. Водночас оптимізація інструментів пошуку за індикаторами компрометації забезпечила аналітику безпеки можливість оперативно локалізувати джерела загроз за конкретними IP-адресами чи іменами користувачів, що суттєво скорочує час на розслідування інцидентів. Комплексна оцінка функціонування рішення довела стабільність централізованого збору логів та надійність моніторингу подій Active Directory . Таким чином, розгорнута система повністю виконує покладені на неї завдання, забезпечуючи надійний моніторинг і базовий рівень інформаційної безпеки в межах досліджуваної інфраструктури.

Висновки

У результаті виконання кваліфікаційної роботи на тему «Проєкт підсистеми безпекового моніторингу доменної інфраструктури Microsoft Active Directory із застосуванням Graylog» було досягнуто поставленої мети та виконано всі визначені завдання.

На першому етапі роботи було проведено аналіз особливостей побудови доменних інфраструктур на базі Microsoft Active Directory та досліджено сучасні підходи до організації безпекового моніторингу. Розглянуто принципи функціонування Active Directory, механізми автентифікації та авторизації користувачів, особливості роботи служб DNS і Group Policy, а також типові загрози інформаційній безпеці доменних середовищ. Додатково було виконано аналіз засобів централізованого збору та аналізу журналів подій, за результатами якого для реалізації проєкту обрано систему Graylog.

На другому етапі було спроєктовано лабораторну інфраструктуру та виконано її розгортання у середовищі Oracle VirtualBox. Створено ізольовану мережу NAT Network, налаштовано схему адресації та забезпечено мережеву взаємодію між усіма вузлами. Розгорнуто доменне середовище Microsoft Active Directory, що включає два контролери домену, клієнтську робочу станцію та окремий сервер моніторингу. Виконано налаштування служби DNS, реплікації між контролерами домену та підключення клієнтської станції до домену.

Наступним завданням стало впровадження системи централізованого збору журналів подій. Для цього було розгорнуто сервер Graylog на базі Ubuntu Server, налаштовано приймання повідомлень та створено механізми зберігання і пошуку логів. Для передачі подій безпеки з вузлів доменної інфраструктури використано агенти Winlogbeat та NXLog, що забезпечили централізований збір журналів із контролерів домену та клієнтської станції.

У процесі виконання роботи також було реалізовано аудит подій безпеки Active Directory. Налаштовано журналювання подій автентифікації користувачів, змін облікових записів, модифікації груп безпеки та використання привілейованих облікових записів. Це дозволило забезпечити отримання детальної інформації про дії користувачів і адміністраторів у доменному середовищі.

Окрему увагу було приділено реалізації механізмів виявлення інцидентів інформаційної безпеки. У ході роботи налаштовано моніторинг подій невдалих спроб входу до системи, що дозволяє виявляти атаки типу brute-force. Також реалізовано контроль створення та видалення облікових записів, змін у групах безпеки, використання привілейованих прав доступу та подій антивірусного захисту Windows Defender.

Для перевірки працездатності створеної системи було проведено серію тестувань. Змодельовано невдалі спроби автентифікації користувачів, виконано створення та модифікацію облікових записів Active Directory, проведено перевірку моніторингу адміністративної активності, а також використано тестовий файл EICAR для перевірки обробки подій антивірусного захисту. Усі тестові сценарії були успішно зафіксовані системою Graylog та відображені в централізованому журналі подій.

Результати виконаної роботи підтвердили доцільність використання Graylog як платформи централізованого моніторингу подій безпеки в доменних середовищах Microsoft Active Directory. Розроблена підсистема забезпечує збір, зберігання та аналіз журналів подій, контроль процесів автентифікації користувачів, моніторинг змін об'єктів домену та виявлення типових загроз інформаційній безпеці.

Таким чином, поставлена мета кваліфікаційної роботи досягнута, а створене лабораторне середовище може використовуватися як основа для подальших досліджень і вдосконалення засобів моніторингу та захисту доменних інфраструктур.

Список використаної літератури

1. Microsoft Corporation. Active Directory Domain Services Overview [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/windows-server/identity/ad-ds/get-started/virtual-d/active-directory-domain-services-overview
2. Microsoft Corporation. Active Directory Administrative Center [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/windows-server/identity/ad-ds/get-started/adac/active-directory-administrative-center
3. Microsoft Corporation. Security Auditing Overview [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/windows/security/threat-protection/auditing/basic-security-audit-policy-settings
4. Microsoft Corporation. Windows Security Auditing Event IDs [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/windows/security/threat-protection/auditing/security-auditing-overview
5. Microsoft Corporation. Group Policy Overview [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview
6. Microsoft Corporation. Kerberos Authentication Overview [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/windows-server/security/kerberos/kerberos-authentication-overview
7. Microsoft Corporation. DNS and Active Directory Integration [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/windows-server/networking/dns/dns-top
8. Oracle Corporation. Oracle VM VirtualBox User Manual. – Oracle, 2024. – 1100 p.
9. Graylog Inc. Graylog Documentation [Електронний ресурс]. – Режим доступу: https://go2docs.graylog.org

10. Graylog Inc. Graylog Security Documentation [Електронний ресурс]. – Режим доступу: https://go2docs.graylog.org/current/home.htm

11. Winlogbeat Reference Documentation [Електронний ресурс]. – Режим доступу: https://www.elastic.co/guide/en/beats/winlogbeat/current/index.html

12. NXLog Documentation [Електронний ресурс]. – Режим доступу: https://docs.nxlog.co

13. OpenSearch Documentation [Електронний ресурс]. – Режим доступу: https://opensearch.org/docs/latest

14. MongoDB Documentation [Електронний ресурс]. – Режим доступу: https://www.mongodb.com/docs

15. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Pearson, 2023. – 816 p.

16. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. – Addison-Wesley, 2019. – 304 p.

17. Easttom C. Network Defense and Countermeasures. – Springer, 2022. – 410 p.

18. Maiwald E. Fundamentals of Network Security. – McGraw-Hill Education, 2021. – 528 p.

19. Kim D., Solomon M. Fundamentals of Information Systems Security. – Jones & Bartlett Learning, 2022. – 760 p.

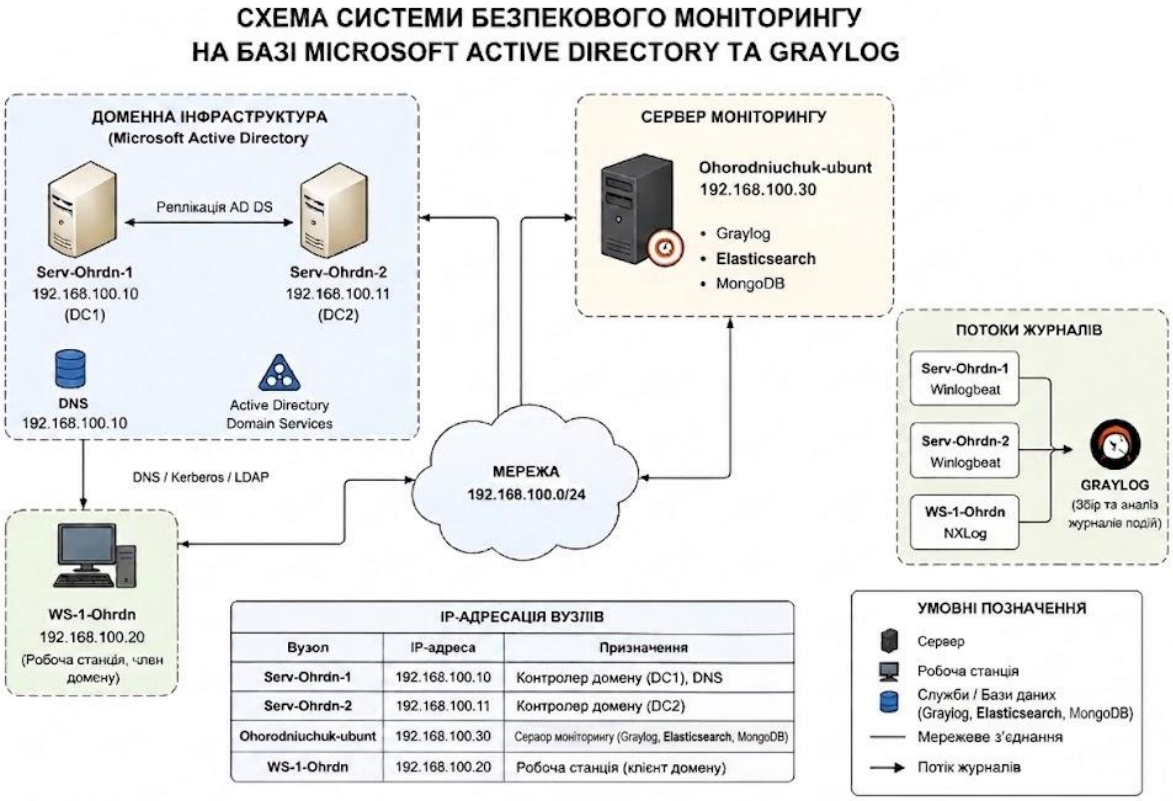
20. EICAR. European Institute for Computer Antivirus Research [Електронний ресурс]. – Режим доступу: https://www.eicar.org

21. Програмне забезпечення // Освітній портал Державного університету «Житомирська політехніка». URL: Освітній портал Житомирської політехніки

ДОДАТКИ

Додаток А

Детальна схема побудови системи



Додаток Б

Конфігурація NXLog та Winlogbeat

Конфігурація NXLog для робочої станції :

```
define ROOT C:\Program Files (x86)\nxlog
Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data\data
LogFile   %ROOT%\data\nxlog.log
<Extension gelf>
   Module      xm_gelf
</Extension>
<Input windows_events>
   Module      im_msvistalog
   Query       <QueryList>\
               <Query Id="0">\
                  <Select Path="Application">*</Select>\
                  <Select Path="System">*</Select>\
                  <Select Path="Security">*</Select>\
               </Query>\
            </QueryList>
</Input>
<Output graylog_out>
   Module      om_udp
   Host        192.168.100.30
   Port        12201
   OutputType  GELF
</Output>
<Route r1>
```

```
    Path        windows_events => graylog_out
</Route>
```

Конфігурація Winlogbeat для контролерів домену:

```
winlogbeat.event_logs:
  - name: Security
  - name: System
  - name: Application

output.logstash:
  hosts: ["192.168.100.30:5044"]

logging.level: info
```

Додаток В

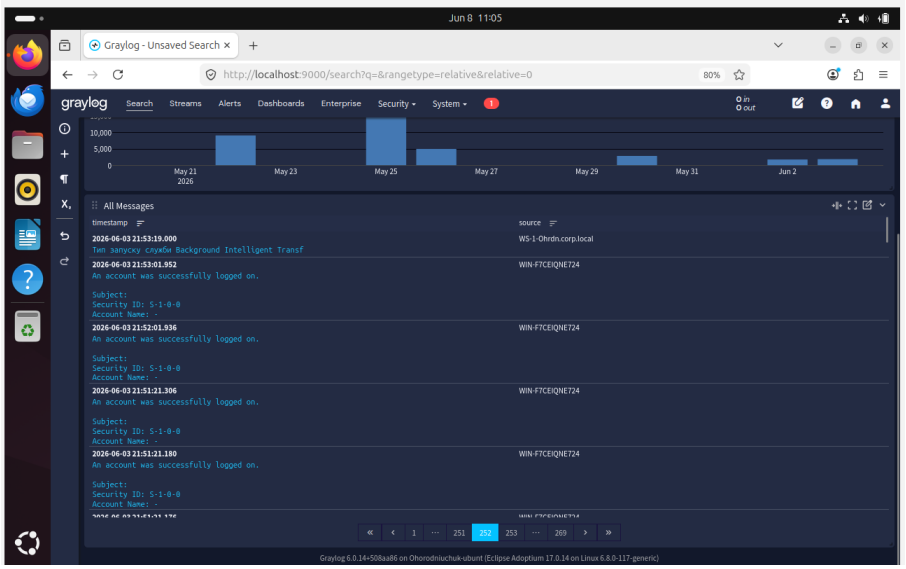
Скрипт на PowerShell для надсилання логів

```
$TargetIP = "192.168.100.30"
$TargetPort = 12201
$UdpClient = New-Object System.Net.Sockets.UdpClient
$TotalLogs = 5000
Write-Host "Запуск генерації великої кількості логів..." -ForegroundColor Green
for ($i = 1; $i -le $TotalLogs; $i++) {
   $GelfMessage = @{
      version       = "1.1"
      host          = "WS-1-Ohrdn-TestGen"
      short_message = "Test stress log message number $i"
      full_message  = "Detailed flood log for testing Graylog performance and
Elasticsearch indexing speed."
      level         = 6  # Informational
      _test_batch   = "StressTest-01"
      _loop_index   = $i
   } | ConvertTo-Json -Compress
   $Bytes = [System.Text.Encoding]::UTF8.GetBytes($GelfMessage)
   $bytesSent = $UdpClient.Send($Bytes, $Bytes.Length, $TargetIP, $TargetPort)
   Start-Sleep -Milliseconds 1
}
$UdpClient.Close()
Write-Host "Успішно надіслано $TotalLogs тестових логів!" -ForegroundColor
Cyan
```

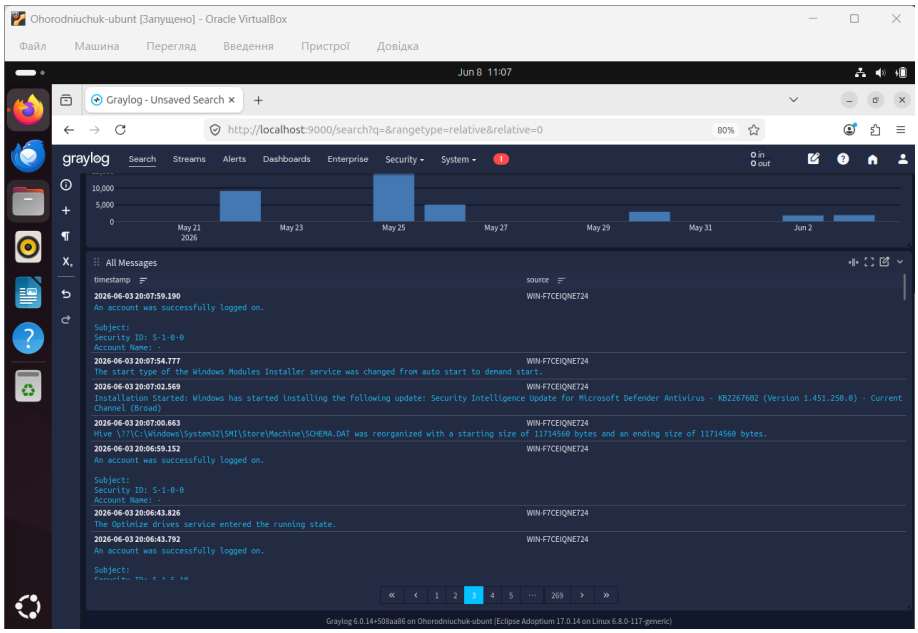
Додаток Г

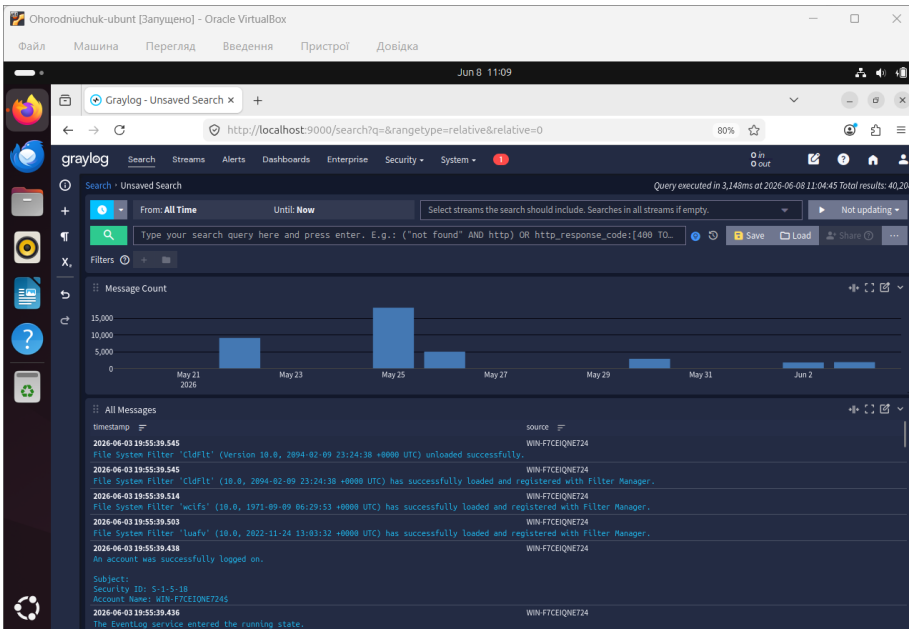
Результати тестування системи моніторингу

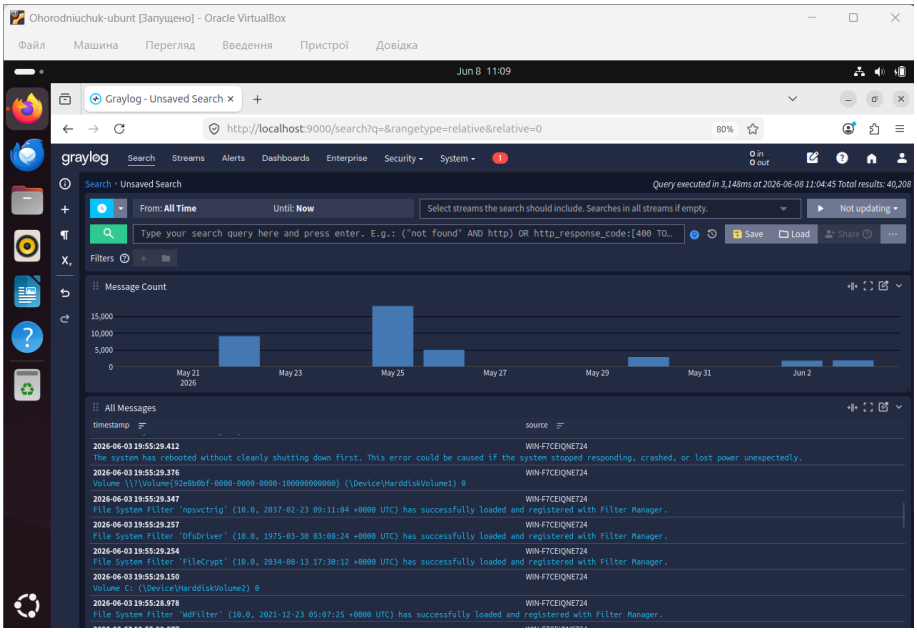
Результат надсилання фейкових логів:



Результат логів надісланих в ході тестування:

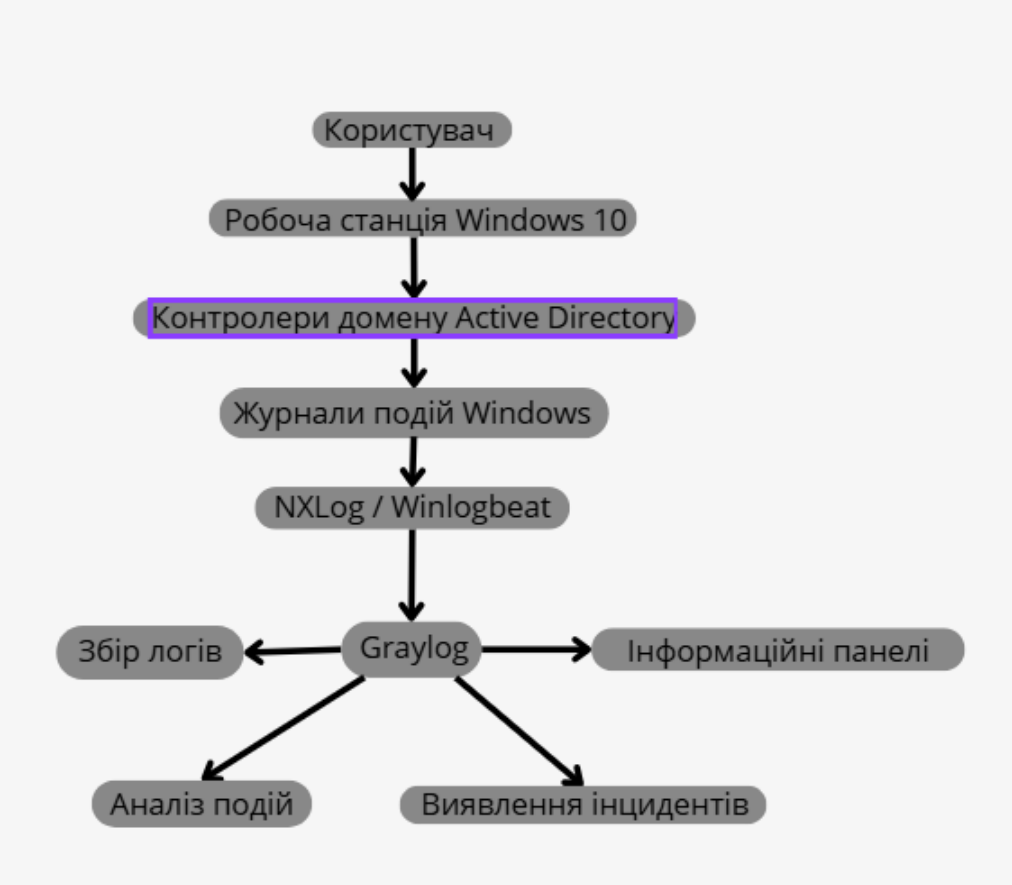



Ohorodniuchuk-ubunt [Запущено] - Oracle VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Jun 8 11:09
Graylog - Unsaved Search
http://localhost:9000/search?q=&rangetype=relative&relative=0
graylog
Search Streams Alerts Dashboards Enterprise Security System
Search › Unsaved Search
From: All Time Until: Now
Select streams the search should include. Searches in all streams if empty.
Not updating
Type your search query here and press enter. E.g.: ("not found" AND http) OR http_response_code:[400 TO...
Save Load
Filters
Message Count
15,000
10,000
5,000
0
May 21 2026
May 23
May 25
May 27
May 29
May 31
Jun 2
All Messages
timestamp
source
2026-06-03 19:55:39.545
WIN-F7CEIQNE724
File System Filter 'CldFlt' (Version 10.0, 2094-02-09 23:24:38 +0000 UTC) unloaded successfully.
2026-06-03 19:55:39.545
WIN-F7CEIQNE724
File System Filter 'CldFlt' (10.0, 2094-02-09 23:24:38 +0000 UTC) has successfully loaded and registered with Filter Manager.
2026-06-03 19:55:39.514
WIN-F7CEIQNE724
File System Filter 'wcifs' (10.0, 1971-09-09 06:29:53 +0000 UTC) has successfully loaded and registered with Filter Manager.
2026-06-03 19:55:39.503
WIN-F7CEIQNE724
File System Filter 'luafv' (10.0, 2022-11-24 13:03:32 +0000 UTC) has successfully loaded and registered with Filter Manager.
2026-06-03 19:55:39.438
WIN-F7CEIQNE724
An account was successfully logged on.
Subject:
Security ID: S-1-5-18
Account Name: WIN-F7CEIQNE724$
2026-06-03 19:55:39.436
WIN-F7CEIQNE724
The EventLog service entered the running state.


Ohorodniuchuk-ubunt [Запущено] - Oracle VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
Jun 8 11:09
Graylog - Unsaved Search
http://localhost:9000/search?q=&rangetype=relative&relative=0
graylog
Search Streams Alerts Dashboards Enterprise Security System
Search › Unsaved Search
From: All Time Until: Now
Select streams the search should include. Searches in all streams if empty.
Not updating
Type your search query here and press enter. E.g.: ("not found" AND http) OR http_response_code:[400 TO...
Save Load
Filters
Message Count
15,000
10,000
5,000
0
May 21 2026
May 23
May 25
May 27
May 29
May 31
Jun 2
All Messages
timestamp
source
2026-06-03 19:55:29.412
WIN-F7CEIQNE724
The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.
2026-06-03 19:55:29.376
WIN-F7CEIQNE724
Volume \\?\Volume{92e8b0bf-0000-0000-0000-100000000000} (\Device\HarddiskVolume1) 0
2026-06-03 19:55:29.347
WIN-F7CEIQNE724
File System Filter 'npsvctrig' (10.0, 2037-02-23 09:11:04 +0000 UTC) has successfully loaded and registered with Filter Manager.
2026-06-03 19:55:29.257
WIN-F7CEIQNE724
File System Filter 'DfsDriver' (10.0, 1975-03-30 03:08:24 +0000 UTC) has successfully loaded and registered with Filter Manager.
2026-06-03 19:55:29.254
WIN-F7CEIQNE724
File System Filter 'FileCrypt' (10.0, 2034-08-13 17:30:12 +0000 UTC) has successfully loaded and registered with Filter Manager.
2026-06-03 19:55:29.150
WIN-F7CEIQNE724
Volume C: (\Device\HarddiskVolume2) 0
2026-06-03 19:55:28.978
WIN-F7CEIQNE724
File System Filter 'WdFilter' (10.0, 2021-12-23 05:07:25 +0000 UTC) has successfully loaded and registered with Filter Manager.

Додаток Ґ

Схеми до виконаної роботи



Функціональна схема

Відповідає на питання функціонального навантаження елементів проєкту

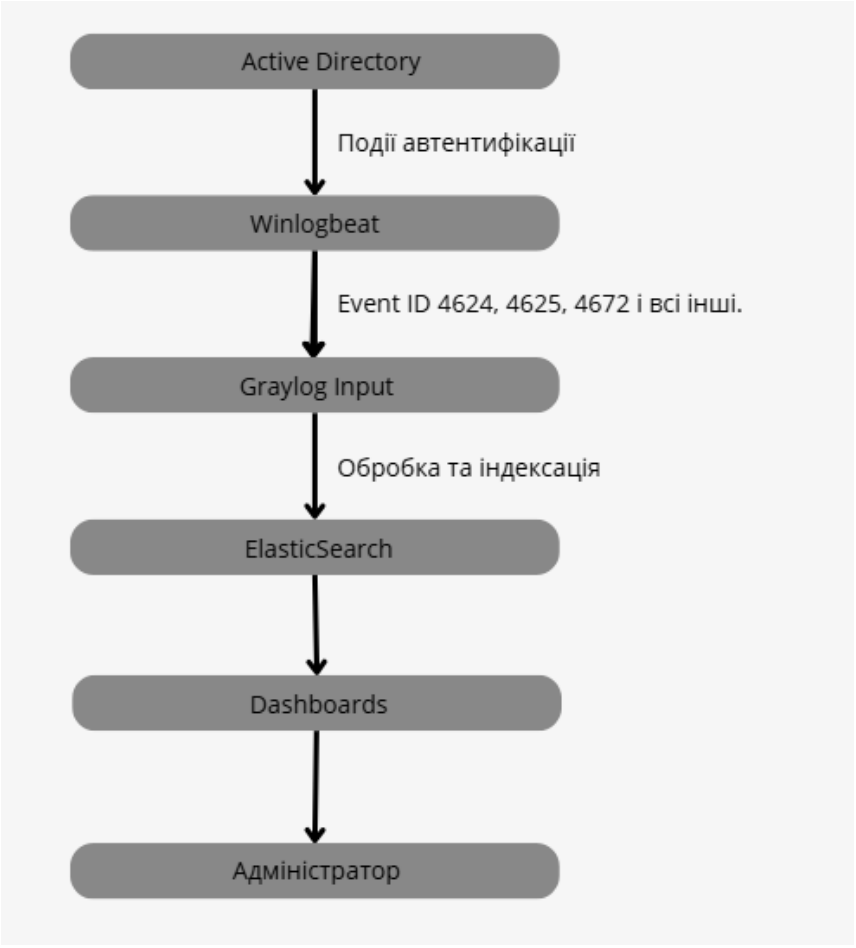


Схема інформаційних потоків

Схема показує яка інформація куди передається та на підставі чого