Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

Комплексна бакалаврська кваліфікаційна робота на тему:
«Кіберполігон для дослідження подій інформаційної безпеки. Частина 2. Обробка на основі Graylog»

Виконав: студент 4 курсу групи 1БС-21МС
спеціальності 125 Кібербезпека
_____ Лазуренко І.Д.
Керівник: к. т. н., доцент каф. ЗІ
_____ Войтович О. П.
«16» червня 2023 р.
Рецензент: к. т. н. доцент каф. ПЗ
_____ Коваленко О. О.
«16» червня 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«16» червня 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти I (бакалаврський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Зав. кафедри ЗІ,
к. т. н., проф.
Володимир ЛУЖЕЦЬКИЙ
«20» березня 2023 року

З А В Д А Н Н Я
НА КОМПЛЕКСНУ БАКАЛАВРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Лазуренку Івану Дмитровичу

1. Тема роботи: «Кіберполігон для дослідження подій інформаційної безпеки. Частина 2. Обробка на основі Graylog»
керівник роботи: Войтович Олеся Петрівна, к. т. н., доцент кафедри ЗІ, затверджені наказом ректора ВНТУ від 20 березня 2023 року №67.

2. Строк подання студентом роботи 16 червня 2023 р.

3. Вихідні дані до роботи:

- Розробка кіберполігону на базі кафедри захисту інформації;
- Встановлення налаштування системи моніторингу;
- Налаштування правил фільтрації та реагування на події;

4. Зміст текстової частини: Вступ. 1. Аналіз предметної області. 2. Обґрунтування обраних рішень. 3. Тестування обраних рішень. Висновки. Список використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: Потік лог-даних на сервері (плакат А4). Схема взаємодії компонентів Elastic Stack (плакат А4). Порівняння основних параметрів додатків для роботи з логами (плакат А4). Схема роботи Graylog-серверу (плакат А4). Результат налаштованого часового фільтру (плакат А4). Результат створення події (плакат А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Войтович О. П., к.т.н., доц. каф.ЗІ	20.03.23	16.06.23
2	Войтович О. П., к.т.н., доц. каф.ЗІ	20.03.23	16.06.23
3	Войтович О. П., к.т.н., доц. каф.ЗІ	20.03.23	16.06.23

7. Дата видачі завдання 20 березня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської кваліфікаційної роботи	Строк виконання етапів роботи	Приміт
1	Аналіз завдання. Вступ	23.03.23 – 24.03.23	
2	Розробка технічного завдання	25.03.23 – 02.04.23	
3	Аналіз інформаційних джерел за напрямком бакалаврської дипломної роботи	03.04.23 – 17.04.23	
4	Розробка рішень, моделей, алгоритмів	18.04.23 – 06.05.23	
5	Практична реалізація, моделювання, експериментування, результати	15.05.23 – 30.05.23	
6	Аналіз виконання ТЗ, висновки	01.06.23 – 03.06.23	
7	Оформлення пояснювальної записки	04.06.23 – 13.06.23	
8	Попередній захист БКР	14.06.23 – 14.06.23	
9	Виправлення зауважень, підготовка ілюстративного матеріалу	15.06.23 – 19.06.23	
10	Представлення БКР до захисту, рецензування	20.06.23 – 23.06.23	

Студент _____ Іван ЛАЗУРЕНК

Керівник роботи _____ Олеся ВОЙТОВИ

АНОТАЦІЯ

Комплексна бакалаврська кваліфікаційна робота складається з 62 сторінок формату А4, на яких є 20 рисунків, 2 таблиць, 5 схем, список використаних джерел містить 25 найменувань.

Комплексна бакалаврська робота присвячена покращенні безпеки інформаційно комунікаційної системи шляхом розробки та реалізації кіберполігону на основі системи моніторингу GrayLog.

Розглянуто принципи побудови кіберполігону, на основі яких було створено власній прототип системи. Проаналізовано існуючі програмні рішення для моніторингу за лог-даними. Розглянуто основний функціонал одної із систем моніторингу Graylog, на основі якої відбувалося подальше налаштування фільтрації, потоків та налаштування системи сповіщень.

Ключові слова: кібербезпека, керування інцидентами, системи керування логами, системи SIEM, система GrayLog.

ABSTRACT

The comprehensive bachelor's qualification work consists of 62 pages of A4 format, on which there are 25 figures, 2 tables, 5 diagrams, the list of used sources contains 20 names.

The complex bachelor's work is devoted to improving the security of the information and communication system by developing and implementing a cyber polygon based on the GrayLog monitoring system.

The principles of building a cyber polygon were considered, on the basis of which a prototype system was created. Existing software solutions for monitoring by log data were analyzed. The main functionality of one of the monitoring systems was considered Graylog, on the basis of which the further setting of filtering, flows and setting of the notification system took place.

Keywords: cyber security, incident management, log management systems, SIEM systems, GrayLog system.

ЗМІСТ

ВСТУП

Сучасний цифровий світ потребує надійного та ефективного захисту від кіберзагроз. З кожним днем зростають обсяги і складність кібератак, що ставить перед організаціями серйозні виклики в галузі кібербезпеки. Одним із найефективніших підходів до розв'язання цих проблем є побудова кіберполігону, який забезпечує постійний моніторинг, аналіз та реагування на кіберзагрози.

GrayLog є потужним інструментом для збору, аналізу та візуалізації журнальних даних, що дозволяє забезпечити централізований моніторинг та аналіз подій, що відбуваються у мережі.

Предметом дослідження є кіберполігон для дослідження подій кібербезпеки на основі системи моніторингу за лог-даними GrayLog.

Об’єктом дослідження є процес моніторингу подій інформаційної безпеки на базі системи моніторингу за лог-даними GrayLog.

Мета бакалаврської роботи полягає у покращенні безпеки інформаційно комунікаційної системи шляхом розробки та реалізації кіберполігону на основі системи моніторингу GrayLog.

Відповідно до мети **завданнями** є:

- аналіз поточного стану кібербезпеки: проведення огляду існуючих систем безпеки та ідентифікація можливих проблем та слабких місць;
- проектування архітектури кіберполігону: визначення необхідних компонентів, їх взаємодію та розміщення для ефективного моніторингу та аналізу;
- впровадження та налаштування GrayLog: розгляд можливостей та функціональності GrayLog, його інтеграція з існуючими системами безпеки та налаштування для вимог кіберполігону.
- тестування та оцінка ефективності: проведення реалістичних тестів та оцінка ефективності кіберполігону на основі зібраних журнальних даних.

Результати бакалаврської роботи можливо використовувати у навчальному процесі, що надасть практичних навичок та більш глибокого розуміння поняття кіберполігону та принципів його роботи, або маштабувати

прототип та впровадити його у систему університету, щоб покращити заходи з кібербезпеки та забезпечити безпечну та надійну роботу інформаційних систем.

Проміжні результати бакалаврської роботи опубліковані у матеріалах LII Науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії (2023) [1].

1 АНАЛІЗ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1.1 Суть проблеми та необхідність набуття навичок роботи з логами

З кожним роком процес все більше галузей людської діяльності підлягають діджиталізації. Інтернет магазини, банки, комунальні сайти, сфери послуг, ігрова індустрія, пошта, майже усі повсякденні види діяльності перенесли свою діяльність до глобальної мережі, не кажучи про внутрішні мережі на підприємствах чи інших установах.

Кожна компанія чи підприємство повинно забезпечити швидку та якісну взаємодію між працівниками, надати доступ до певної інформації та можливість зберігати дані для подальшої їх обробки і використанні. Раніше це відбувалося за рахунок паперової документації чи в усній формі, якщо це було допустимо. Затрачений час на написання та оформлення документів, пошук та взагалі ознайомлення співробітників з ними займає досить великий проміжок часу, саме тому сервера та локальні мережі стали невід’ємною ланку у сучасних компаній будь-якого направлення чи спеціалізації.

Сервера потребують налаштування та підтримки, коректності роботи, оскільки втрата даних чи доступу до розгорнутому додатку на ньому може призупинити роботу установи або задати її величезних збитків. Виходячи з цього, можна зробити висновок, що слідкування за серверами та мережами є досить важливим, саме тому комп’ютери ведуть власну звітність про те, що саме відбувається з ними. Такі звіти отримали назву логи.

Файли логів зберігаються на комп’ютерах, в них записані усі події що відбуваються на пристрої, формуючи щось схоже на звіт про виконану роботу. Оскільки основне програмне забезпечення зазвичай робить записи у журнали, то кожна програма матиме свій журнал логів. Завдяки цьому, спеціаліст, може більш швидко знайти помилку, яка також буде записана у файл логів, проаналізувати її та прийняти рішення за для її вирішення.

Зазвичай на серверах потік логів дуже великий, оскільки майже весь час на ньому щось відбувається, тому вчасно знайти помилку стає важкою задачею. Приклад потоку лог-даних на сервері зображено на рисунку 1.1.

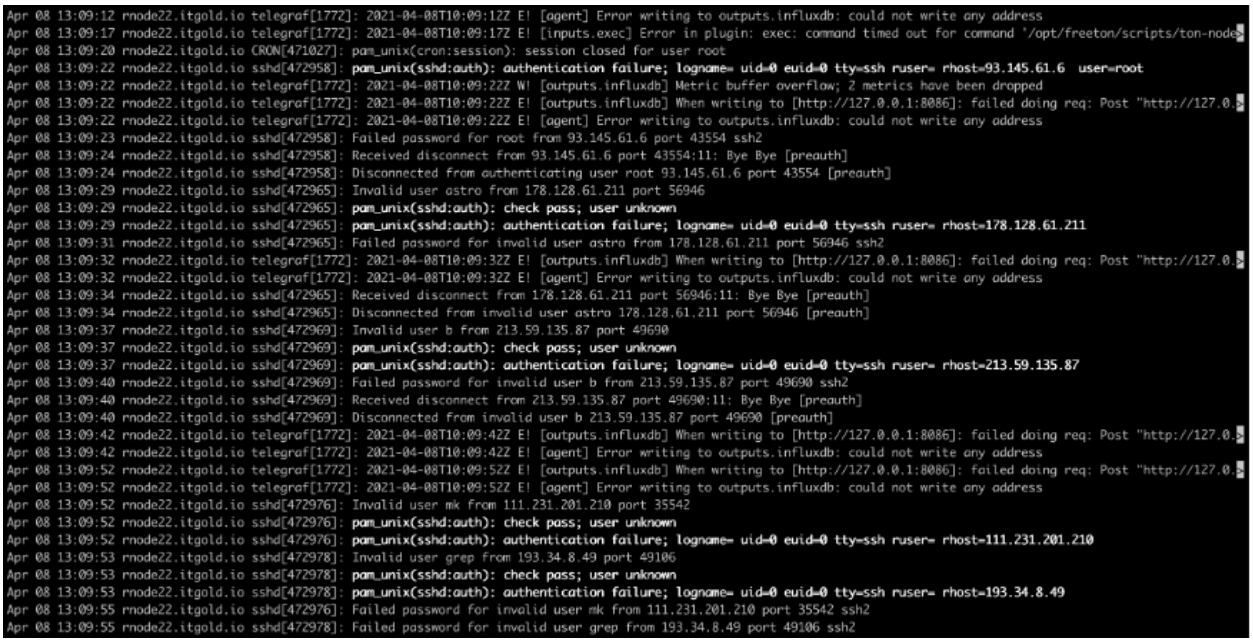


Рисунок 1.1 – Потік лог-даних на сервері

Потік даних на сервері залежить від самого підприємства чи установи і щосекундно можуть надходить по декілька запитів. При такій швидкості потоку важко навіть помітити підозрілі або пошкодженні дані, не кажучи вже про їх аналіз і реагування.

Саме тому було розроблено програмне забезпечення для фільтрації логів. Такі програми полегшують роботу та значно прискорюють пошук місця виникнення збою.

1.2 Поняття логів, їх призначення та використання

Логи (лог-файли) – це файли, які містять системну інформацію про роботу сервера або комп’ютера та певні дії користувача або програми [2]. Іноді також вживається україномовний аналог поняття – журнал.

Їх призначення – протоколювання операцій, які виконують на машині, для подальшого аналізу цих операцій адміністратором. Регулярний перегляд журналів дозволить визначити помилки в роботі системи, конкретного сервісу

або сайту (особливо приховані помилки, які не видно при перегляді в браузері), діагностувати зловмисну активність, зібрати статистику відвідувань сайту.

Серверні логи є записами подій, які сталися на сервері або в додатку, і зберігаються у вигляді текстових файлів або в базі даних. Логи дозволяють відстежувати та аналізувати різноманітну інформацію, що стосується роботи сервера, таку як вхідні запити, відповіді сервера, помилки, стан системи та інші події.

Аналіз серверних логів може допомогти виявити проблеми безпеки, оптимізувати продуктивність сервера, виявити та виправити помилки програмного забезпечення, відновити стан системи після відмови та забезпечити аудит історії подій. Зберігання та аналіз серверних логів використовується в різних сферах, включаючи веб-хостинг, інтернет-сервіси, системи моніторингу, програмне забезпечення, мережі та безпеку.

Серверні логи можна класифікувати за різними критеріями, такими як джерело логів, тип подій, рівень деталізації та інші. Ось кілька загальних класифікаційних категорій:

За джерелом логів:

– системні логи: Записують події, що стосуються операційної системи сервера, такі як завантаження, вимкнення, помилки ядра, встановлення пакетів тощо;

– додаткові логи: Включають логи додатків або служб, які працюють на сервері, наприклад, веб-сервери, бази даних, електронна пошта, проксі-сервери тощо;

– аудиторські логи: Використовуються для записування подій, пов'язаних з безпекою та аудитом, такі як успішні та невдачні авторизації, доступ до конфіденційних даних, зміна налаштувань тощо;

За типом подій:

– інформаційні логи: Включають інформацію про нормальну роботу системи або додатків, наприклад, завантаження послуг, успішні операції тощо;

– попереджувальні логи: Записують попередження про потенційні проблеми, які потребують уваги адміністратора, наприклад, низький рівень дискового простору, підозрілі активності тощо;

– помилкові логи: Містять повідомлення про помилки, які виникли в процесі роботи системи або додатків, такі як виключення, невдалий доступ, нездатність виконати операцію тощо;

За рівнем деталізації:

– стандартні логи: Включають основну інформацію про події, наприклад, час, джерело, тип події тощо;

– розширені логи: Містять додаткову детальну інформацію про події, таку як параметри запитів, ідентифікатори користувачів, IP-адреси, статусні коди тощо;

Це лише загальні категорії, а конкретна класифікація серверних логів може варіюватися в залежності від системи, додатків та вимог до ведення журналів.

1.3 Система моніторингу за лог-даними, аналіз та способи використання

Система моніторингу за лог-даними є компонентом інформаційної системи, який відповідає за автентифікацію та авторизацію користувачів у системі. Він забезпечує централізований доступ до різних ресурсів та послуг, контролює права доступу та забезпечує безпеку інформації.

Основні функції центрального логін-сервера включають:

– автентифікація: Перевірка ідентифікаційних даних користувача, таких як ім'я користувача і пароль, для підтвердження його особи;

– авторизація: Перевірка прав доступу користувача до конкретних ресурсів або послуг. Центральний логін-сервер містить інформацію про права доступу користувачів та відповідає за їх управління;

– керування обліковими записами: Центральний логін-сервер зберігає і керує обліковими записами користувачів, включаючи створення нових облікових записів, зміну паролів та інші адміністративні завдання;

– журналювання та моніторинг: Центральний логін-сервер веде журнал подій, пов'язаних з аутентифікацією та авторизацією користувачів, що дозволяє відслідковувати та аналізувати дії користувачів у системі;

– забезпечення безпеки: Центральний логін-сервер використовує різні механізми безпеки, такі як шифрування трафіку та захист від несанкціонованого доступу, для забезпечення безпеки інформації та захисту користувачів;

– інтеграція з іншими системами: Центральний логін-сервер може бути інтегрований з іншими системами, такими як електронна пошта, бази даних або хмарні сервіси, що дозволяє користувачам отримувати доступ до цих ресурсів з використанням одних і тих же авторизаційних даних;

Застосування центральних логін-серверів поширені в корпоративних середовищах, де велика кількість користувачів має доступ до різних ресурсів. Вони спрощують процес автентифікації та авторизації, поліпшують безпеку і зручність для користувачів та дозволяють централізовано керувати правами доступу.

На сьогоднішній день робота з великою кількістю даних кількістю даних необхідна у будь якій сфері діяльності. Ці дані надходять із різних джерел, як-от пристроїв, програм і операційних систем. Централізована система керування журналами (LMS), як-от Graylog, надає засоби для агрегування, організації та розуміння всіх цих даних [3].

Файли журналу – це текстові файли. Вони містять велику кількість інформації – назву програми, IP-адресу, мітку часу та місце призначення. Усі програми та навіть операційні системи самі створюють ці журнали, що містять величезні обсяги даних, які потрібно проаналізувати, для подальшого їх розуміння та використання.

Існує кілька додатків та інструментів, які допомагають у роботі з лог-файлами та аналізі логів. Ось кілька популярних додатків, які широко використовуються для цих цілей:

1. Elastic Stack (раніше відомий як ELK Stack): Elastic Stack складається з Elasticsearch, Logstash та Kibana. Elasticsearch є потужним розподіленим двигуном пошуку та аналізу даних, Logstash використовується для збору,

обробки та пересилання лог-даних, а Kibana забезпечує візуалізацію та інтерактивний аналіз цих даних. Elastic Stack дозволяє індексувати, зберігати, пошуково аналізувати та візуалізувати лог-файли з різних джерел [3].

2. Splunk: Splunk є інтегрованою платформою для збору, індексації, пошуку та аналізу лог-даних. Він дозволяє візуалізувати дані у реальному часі, використовувати запити для пошуку конкретної інформації та створювати звіти на основі цих даних. Splunk також надає можливості моніторингу та сповіщення про події [5].

3. Graylog: Graylog є відкритим рішенням для збору, індексації та аналізу лог-даних. Він дозволяє централізовано збирати логи з різних джерел, використовувати потужні пошукові запити для аналізу даних та створювати візуалізації для легкого сприйняття інформації. Graylog також має можливості моніторингу та сповіщення [3].

4. Loggly: Loggly є хмарною платформою для збору, аналізу та моніторингу лог-даних. Він надає простий інтерфейс для завантаження та відображення лог-файлів, можливість використовувати пошукові запити для аналізу даних та створювати звіти. Loggly також підтримує моніторинг, алерти та інтеграцію з іншими інструментами [6].

Оскільки усі ці програми виконують подібні функції, більшість можливостей та структура у них схожі. Порівняння основних параметрів додатків для роботи з логами зображено у таблиці 1.1.

Це загальні характеристики, котрі можуть змінюватись за рахунок різних варіантів підписок для кожного з додатків.

Ці додатки надають різноманітні функції для роботи з лог-файлами, дозволяючи збирати, аналізувати, візуалізувати та моніторити дані логування. Вибір конкретного додатка залежить від потреб організації, розмірів проекту та бюджетних обмежень.

Таблиця 1.1 – Результати аналізу основних параметрів додатків для роботи з логами

Додаток	Опис	Тип додатка	Інтеграція
Elastic Stack	Потужний стек для збору, аналізу та візуалізації логів	Відкритий, self-hosted	Інтеграція з Logstash, Elasticsearch API, Kibana, Beats
Splunk	Інтегрована платформа для аналізу та моніторингу	Комерційна, self-hosted	Інтеграція з API та SDK, Universal Forwarder, різноманітні джерела даних
Graylog	Відкрите рішення для збору та аналізу логів	Відкрите, self-hosted	Інтеграція з ріними джерелами та агентами даних, Graylog API
Loggly	Хмарна платформа для збору та аналізу логів	Хмарна	Інтеграційні інструменти відсутні

1.2.1 Аналіз додатку Elastic Stack

Elastic Stack, також відомий як ELK Stack, є популярним набором інструментів для збору, зберігання, пошуку та візуалізації даних. Включає в себе такі компоненти, як Elasticsearch, Logstash, Beats і Kibana. Для більш детального аналізу компоненти будуть розглянуті кожен окремо та їхні можливості, задля розуміння їх суміжної роботи [7].

Elasticsearch є основним компонентом Elastic Stack. Це розподілена пошукова та аналітична система, побудована на основі Apache Lucene. Elasticsearch забезпечує швидкий пошук та аналіз великого обсягу структурованих та неструктурованих даних. Він працює на основі розподіленої архітектури, яка дозволяє горизонтально масштабувати систему. Elasticsearch також надає можливість виконувати розширені запити, використовуючи мову запитів JSON[8].

Основні можливості Elasticsearch:

– швидкий пошук та індексація даних;

– розподілена архітектура для горизонтального масштабування;

– підтримка реплікації та шарування даних для забезпечення високої доступності та надійності;

– аналітика та агрегація даних для виконання складних операцій та отримання інсайтів;

– інтеграція з різними джерелами даних та інструментами;

Logstash використовується для збору, обробки та передачі лог-файлів та інших даних в різноманітних форматах до Elasticsearch для подальшого аналізу. Він пропонує розширені можливості фільтрації та перетворення даних, що дозволяє структурувати та підготувати їх для зберігання та пошуку.

Основні можливості Logstash:

– збір, фільтрація та перетворення даних з різноманітних джерел;

– підтримка різних вхідних та вихідних плагінів для обробки різних форматів даних;

– можливість налаштування послідовності операцій обробки даних;

– підтримка розподіленої обробки для швидкості та масштабованості;

Beats є легковаговими агентами, які використовуються для збору та відправки даних до Logstash або Elasticsearch безпосередньо. Існує кілька видів Beats, які спеціалізуються на різних типах даних, наприклад: Filebeat – для збору лог-файлів з файлових систем; Metricbeat – для збору метрик систем та служб; Packetbeat – для аналізу мережевого трафіку [8].

Основні можливості Beats:

– легка та ефективна передача даних до Elasticsearch або Logstash;

– підтримка різних типів даних та протоколів;

– можливість налаштування фільтрації та обробки даних перед відправкою;

Kibana – це інтерактивний інструмент візуалізації та аналізу даних, який надає користувачам гнучкі можливості для дослідження та спостереження даних, зброячуючи їх дашбордами, графіками, діаграмами тощо. Kibana працює в парі з

Elasticsearch і надає інтерфейс для виконання запитів до даних, відображення результатів та налаштування візуалізаційних елементів [9].

Основні можливості Kibana:

– створення дашбордів для візуалізації даних у режимі реального часу;

– виконання запитів та агрегація даних з Elasticsearch;

– налаштування графіків, діаграм, карт тощо для аналізу даних;

– інтеграція з іншими інструментами Elastic Stack;

У цьому аналізі було розглянуто основні компоненти Elastic Stack – Elasticsearch, Logstash, Beats і Kibana. Кожен з цих компонентів виконує важливі функції у зборі, зберіганні, обробці та аналізі даних, схему взаємодії компонентів у Elastic Stack зображено на рисунку 1.2. За допомогою Elastic Stack можна побудувати потужну систему для розуміння та отримання інсайтів з великого обсягу даних.

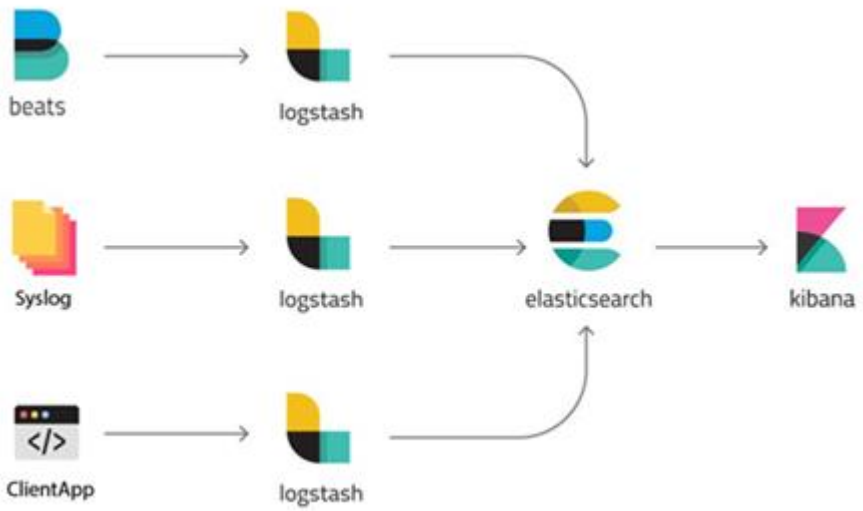


Рисунок 1.2 – Схема взаємодії компонентів Elastic Stack

Але така потужна система як Elastic Stack має і недоліки у вигляді складності у налаштуванні та встановлення кожного з компонентів. Використання такої системи у великих проектах буде зручним, але для менш глобальних рішень його використання буде недоцільним, оскільки є більш прості у налаштуванні додатки.

1.2.2 Аналіз додатку Splunk

Splunk є комерційною платформою для збору, індексування, пошуку та аналізу великого обсягу даних з різних джерел [10].

Основні особливості Splunk.

– Збір та індексація даних: Splunk дозволяє збирати дані з різних джерел, включаючи серверні журнали, логи додатків, метрики систем та інші джерела. Він індексує ці дані, створюючи швидкий доступ до них для подальшого пошуку та аналізу.

– Потужний пошук та аналітика: Splunk надає розширені можливості пошуку та аналізу даних. Він підтримує мову запитів SPL (Splunk Processing Language), яка дозволяє виконувати складні пошукові запити та агрегацію даних. Крім того, Splunk пропонує великий набір вбудованих функцій та візуалізацій для виведення результатів аналізу.

– Моніторинг та алертинг: Splunk дозволяє встановлювати моніторинг параметрів системи, додатків або мережі. Він може виявляти аномалії або проблеми та надсилати сповіщення або алерти. Це дозволяє оперативно виявляти та реагувати на проблеми в реальному часі.

– Розширені можливості машинного навчання: Splunk підтримує інтеграцію з різними інструментами машинного навчання, такими як Python або R. Це дозволяє виконувати складний аналіз даних, прогнозування та розробку моделей.

– Розподілена архітектура: Splunk працює на основі розподіленої архітектури, що дозволяє горизонтально масштабувати систему. Ви можете розгортати кластери Splunk, щоб обробляти великі обсяги даних та забезпечити високу доступність.

Як недолік можна відзначити функцію self-hosted, котра у даному додатку є лише комерційною. Одним з недоліків комерційної self-hosted версії Splunk є висока вартість. Ліцензія Splunk може бути досить дорогим варіантом для підприємств, особливо якщо мається потреба великого обсягу даних або розгортання на багатьох серверах.

Крім того, комерційна версія Splunk має обмеження в ліцензійних обсягах даних, що може стати перешкодою для організацій з великими обсягами даних.

Перевищення обсягу даних може призвести до додаткових витрат на розширення ліцензії або втрату доступу до даних.

Окрім цього, обслуговування та налагодження самостійного розгортання Splunk може вимагати великих зусиль та технічної експертизи. Розгортання та управління Splunk можуть бути складними завданнями для команди IT без достатнього досвіду.

Загалом, Splunk є потужною комерційною платформою для збору та аналізу даних, але його комерційна self-hosted версія має обмеження вартості, ліцензійного обсягу даних та може вимагати додаткових зусиль для розгортання та управління.

1.2.3 Аналіз додатку Graylog

Graylog – це потужний сервер журналювання та аналізу журналів, призначений для централізованого збору, аналізу та візуалізації журнальних даних з різних джерел. Він надає можливість зібрати та обробити великі обсяги журнальних записів з різних джерел, таких як сервери, додатки, мережеві пристрої та інші системи [11].

Основні особливості та можливості Graylog сервера включають.

– Централізований збір журналів: Graylog дозволяє централізовано збирати журнали з різних джерел у реальному часі. Він підтримує різні протоколи збору журналів, такі як syslog, GELF (Graylog Extended Log Format), та багато інших.

– Пошук та фільтрація даних: Завдяки потужному пошуковому двигуну, Graylog дозволяє виконувати швидкий пошук і фільтрацію журнальних даних за різними критеріями, такими як час, рівень журналу, джерело, ключові слова тощо. Це допомагає знайти необхідну інформацію та аналізувати її.

– Аналіз та візуалізація даних: Graylog надає можливості для аналізу та візуалізації журнальних даних за допомогою гнучких запитів і різних типів графіків, діаграм та інших візуальних елементів. Це допомагає відстежувати тренди, виявляти проблеми та отримувати цінні інсайти зі зібраних даних.

– Система оповіщень: Graylog дозволяє налаштувати систему оповіщень, що дозволяє отримувати сповіщення про події, помилки або інші

важливі події на основі заданих правил і фільтрів. Це допомагає оперативно реагувати на проблеми та забезпечує моніторинг системи в режимі реального часу.

– Розширюваність та інтеграція: Graylog має розширену систему плагінів та API, що дозволяє розширити його функціональність та інтегрувати з іншими системами. Він також підтримує інтеграцію з іншими інструментами моніторингу, логування та аналізу даних.

Загалом, Graylog сервер є потужним інструментом для збору, аналізу та візуалізації журнальних даних. Він допомагає управляти та моніторити сервери, додатки та мережеві пристрої, спрощуючи процес аналізу та виявлення проблем для підтримки надійності та безпеки інфраструктури [12]. Блок-схема з принципом роботи Graylog серверу зображено на рисунку 1.3.

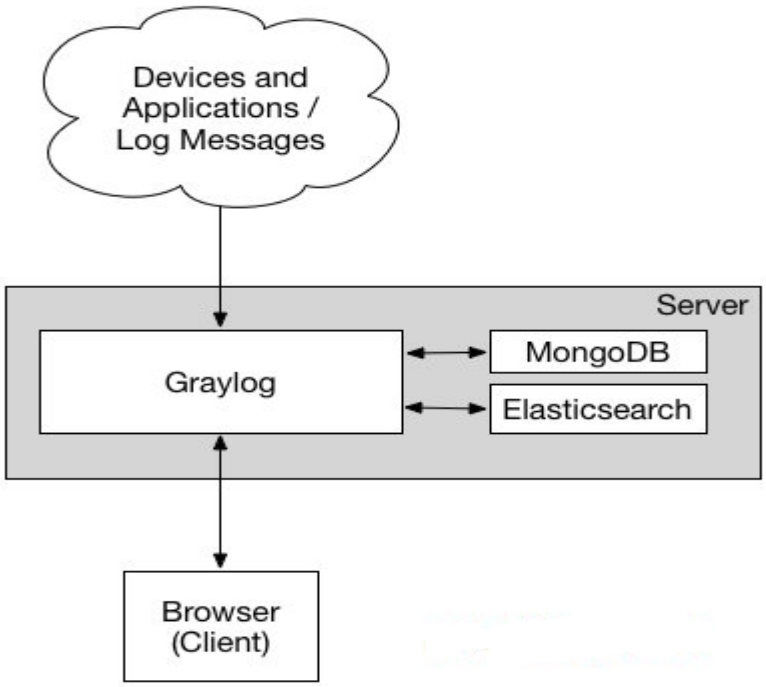


Рисунок 1.3 – Узагальнена схема Graylog-серверу

Кожен з цих аналогів має свої переваги та особливості, і вибір між ними залежить від конкретних потреб та обмежень вашої організації. Graylog, на відміну від деяких інших аналогів, пропонує відкрите джерело і може бути зручним варіантом для організацій з обмеженими бюджетами, які шукають розширюваність та гнучкість в налаштуванні системи журналювання та аналізу.

1.2.4 Аналіз додатку Loggly

Loggly є хмарною платформою журналювання, яка надає потужні інструменти для збору, аналізу та моніторингу лог-файлів [13].

Основні функції Loggly.

Збір та агрегація даних: Loggly дозволяє збирати лог-файли з різних джерел, включаючи сервери, додатки та сервіси. Ви можете легко налаштувати інтеграцію зі своїми системами і передавати логи в Loggly для подальшого аналізу.

Пошук та фільтрація даних: Loggly надає потужні можливості пошуку та фільтрації даних. Ви можете виконувати швидкі пошукові запити за різними параметрами, застосовувати фільтри та використовувати регулярні вирази для точного пошуку потрібної інформації.

Аналіз та візуалізація даних: Loggly дозволяє аналізувати дані та створювати візуалізації для кращого розуміння лог-файлів. Ви можете створювати графіки, діаграми та інші візуальні елементи, щоб відстежувати тренди та знайти корисну інформацію.

Алертинг: Loggly дозволяє налаштовувати правила алертингу на основі визначених умов. Ви можете отримувати сповіщення або повідомлення, коли виникають певні події або стан системи відхиляється від заданих меж.

Інтеграція з іншими інструментами: Loggly підтримує інтеграцію з різними інструментами та сервісами, такими як Slack, Jira, HipChat та багатьма іншими. Ви можете легко інтегрувати Loggly з вашими іншими інструментами для автоматизації робочих процесів та спрощення взаємодії.

Хмарна платформа: Loggly пропонує хмарний підхід до журналювання, що забезпечує легкість встановлення, масштабованість та доступність. Ви можете швидко розгорнути Loggly та почати збирати та аналізувати лог-файли без необхідності установки та управління власною інфраструктурою [14].

Легкість використання: Loggly має інтуїтивно зрозумілий інтерфейс, який дозволяє легко налаштовувати і користуватися платформою. Вам не потрібно мати глибокі технічні знання для початку використання Loggly та отримання цінної інформації з лог-файлів.

Моніторинг в реальному часі: Loggly забезпечує моніторинг лог-файлів в реальному часі, що дозволяє вам відстежувати стан системи та виявляти потенційні проблеми миттєво. Ви можете отримувати повідомлення про критичні події та приймати швидкі заходи для усунення проблем.

Розширені можливості пошуку: Loggly має потужний двигун пошуку, який дозволяє швидко знаходити потрібну інформацію великих обсягів лог-файлів. Ви можете застосовувати складні фільтри та пошукові запити для точного виділення важливих даних.

Автоматизований алертинг: Loggly дозволяє налаштовувати автоматичне сповіщення та алерти на основі певних умов. Це допомагає оперативно виявляти проблеми та реагувати на них вчасно.

Обмежені інтеграції: Одним з недоліків Loggly є обмежена кількість інтеграцій з іншими інструментами порівняно з іншими рішеннями на ринку. Це може бути недоліком для організацій, які прагнуть синхронізувати журнали з багатьма іншими інструментами та сервісами.

Цінова політика: Loggly пропонує платні плани, а це може бути обмеженням для деяких організацій з обмеженим бюджетом. Вартість використання Loggly може залежати від обсягу даних та потреб користувача, тому перед вибором потрібно уважно оцінювати витрати.

Загалом, Loggly є потужною хмарною платформою журналювання з великим набором функцій та переваг. Він надає легкість використання, розширені можливості пошуку та аналізу даних, а також автоматизований алертинг. Однак, обмежені інтеграції та цінова політика можуть бути факторами, які слід враховувати при розгляді Loggly як рішення для вашої організації.

1.4 Постановка завдання

Аналіз подій, що відбуваються на сервері та швидке виявлення підозрілих подій є досить важливою складовою у роботі кіберполігону. Graylog є досить важливим інструментом для збору, аналізу та візуалізації журналів, який забезпечить усе необхідне для зручного функціоналу в середовищі

кіберполігону. Більш детальне порівняння функціонала Graylog з аналогічними за функціоналом програмними засобами показано у таблиці 1.2.

Таблиця 1.2 – Результат порівняння функціонала Graylog з аналогами

Функціонал	Elastic Stack	Splunk	Graylog	Loggly
Збір логів	Elasticsearch та Logstash забезпечують збір логів з різних джерел	Можливість збирати логи з різних джерел	Збір логів з різних джерел	Збір логів з різних джерел
Аналіз логів	Elasticsearch надає потужний механізм пошуку, фільтрації та аналізу лог-даних	Розширений аналіз лог-даних, включаючи запити та звіти	Пошук, фільтрація, аналіз та візуалізація лог-даних	Аналіз лог-даних, включаючи пошук та фільтрацію
Візуалізація	Kibana дозволяє створювати графіки та дашборди на основі лог-даних	Вбудований інструмент візуалізації з можливістю створення графіків, діаграм та інших візуальних компонентів	Можливість візуалізувати дані у реальному часі та створювати власні графіки	Візуалізація лог-даних на основі шаблонів та настроювання
Моніторинг	Можливість моніторити лог-дані у реальному часі	Моніторинг лог-даних та статусу системи у реальному часі	Моніторинг лог-даних та системних параметрів	Моніторинг лог-даних та інфраструктури
Алертинг	Elastic Stack може надсилати сповіщення на основі визначених умов	Система алертів для сповіщення про події та стан системи	Система алертів для сповіщення про події та помилки	Алерти на основі заданих умов
Інтеграція	Широкі можливості інтеграції з іншими інструментами та сервісами	Широкі можливості інтеграції з різними системами та сервісами	Інтеграція з іншими системами та сервісами	Обмежені інтеграції з іншими сервісами та інструментами

Централізований збір журнальних дозволить збирати журнальні дані з різних джерел, включаючи сервери, додатки та мережеві пристрої. Це дасть

змогу збирати і аналізувати всі події, що відбуваються в мережі кіберполігону, і забезпечує централізований погляд на всі дані.

Моніторинг та аналіз подій у реальному часі забезпечить можливість оперативно реагувати на потенційні загрози та інциденти безпеки. Візуалізація журнальних даних у вигляді графіків та графіків сприяє швидкому виявленню аномалій та підозрілих активностей.

Graylog має розширені функції пошуку та фільтрації журнальних даних, що дозволяє виконувати детальний аналіз подій та шукати специфічну інформацію. Це допомагає виявляти вразливості, атаки та несправності в системі кіберполігону. Також Graylog підтримує інтеграцію з іншими інструментами моніторингу та безпеки, такими як системи SIEM (Security Information and Event Management). Це дозволяє покращити синхронізацію та обмін даними між різними системами, що сприяє комплексному аналізу та виявленню загроз.

Унікальною властивістю у Graylog є можливість налаштування правил спостереження та реагування на події. Іншими словами – це можливість встановити автоматичні оповіщення, запускати скрипти або виконувати інші дії при специфічних умовах або виявленні підозрілого знаку.

Загалом, Graylog є потужним інструментом для збору, аналізу та візуалізації журналів, який може допомогти в побудові ефективного кіберполігону шляхом моніторингу та виявлення потенційних загроз та інцидентів безпеки у режимі реального часу. Його розширені можливості аналітики та інтеграція з іншими інструментами роблять його привабливим варіантом для організацій, які прагнуть підвищити рівень безпеки серверних систем.

2 ПРОЕКТУВАННЯ СЕРЕДОВИЩА ТА АЛГОРИТМИ РОБОТИ МЕХАНІЗМІВ GRAYLOG

2.1 Визначення вимог до середовища

Визначення вимог до середовища для побудови кіберполігону включає ідентифікацію ключових параметрів та функцій, які повинні бути забезпечені для ефективної роботи кіберполігону. Основні вимоги можна поділити на кілька категорій:

1) Безпека:

– фізична безпека: Забезпечення безпеки серверних приміщень, мережевого обладнання та інфраструктури для захисту від несанкціонованого доступу;

– логічна безпека: Застосування механізмів автентифікації, авторизації та контролю доступу, шифрування даних та захисту від кібератак;

2) Інфраструктура:

– системи зберігання даних: Наявність потужних та надійних систем зберігання даних для обробки та аналізу великих обсягів інформації;

– мережева інфраструктура: Надійні та швидкі мережеві з'єднання для передачі даних між компонентами кіберполігону та зовнішніми джерелами;

3) Масштабованість:

– гнучкість мережі: Здатність розширювати мережу для підключення нових компонентів та забезпечення високої пропускної здатності;

– розширюваність ресурсів: Можливість додавання нових серверів та обчислювальних ресурсів для врахування зростаючих потреб кіберполігону;

4) Відтворюваність:

– відтворення кібератак: Здатність відтворювати реальні кібератаки для аналізу та тестування ефективності заходів безпеки;

– повторюваність результатів: Забезпечення точності та повторюваності результатів тестування та аналізу;

5) Моніторинг та аналітика:

– система моніторингу: Наявність системи моніторингу для виявлення активності, інцидентів та незвичайної поведінки;

– аналітичні засоби: Можливість аналізувати зібрані дані для виявлення тенденцій, патернів та критичних вразливостей;

6) Гнучкість:

– підтримка різних типів тестування: Забезпечення можливості проведення різних видів тестів, включаючи вразливість, стійкість та відновлення після кібератак;

– інтеграція з іншими системами: Здатність інтегруватись з іншими системами кібербезпеки для обміну даними та спільної роботи;

7) Навчання та підтримка:

– документація: Наявність документації, яка описує функціональні можливості, налаштування та процедури роботи з кіберполігоном;

– навчання та підтримка: Забезпечення навчальних матеріалів, тренінгів та підтримки користувачам для ефективного використання кіберполігону;

Проаналізувавши основні категорії вимог до побудови кіберполігону та визначившись з потребами в рамках лабораторного стенду, було прийнято рішення зосередити увагу на таких пунктах: моніторинг та аналітика, гнучкість, навчання та підтримка. Дані пункти є основними, оскільки дана система розрахована на різноманітні методи використання, як для впровадження у глобальну систему університету так і для навчального процесу студентів, за для проведення лабораторних чи практичних роботі.

2.2 Підготовка конфігурації

Після визначення, які саме задачі та функції необхідні у даному кіберполігоні, необхідно визнати відповідну до вимог конфігурацію. При побудові кіберполігону поняття конфігурація можна поділити на 2 основні частини, а саме: конфігурація фізичного середовища, конфігурація програмної складової.

2.2.1 Встановлення та налаштування фізичних серверів та мережевої інфраструктури.

Встановлення та налаштування фізичних серверів та мережевої інфраструктури для побудови кіберполігону в університеті вимагає деяких кроків та процесів. Після попереднього аналізу вимог та наявного обладнання, було прийняте рішення побудувати мережу, яка за необхідності може масштабуватись та використовуватиме мінімальну кількість обладнання для базової і коректної роботи.

Загальна мережева структура складається з 3 основних складових.

1) Сервер і моніторинг. В якості серверу виступає одна з найпотужніших, за конфігурацією, машина, оскільки сервер повинен швидко обробляти усі запити і події що відбуваються. Моніторинг не обов’язково повинен буди розміщеним на серверному комп’ютері, завдяки цьому є можливість розширити кількість систем моніторингу на одному сервері, або навпаки, підключити декілька серверів до одного монітору.

2) Комп’ютери з боку атакуючої сторони. Кількість комп’ютерів, що проводять атаку на сервер залежить від можливостей мережевого обладнання. В якості операційних систем, встановлених на атакуючі машини можуть виступати: Windows, Linux, Ubuntu. Також можливий варіант проведення атаки з віртуальних машин, розгорнутих на ОС Windows.

3) Мережеве обладнання та вузли мережі. Мережеве обладнання відповідає за кількість підключених комп’ютерів та різноманітність способів їх підключення до загальної мережі в основі якої знаходиться сервер. В залежності від обладнання можливо реалізувати атаку через пряме підключення до серверу, підключення через Wi-Fi чи мережу інтернет. Комп'ютери-сервери можуть бути різних типів, спеціалізованих для виконання серверних завдань та надання різних послуг. Комп'ютери-сервери бувають декількох типів: баштовий сервер, шасі-сервер, сервери на основі хмари, мікросервер.

Схематичне зображення побудованої мережі кіберполігону зображено на рисунку 2.1.

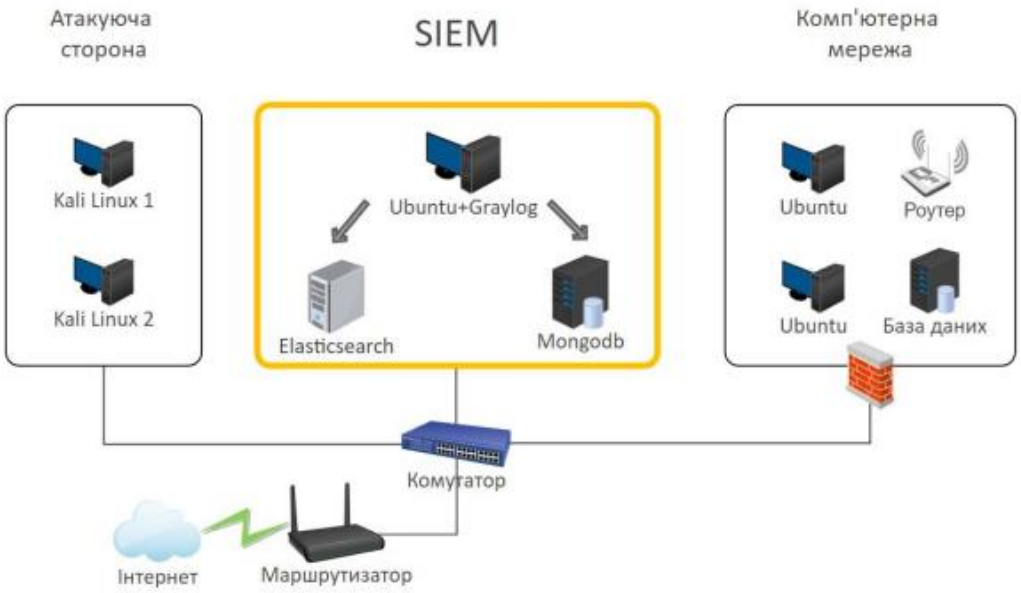


Рисунок 2.1 – Схема загальної мережі кіберполігону

2.2.2 Розгортання необхідного програмного забезпечення та налаштування оперативної системи.

Як сервер було обрано одну з найпотужніших машин, наявних у вільному доступі. Вибір зумовлено тим, що сервер повинен працювати якомога швидше, для забезпечення зв’язку з іншими комп’ютерами та обладнанням підключеним до мережі.

Як основна операційна система використовується остання версія ОС Ubuntu:22.04. Ubuntu – це одна з найпопулярніших та визнаних операційних систем з відкритим вихідним кодом. Вона базується на лінуксовому ядрі і розробляється і підтримується компанією Canonical Ltd. Ubuntu надає відмінну комбінацію простоти використання, стабільності та безпеки, що робить її відмінним вибором для домашніх, комерційних та серверних середовищ [14].

Необхідно відзначити, що Ubuntu є популярним вибором для серверних систем, забезпечуючи надійність, швидкість та безпеку. Вона підтримує широкий спектр серверних програм та має велику підтримку у сфері хмарних технологій.

Таким чином, при використанні Ubuntu, як серверної ОС, можливо уникнути специфічних налаштувань і використовувати її одразу для подальшого

розгортання серверу. Також, дана операційна система є безкоштовною, що дає змогу зекономити фінанси і використати їх підвищення потужності серверу.

Після встановлення операційної системи необхідно встановити та оновити до останньої версії пакет Java, який необідний для коректної роботи певних компонентів системи моніторингу. Мінімальна рекомендована для встановлення версія – Java 8. Для встановлення необхідно виконати такі команди [15].

Перед встановленням Java рекомендується оновити системні пакети : `sudo apt update && sudo apt -y full-upgrade .`

Встановлюємо Java 11 :

```
sudo apt update
sudo apt install vim apt-transport-https openjdk-11-jre-headless uuid-runtime pwgen curl dirmngr
```

Для перевірки версії Java використовується команда : `java -version`. Результат успішного становлення Java показано на рисунку 2.2.

Рисунок 2.2 – Результат успішного становлення Java

2.3 Алгоритм взаємодії між компонентами Graylog

Загальна конфігурація системи моніторингу на основі Graylog складається із декількох компонентів, взаємодія між якими забезпечує коректне функціонування усієї системи. Схема взаємодії між компонентами Graylog, серверною машиною та користувачем зображено на рисунку 2.3.

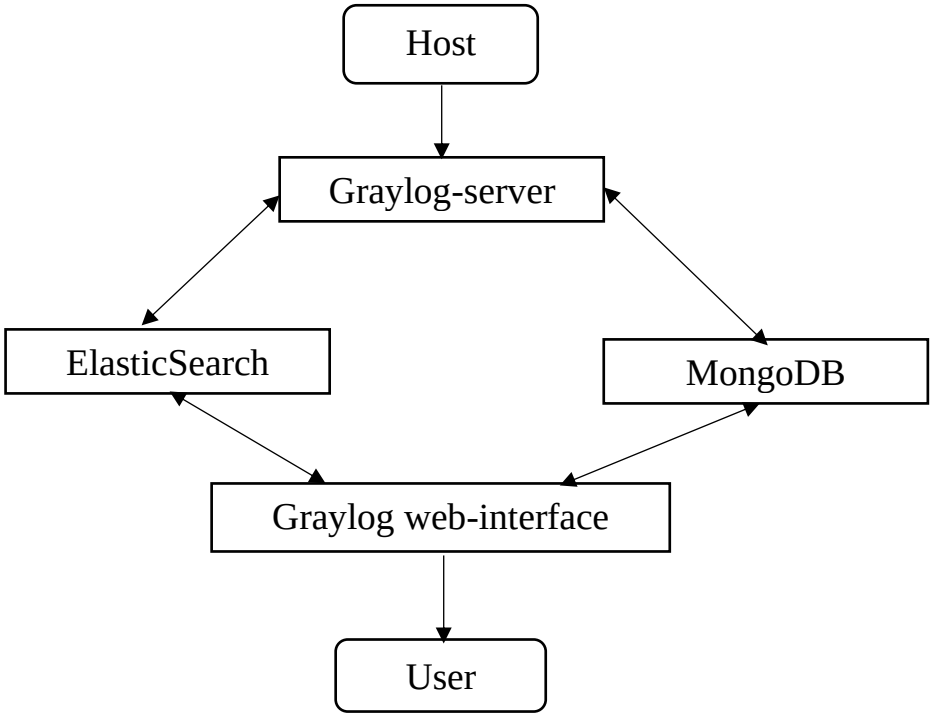


Рисунок 2.3 – Схема взаємодії між компонентами Graylog

В якості хоста виступає комп’ютер, на якому будуть встановлені усі наступні компоненти. Компоненти можуть бути встановлені одразу на серверну машини і працювати безпосередньо на ній, без використання додаткового обладнання.

Першим компонентом для встановлення є Graylog Server. Це головний компонент системи, який виконує роль центрального сервера. Він приймає дані з різних джерел, обробляє їх, зберігає у базі даних і надає можливість пошуку, фільтрації та візуалізації даних через веб-інтерфейс.

Наступним компонентом виступає Elasticsearch. Це розподілена пошукова та аналітична система, яка використовується Graylog для зберігання та індексування лог-даних. Elasticsearch забезпечує швидкий доступ до даних та потужні можливості пошуку та аналітики.

Для реалізації збереження даних встановлюється MongoDB. Ця база даних використовується Graylog для зберігання метаданих системи, таких як конфігураційна інформація, правила появлення та інші дані, що використовуються для функціонування системи.

Після налаштування попередніх трьох компонентів з’явиться доступ до Web Interface. Це веб-інтерфейс, який надає користувачам можливість

взаємодіяти з Graylog. Ви можете переглядати лог-дані, налаштовувати правила появлення, створювати та відстежувати оповіщення, аналізувати дані за допомогою графіків та інших інструментів.

Ці компоненти взаємодіють між собою таким чином:

– graylog Server приймає лог-дані від різних джерел та розподіляє їх для обробки;

– дані проходять через обробку та індексацію в Elasticsearch для забезпечення швидкого доступу до них;

– mongoDB використовується для зберігання метаданих системи, таких як правила появлення, конфігураційна інформація та інше;

– з Graylog Web Interface користувачі можуть переглядати, фільтрувати та аналізувати лог-дані через веб-браузер;

Така взаємодія компонентів дозволяє Graylog ефективно збирати, зберігати та аналізувати лог-дані, що допомагає забезпечити централізоване керування та моніторинг логів у середовищі.

2.4 Алгоритми роботи сповіщень та потоків логів

Одними з найважливіших особливостей Graylog є можливість фільтрації логів, створюючи відповідні потоки лог-даних, та оповіщення оператора системи за певних обставинах чи подіях виниклими під час роботи серверу. Кожен з цих методів має свій певний алгоритм роботи, котрі варто розуміти під час налаштування системи.

2.4.1 Алгоритм роботи механізму сповіщень

В Graylog alerts (сповіщення) використовуються для виявлення певних умов або подій у лог-даних та автоматичного сповіщення про них. Робота з alerts в Graylog включає такі кроки:

– налаштування правил: спочатку налаштовуються правила, що визначають умови, за яких має спрацювати сповіщення. Можливо використовувати різні умови, такі як ключові слова, рівні журналювання, часові

пояси, агрегації тощо. Наприклад, правило може виявляти певний тип атаки або несправність системи;

– створення сповіщень: Після налаштування правила необхідно створити сповіщення, вказуючи спосіботримання повідомлення. Graylog підтримує різні способи сповіщення, такі як електронна пошта, Slack, HTTP-запити, Discord, Telergam і багато інших. Також можливо можете встановити канали сповіщень та налаштувати шаблони повідомлень;

– тестування та налагодження: Перед активацією правил і сповіщень важливо протестувати їх, щоб переконатися в їх коректності та працездатності. Graylog надає можливість виконати тестові запити або симулювати події для перевірки відповіді системи на правила та відправку сповіщень;

– моніторинг та аналіз: Після активації сповіщень Graylog буде автоматично моніторити лог-дані та перевіряти їх на відповідність правилам. Якщо виявляється відповідна умова, система спрацьовує та надсилає сповіщення до налаштованих каналів;

Після отримання сповіщення оператор системи може проаналізувати подію, з'ясовувати причини та приймати відповідні заходи. При необхідності можливо вносити зміни в правила або налаштування сповіщень, щоб вдосконалити систему виявлення та сповіщення. Схема роботи системи сповіщень показана на рисунку 2.7.

Рисунок 2.7 – Схема роботи системи сповіщень

Завдяки циклу налаштування, тестування та аналізу, alerts в Graylog допомагають виявляти потенційні проблеми та інциденти безпеки, що дозволяє оперативно реагувати на них та забезпечувати безпеку інформаційної системи.

2.4.2 Алгоритм роботи механізму потоків

У Graylog streams (потік) є механізмом для організації та керування лог-даними, що надходять до системи. Stream дозволяє фільтрувати та спрямовувати лог-події до відповідних категорій для подальшого аналізу та обробки. Схема роботи механізму потоків лог-даних зображено на рисунку 2.8.

Рисунок 2.8 – Схема роботи механізму потоків лог-даних

1) Налаштування потоків: Користувачі налаштовують потоки в Graylog, визначаючи критерії фільтрації для лог-подій. Критерії можуть включати ключові слова, джерела, рівні журналювання та інші параметри. Наприклад,

потік може бути налаштований для фільтрації всіх лог-подій, пов'язаних з певним додатком або сервером.

2) Маршрутизація лог-даних: Коли лог-події надходять до Graylog, система використовує налаштовані потоки для визначення, до якого потоку вони повинні бути направлені. Лог-події, що відповідають критеріям потоку, автоматично маршрутизуються до цього потоку для подальшої обробки.

3) Аналіз та обробка в потоках: У кожному потоці можуть бути встановлені різні правила аналізу та обробки лог-подій. Наприклад, можуть бути визначені фільтри, що виключають певні події або сповіщення про критичні проблеми. Крім того, можна виконувати додаткові дії, такі як індексування лог-подій, виклик зовнішніх сервісів або відправка сповіщень.

Після маршрутизації лог-подій до потоків Graylog надає різноманітні можливості для подальшого аналізу та візуалізації даних, а саме:

- сортування потоку за різноманітними параметрами;
- статистичні данні по кількості логів;
- статистичні дані про використання трафіку;
- візуалізація графіку активісті в певні проміжки часу;

Оператор системи може переглядати лог-події у потоках, застосовувати фільтри, виконувати пошук та використовувати інструменти аналізу для отримання цінної інформації з журналу подій.

Загалом, потоки в Graylog дозволяють категоризувати, фільтрувати та організовувати лог-події для ефективного аналізу та обробки. Вони допомагають зосередитися на конкретних аспектах системи або додатків, спрощують моніторинг та аналітику лог-даних, що робить їх потужним інструментом для кібербезпеки та адміністрування систем.

2.5 Висновки до 2 розділу

В ході проектування системи було розглянуто основні принципи побудови кіберполігонів та необхідних компонентів для його побудови. Основними критеріями при побудові кіберполігону виступатиме забезпечення високої надійності та можливість масштабування системи, шляхом додання нового обладнання.

Було проаналізовано принципи роботи компонентів системи моніторингу Graylog та визначення основних деталей для подальшого їх налаштування. Досліджено принципи взаємодії між компонентами та розглянуто алгоритми та послідовність їх встановлення та налаштування.

Детально розглянуто алгоритми роботи фільтрації лог-даних, а саме, основні критерії за якими може відбуватися фільтрація та де саме вона застосовується. Проаналізовано алгоритми роботи потоків та принципи їх налаштування та застосування у системі моніторингу.

Розглянуто системи сповіщення, необхідність їх використання та принципи їх застосування. Проаналізовано можливі типи сповіщень, можливі способи відправки та загальний алгоритм роботи усієї системи сповіщень.

3 РОЗГОРТАННЯ СИСТЕМИ ЛОГУВАННЯ

3.1 Конфігурація та розгортання системи логування

Загальна конфігурація системи моніторингу на основі Graylog складається із декількох компонентів, взаємодія між якими забезпечує коректне функціонування усієї системи.

Далі необхідно встановити додаток Elasticsearch. Elasticsearch – це інструмент, який використовується для зберігання та аналізу вхідних журналів із зовнішніх джерел. Після виконання певних команд, необхідних для встановлення та оновлення програмного засобу, необхідно налаштувати його для подальшої роботи з Graylog.

Необхідно змінити налаштування для Graylog [16]. Для цього потрібно перейти до файлу elasticsearch.yml за допомогою команди: `sudo vim /etc/elasticsearch/elasticsearch.yml .`

Встановлюємо ім’я за допомогою команди: `cluster.name: graylog .`

Встановлюємо прапорець для автоматичного створення індексів за допомогою команди: `action.auto_create_index: false .`

Далі необхідно перезапустити Elasticsearch server за допомогою настпного ряду команд:

```
sudo systemctl daemon-reload
sudo systemctl restart elasticsearch
sudo systemctl enable elasticsearch
```

Для перевірки успішного встановлення та налаштування Elasticsearch використовується команда: `systemctl status elasticsearch.` Результат успішного встановлення та налаштування Elasticsearch показано на рисунку 3.1.

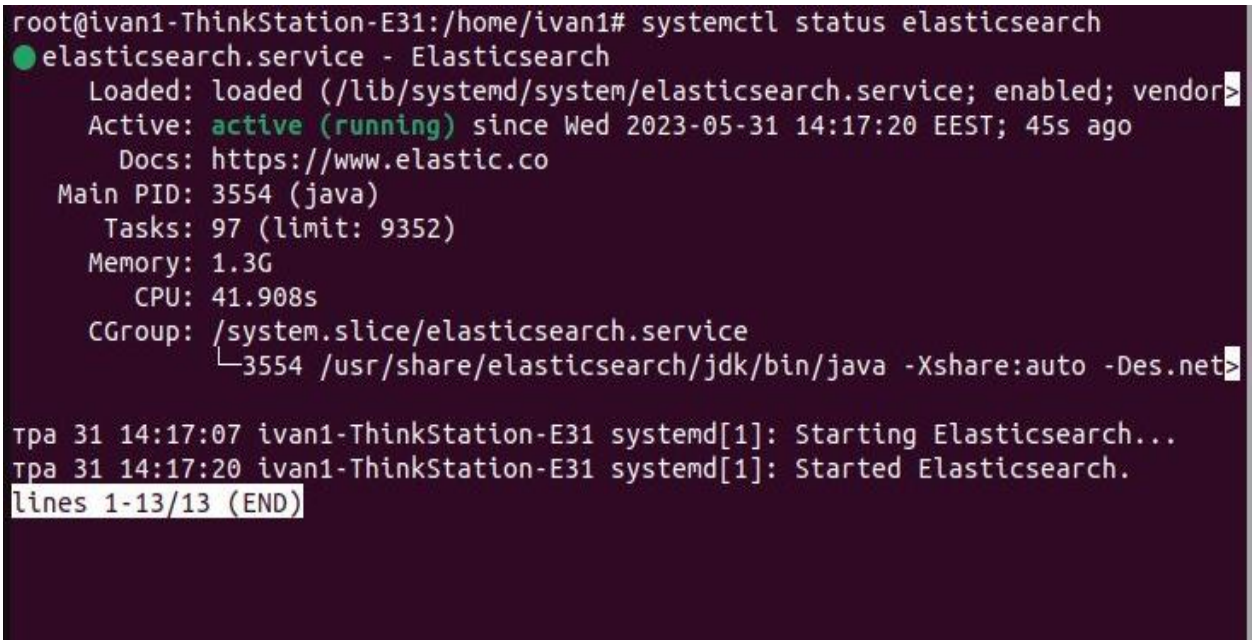


Рисунок 3.1 – Результат успішного встановлення та налаштування Elasticsearch

Наступним кроком необхідно встановити документовану систему управління базами даних Mongodb. Graylog використовує MongoDB як свою базу даних для зберігання лог-даних та інших важливих інформаційних об'єктів. Використання MongoDB дозволяє Graylog зберігати великі обсяги лог-даних та забезпечує швидкий доступ до цих даних.

Mongodb не потребує додаткового налаштування для роботи з Graylog, таким чином, необхідно виконати лише ряд стандартних команд для встановлення додатку та запустити його. Після успішного встановлення та запуску перевіряємо стан за допомогою команди: `systemctl status mongodb`. Результат успішного встановлення Mongodb зображено на рисунку 3.2.

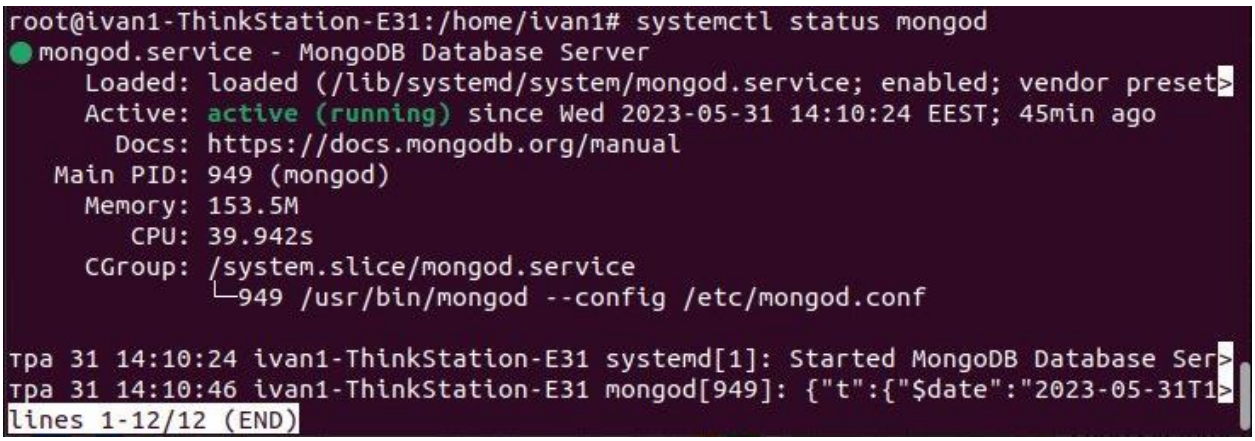


Рисунок 3.2 – Результат успішного встановлення Mongodb

В завершені необхідно встановити та налаштувати Graylog Server. Graylog – це система для аналізу та обробки лог-даних, призначенна для збирання логів з різних джерел, їх аналізу та відповідної візуалізації для забезпечення моніторингу та виявлення проблем у системі.

Для встановлення Graylog необхідно завантажити його з репозиторію за допомогою команд:

```
wget https://packages.graylog2.org/repo/packages/graylog-4.3-repository_latest.deb

sudo dpkg -i graylog-4.3-repository_latest.deb
```

Далі встановлюється Graylog server використовуючи спочатку команду для оновлення, а потім команду для встановлення самого серверу:

```
sudo apt update
sudo apt install graylog-server
```

Після встановлення Graylog server потрібно згенерувати спеціальний секретний пароль за допомогою команди: `pwgen -N 1 -s 96`. В результаті отримуємо унікальний секретній пароль розміром 96 символів.

Даний пароль необхідно занести до файлів конфігурації серверу. Файл конфігурації серверу знаходиться за шляхом /etc/graylog/server/server.conf і навпроти «password_secret = » приписується згенерований секретний пароль.

Для прив’язки веб-інтерфейсу до серверу необхідно зазначити IP адрему та порт. У файлі конфігурацій серверу знайти поле «http_bind_address» і встановити значення за таким патерном (IP:Port), у випадку коли сервер і веб-інтерфейс знаходяться на одній машині можливо використовувати наступне значення: 0.0.0.0:9000.

Наступним кроком є створення хеш-паролю sha256 для адміністратора. Це пароль, який знадобиться для входу у веб-інтерфейс. Для його отримання використовуються команди:

```
echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
Enter Password: password
```

В результаті буде отримано пароль котрий складається із 64 символів. Після отримання даного пароля необхідно занести його до файлу конфігурації у поле «root_password_sha2».

Останнім кроком буде перезапуск Graylog server, та Mongodb, використовуючи наступній ряд команд:

```
sudo systemctl daemon-reload
sudo systemctl restart mongodb graylog-server
sudo systemctl enable mongodb graylog-server
```

Щоб перевірити успішність налаштування Graylog server, потрібно перейти за посиланням наступного типу «http://<serverip_hostname>:9000». У випадку з проведеними налаштування посилання матиме такий вигляд «http://localhost:9000». При переході за даним посиланням відкриється вікно для входу до системи Graylog. Результат успішного налаштування Graylog server зображено на рисунку 3.3.

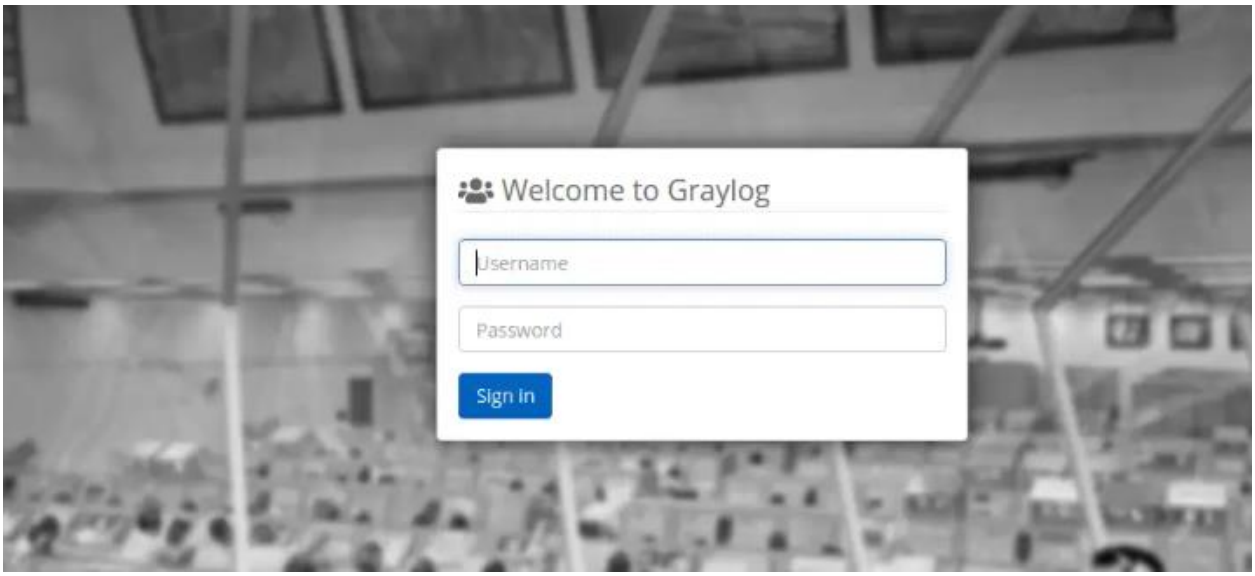


Рисунок 3.3 – Результат успішного налаштування Graylog server

3.2 Налаштування основних функцій Graylog

Щоб перейти до веб-інтерфейсу Graylog необхідно у веб браузері перейти за посиланням «http://localhost:9000» та заповнити поля для входу, а саме ім’я та пароль. Після входу у систему буде відображено стартова сторінка з посиланнями на різноманітні інструкції по налаштуванню різного типу функціоналу.

У шапці вікна знаходяться 6 вкладок з якими буде відбуватись основна робота. Список розпочинається із вкладки «Search», яка призначена для пошуку конкретного логу чи налаштування фільтрів для відповідного відображення логів, що відповідають вказаним критеріям. Візуальна складова вікна Search зображено на рисунку 3.4.

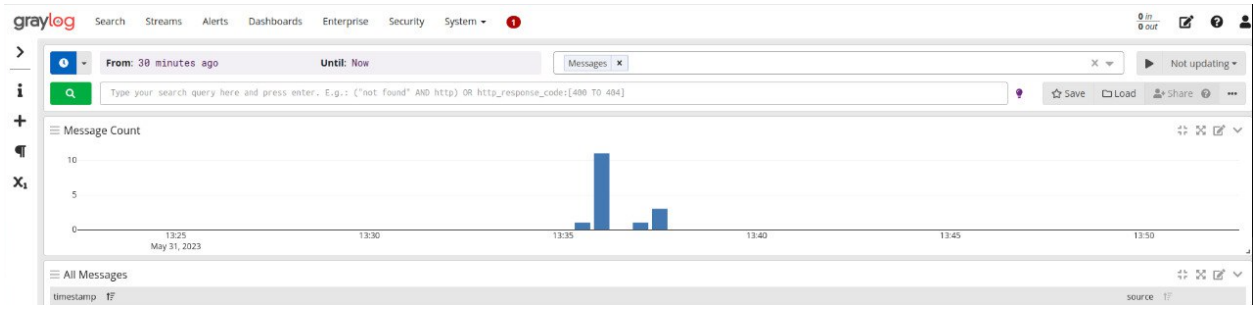


Рисунок 3.4 – Візуальна складова вікна Search

Наступна вкладка під назвою «Streams» відповідає за потоки лог-даних. Дані потоки створюють за замовчування і містять у собі усі дані про подій, системні події та повідомлення. Без цих трьох загальних потоків побачити будь яку реакцію на події у системі було б неможливо, що негативно відображалось би на розумінні системи.

Також можливо створювати власні потоки лог-даних, з певними критеріями для розмежування логів і полегшення їх подальшої обробки. Необхідно зазначити, що пошук певних логів також можливо виконувати у кожному потоці окремо, або навіть у декількох потоках одразу. Візуальна складова вікна Stream зображена на рисунку 3.5.

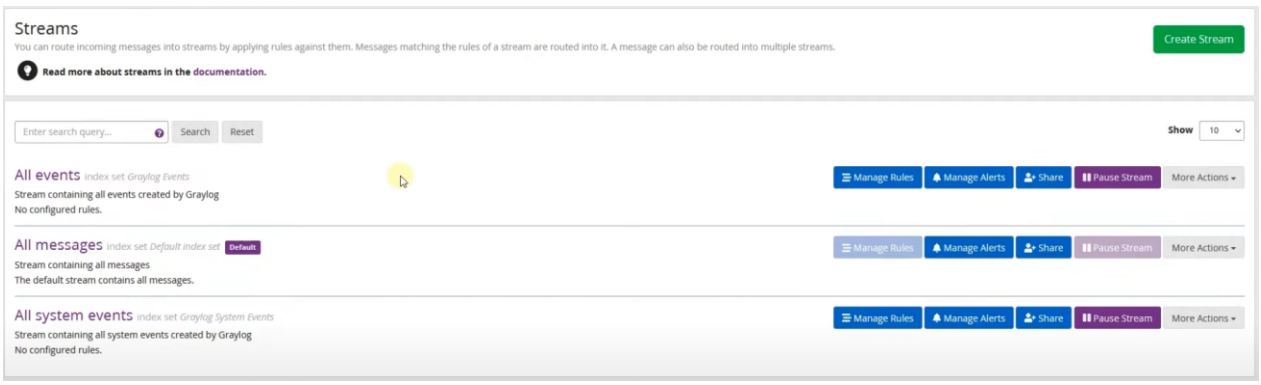


Рисунок 3.5 – Візуальна складова вікна Stream

Наступна вкладка «Alerts» відповідає за сповіщення користувача при виконанні певних умов. Оповіщення мають 2 основних критерія, коли відправляти повідомлення «Event Definitions» та яким чином їх відправляти «Notifications».

За замовчуванням система сповіщень не налаштована, тому дана вкладка є пустою, так само як і її гілки. При натисканні одну з клавіш з меню відкритого вікна Alerts буде відображено текстове повідомлення та кнопка з можливістю створити та налаштувати певний функціонал.

Вкладка «Dashboard» призначена для збору статистичних даних та їх відповідної візуалізації. В даній вкладці можливо налаштувати період для відображуваних даних та переглянути загальну статистику по взаємодії серверу з клієнтами.

Також є можливість налаштовування для конкретного клієнту, де саме відбулось більше всього помилок чи який з клієнтів веде підозрілу активність і у який час.

Далі йде вкладка «Enterprise», яка більш орієнтована на великі мережі. Дана вкладка є комерційною складовою і для її використання необхідно мати ліцензію.

Основними функціоналом, що знаходяться у даному розділі є можливість створення архівів лаг-даних для їх довготривалого зебрігання та формування звітів.

Останньою та самою великою по функціоналу є вкладка «System». Вона дає змогу працювати з наступним спектром можливостей:

- налаштування Graylog в цілому;
- налаштування клієнтів;
- загальний огляд системи, перегляд використаного трафіку;
- налаштування кластерів та вузлів серверів;
- відкриття портів для вхідних та вихідних даних ;
- налаштування перенаправлення лог-даних між серверами;
- налаштування терміну зберігання логів у базі даних;
- створення команди операторів системи;

– розподіл та створення ролей ;

– встановлення плагінів;

Дана вкладка є дуже важливою оскільки містить величезну кількість функціоналу. Також є пункти, які необов’язково змінювати, якщо користувач має не достатній рівень знань та навичок у роботі із системою Graylog.

3.3 Налаштування методів фільтрації

Налаштування фільтрація лог-даних у Graylog відбувається у трьох вкладках і мають свою певну зону поширення.

Seartch.

Фільтрація на вкладці Seartch необхідна для пошуку конкретних лагів. В якості основних методів виступають: фільтр за часовим проміжком, фільтр по потоку лог-даних, пошук по імені параметру.

Щоб налаштувати фільтр по часу необхідно натиснути на синю кнопку з годинником, у відкритому вікні буде список можливих часових термінів, від поточного часу і до певного проміжку у минулому. Для більш детальної фільтрації за часом необхідно натиснути на сусіднє поле з відображеними термінами часу. Після натискання відобразиться вікно, де можливо провести біль детальне налаштування, з якого часу і до якого необхідно відображати логи. Також можливо вказати дати по яким буде відбуватись фільтрація та ключове слово, відповідно до якого будуть відображатись логи. Результат налаштованого часового фільтру зображено на рисунку 3.6.

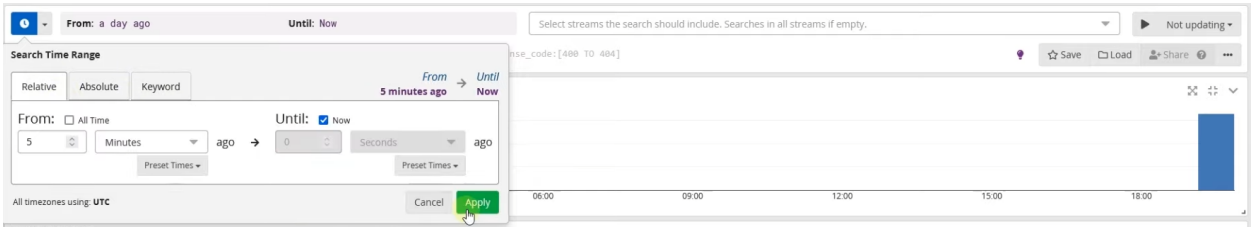


Рисунок 3.6 – Результат налаштованого часового фільтру

Для того щоб фільтрація по часу відбувалась в конкретному потоку лог даних необхідно натиснути на поле з відповідним написом «Select Streams…». При натисканні на поле з’явиться список із усіх існуючих потоків, за один раз

можливо обрати декілька потоків. За замовчуванням дане поле є пустим і фільтрація застосовується одразу до всіх потоків.

Нижче розташоване текстове поле, призначене для пошуку по логів і кнопка для застосування даного фільтру. Для виконання пошуку необхідно ввести назву параметру, за яким буде відбуватись пошук та, через двокрапку, ввести бажане значення. Результат пошуку по параметрам зображено на рисунку 3.7.

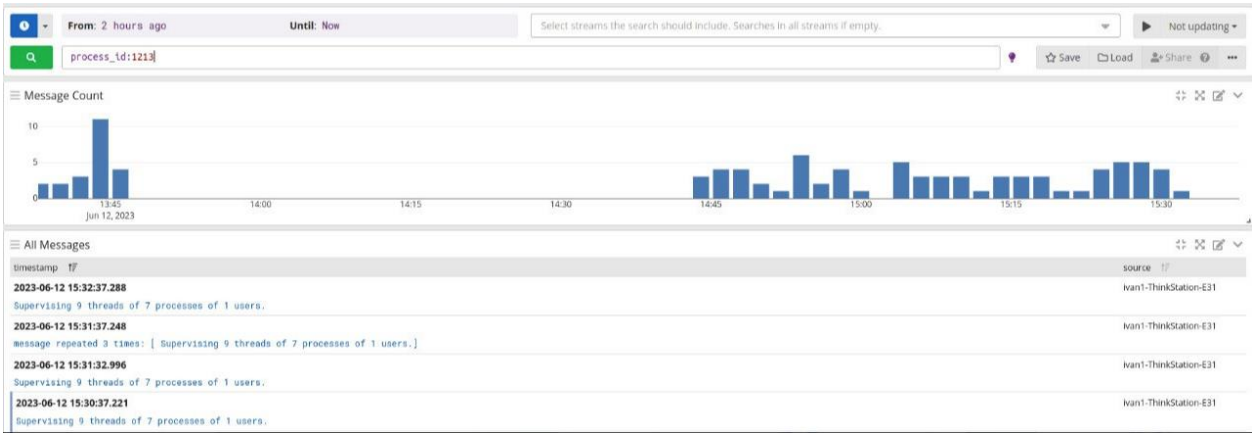


Рисунок 3.7 – Результат пошуку по параметрам

Також наявні кнопки для збереження налаштованого фільтру та загрузки уже файлу налаштувань з комп’ютера. І присутня кнопка для керуванням оновленням графічного інтерфейсу, що дає змогу налаштувати з якою частотою будуть відбуватись зміни на графіку, або взагалі вимкнути автоматичне оновлення і виконувати його лише при натисканні на відповідну кнопку.

Streams.

Фільтрація в потоках даних Streams подана у вигляді правил розподілу. Дані правила вказають які саме логи будуть належати до певного потоку. Кожен з потоків може містити одразу декілька правил, але тільки один тип лог-даних.

Необхідно відзначити, що редагувати привали базових потоків неможливо.

Фільтрацію також можливо виконувати відповідно у обраному потоці. Це можливо зробити на вкладці Search, що дасть змогу звузити пошук бажаної інформації.

3.4 Налаштування потоків лог-даних

Потоки лог-даних необхідні для групування логів за відповідними критеріями. Дана функція дає змогу розмежувати логи, котрі надходять від різних користувачів чи програм, використовуючи правила розподілу.

При переході на вкладку Streams одразу буть відображені три основні потоки лог-даних, а саме:

– All events – призначений для збирання та відображення усіх подій;

– All messages – призначений для збирання та відображення усіх логів;

– All system events – призначений для збирання та відображення усіх системний подій;

Дані потоки створені за допомогою Graylog і редагувати їх правила напряму неможливо.

Для створення власного потоку логів необхідно натисну на відповідну кнопку «Create Stream». Після натискання кнопки з’явиться вікно де необхідно вказати назву та опис створюваного потоку і індексацію логів. Також доступний прапорець, при встановлені якого усі логи, що відповідають правила створюваного потоку, будуть автоматично видалені із основного потоку «All messages». Після заповнення полів необхідно зберегти налаштування. Результат заповненого діалогового вікна для створення потоку лог-даних зображено на рисунку 3.8.

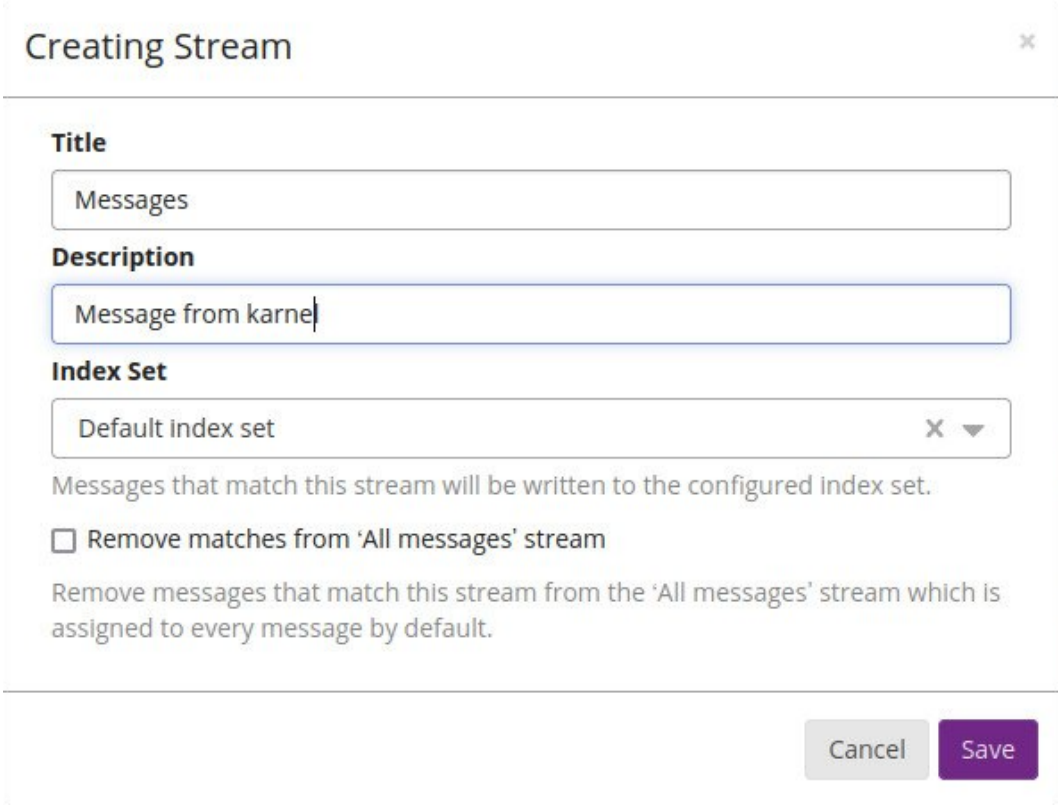


Рисунок 3.8 – Результат заповненого діалогового вікна для створення потоку

Щоб налаштувати правила для розподілу логів необхідно перейти до менеджера правил налаштовуваного потоку натиснувши кнопку «Manage Rules». Після переходу до вікна управління правилами обрати який саме тип логів буде знаходитись у даному потоці.

Далі необхідно створити правила для відбору лог-даних до даного потоку. Для цього необхідно натиснути на кнопку «Add stream rule», після чого з’явиться діалогове вікно з полями, що необхідно заповнити. У даному вікні необхідно вказати:

– параметр «Field», який необхідно відстежити;

– умову «Type», відповідно до якої необхідно перевіряти параметр. В даному полі неможливо встановити власну умов, є можливість обрати одну із запропонованих системою;

– значення «Value», яке повинно відповідати вказаному параметру;

– прапорець «Inverted», котрий вказує на інверсію правила, що відповідатиме правилу по типу (усі випадки крім даного);

– опис «Description», не обов’язкове поли призначене для відображення більш детальної інформації про створене правило;

Результат заповненого вікна для створення правила потоку зображено на рисунку 3.9.

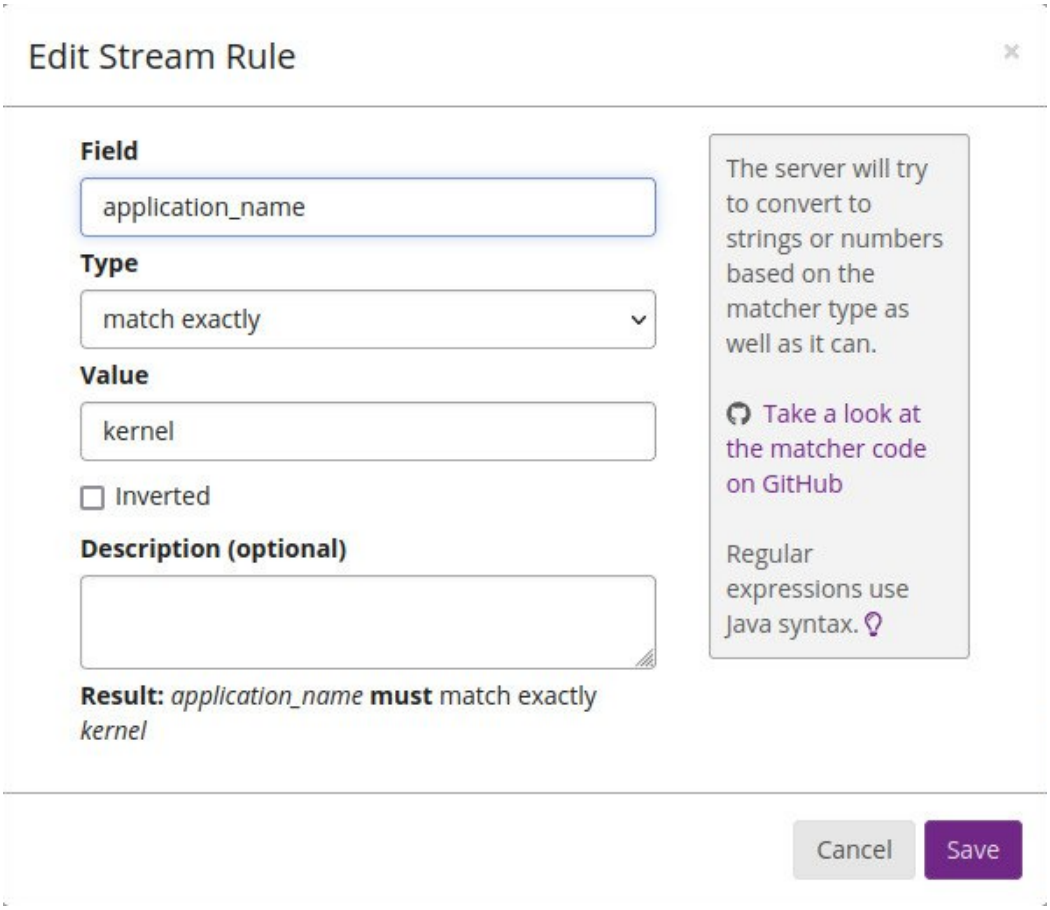


Рисунок 3.9 – Результат заповненого вікна для створення правила потоку

Останнім кроком необхідно обрати один з двох доступних параметрів відбору, згідно з встановленими правилами:

1. Лог-файл повинен відповідати усім встановленим правилам;

2. Лог-файл повинен відповідати хоча б одному із встановлених файлів;

Результат загального налаштування правил відбору до потоку показаний на рисунку 3.10.

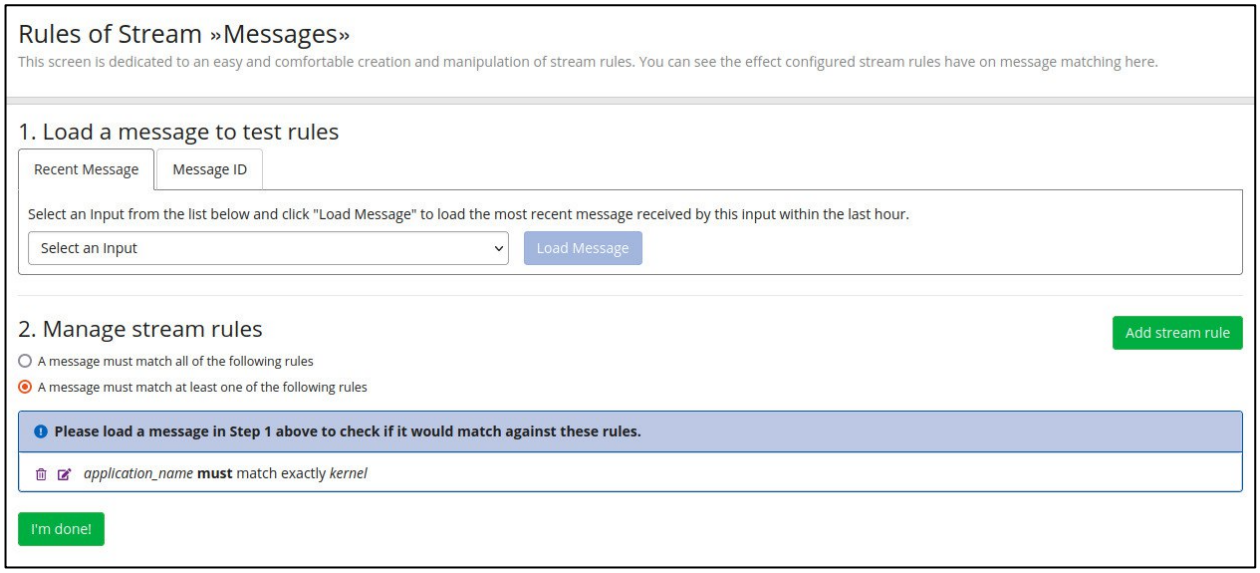


Рисунок 3.10 – Результат загального налаштування правил відбору до потоку

3.5 Налаштування системи подій сповіщень

При переході до вкладки Alerts необхідно натиснути на вкладку «Event Defenition», яка відповідає за створення, налаштування та створення подій. У доступному текстовому полі можливо обрати необхідну створено події із спливаючого списку, за замовчуванням даний список порожній. Щоб створити подію необхідно натиснути на кнопку «Create Event Defenition», що переправляє на відповідне вікно для налаштування події.

Налаштування подій розпочинається із запиту на встановлення імені, опису та пріоритету до створюваної події. Результат заповненого вікна деталей подій зображено на рисунку 3.11.

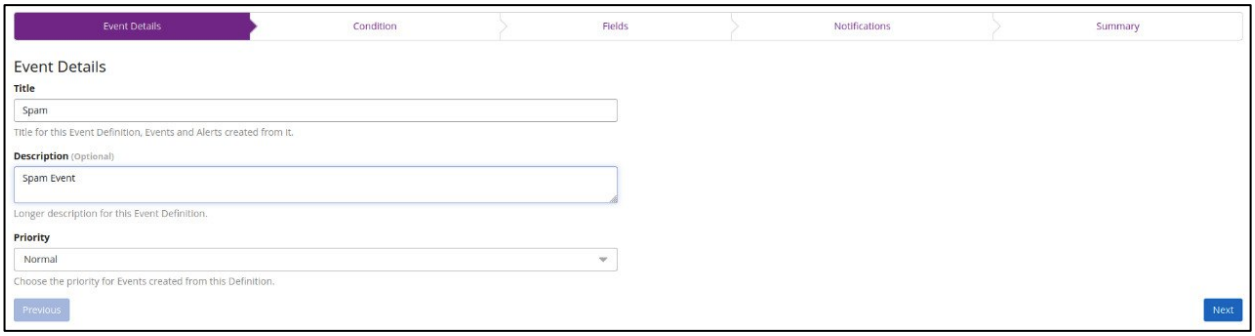


Рисунок 3.11 – Результат заповненого вікна деталей подій

Далі необхідно натиснути на кнопку «Next», щоб перейти до наступного етапу налаштування, або обрати відповідний пункт у верхньому меню. Наступним кроком буде налаштовано фільтрація за критеріями логу та налаштування умов спрацювання події.

Для налаштування умов, необхідно обрати у полі спливаючого списку пункт «Filter & Aggregation», за замовчуванням поле пусте. Після заповнення даного поля з’являться поля для налаштування фільтрації та умов. Поля заповнюються наступним чином:

– встановлюється значення, яке повинно міститись у повідомленні;

– обираються потоки на які буде розповсюджуватись подія;

– встановлюється термін «за останній проміжок часу»;

– встановлюється проміжок «виконувати кожних…»;

Останнім встановлюється прапорець в один за пунктів, фільтрація за результатом або обробка за умовою. Результат налаштованого методо фільтрації для подій зображено на рисунку 3.12.

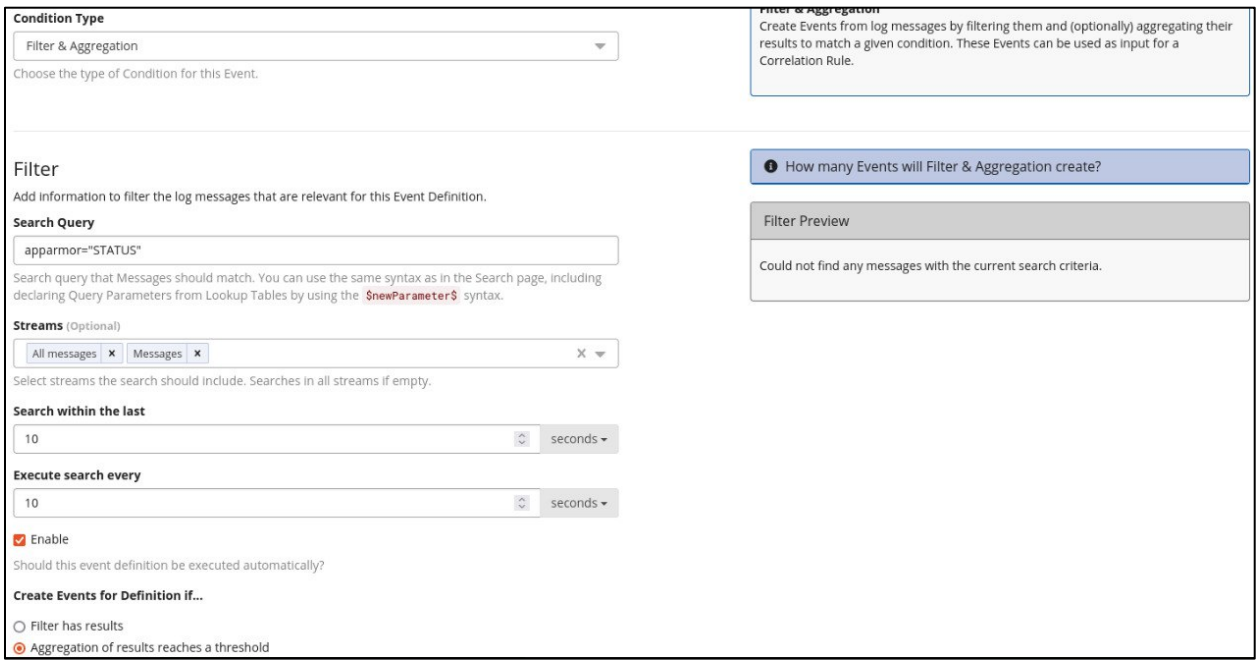


Рисунок 3.12 – Результат налаштованого методо фільтрації для подій

Якщо обрати пункт з налаштування умов спрацювання, з’являться додаткові поля для налаштування умов. Необхідно вказати параметр, який

необхідно перевіряти, обрати його можна з спливаючого списку. Далі встановлюється умова, за якою буде перевірятись обраний параметр. Умова складається з декількох компонентів:

– основна умова, від якої заложать інші;

– умова порівняння, яка порівнює результат основної умові із встановленим значенням;

– встановлене значення, яке виступає у ролі константи;

В результаті заповнення полів умов, у текстовому вікні буде зображено відображено код, що відповідає встановленим налаштуванням. Результат заповнення полів умови зображено на рисунку 3.13.

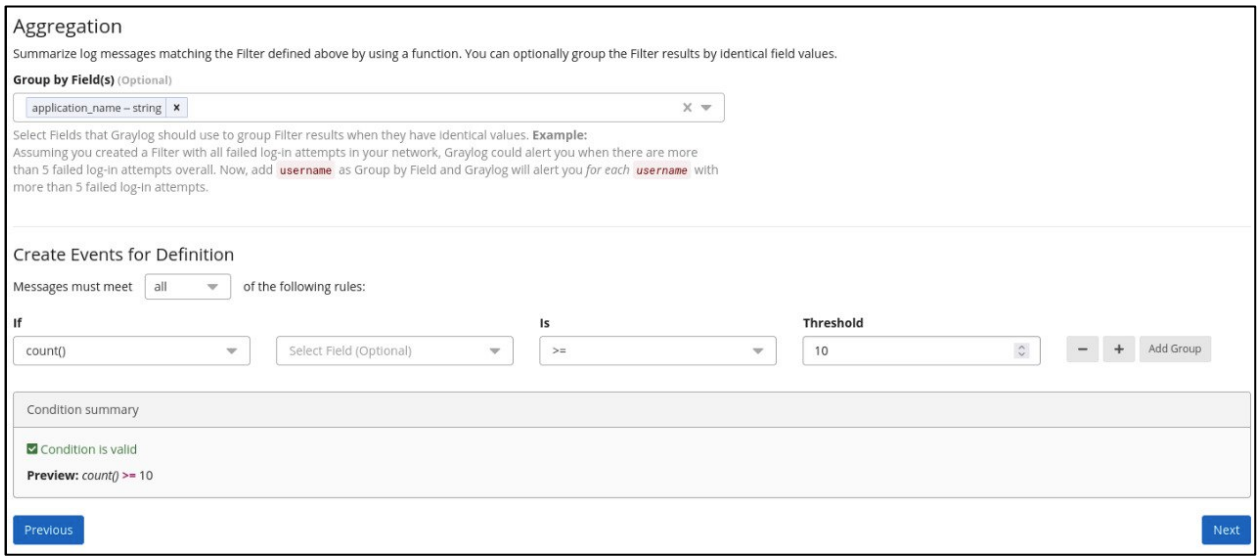


Рисунок 3.13 – Результат заповнення полів умови

В результаті буде створено подію, відповідно до якої можливо виконувати різноманітні налаштування, одним із яких є оповіщення. Результат створення події зображено на рисунку 3.14. У вікні Alerts одразу можливо налаштувати оповіщення та зв’язати його із певною подією.

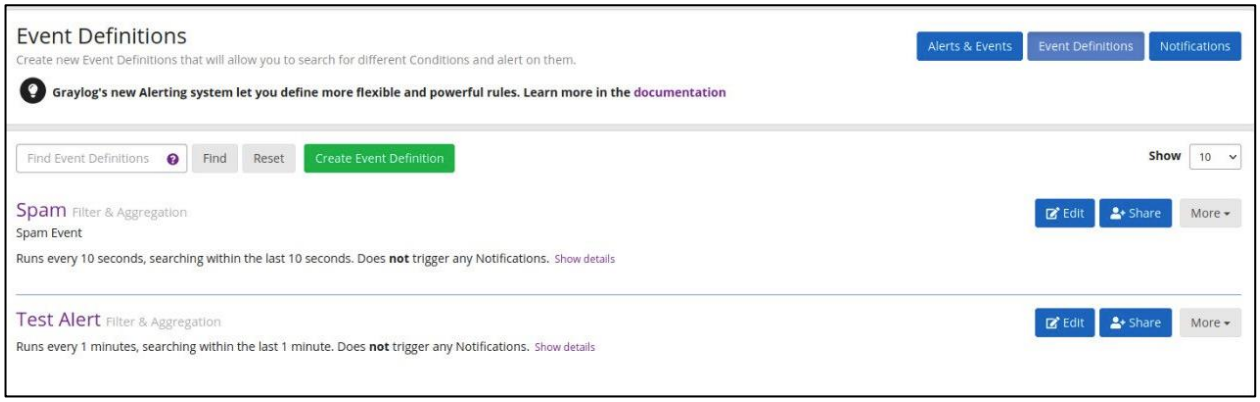


Рисунок 3.14 – Результат створення події

Система оповіщень в Graylog базується на двох основних компонентах: правилах (rules) та джерелах (sources). Правила визначають умови, за яких спрацьовують оповіщення, а джерела вказують, з яких джерел лог-даних мають бути отримані повідомлення для оповіщень.

Існує кілька типів оповіщень, доступних в Graylog:

– email: Цей тип оповіщення використовується для відправки сповіщень на електронну пошту. Ви можете налаштувати отримання повідомлень на вказану електронну адресу або навіть на декілька адрес;

– slack: Graylog може надсилати сповіщення в Slack, що дозволяє вам отримувати повідомлення у вказаних каналах;

– webhook: Цей тип оповіщення дозволяє надсилати HTTP-запити на зазначений URL з інформацією про подію;

– syslog: Якщо ваша інфраструктура використовує протокол Syslog, Graylog може надсилати оповіщення через цей протокол до вказаного Syslog-сервера;

Також доступні різноманітні пакети розширення, для забезпечення більшого спектру можливостей для отримання сповіщень. Можливо встановити плагіни для відправки повідомлення по соц-мережам, наприклад Telegram чи Viber, або іншим додаткам, наприклад Discord.

Далі будуть розглянуті два найпопулярніших методи оповіщення, а саме по Telegram та Email.

3.5.1 Налашутвання системи сповіщень Telegram

Для реалізації системи сповіщень за допомогою Telegram необхідно створити та налаштувати Telegram-бота та підключити його до системи Graylog, виконавши відповідні налаштування.

Створити Telegram-бота можливо за допомогою уже існуючого офіційного бота, знайти його можна по імені «BotFather». Натиснувши кнопку «Старт» чи за допомогою команди /start, бот дасть список команд з їх коротким описом. За допомогою команди /newbot буде розпочато опитування для встановлення відображуваного імені та імені користувача «username», ім’я користувача обов’язково повинно мати закінчення «bot».

Після виконання даного алгоритму BotFather надасть посилання на щойно створеного бота та токен, який необидний для прив’язки до Graylog. Результат виконання алгоритму створення бота зображено на рисунку 3.15.

Наступним кроком необхідно встановити плагін Telegram в Graylog. У Graylog існує плагін Telegram, який дозволяє надсилати сповіщення на телеграм-акаунт, в якості якого виступає раніше створений бот. Для встановлення даного плагіну необхідно виконати команду: graylog-plugin install graylog-plugin-alerts-telegram, або завантажити необхідний .jar файл з GitHub власноруч перемістити його до каталогу «plugins»ю.

Налаштування плагіну Telegram в Graylog. Необхідно відредагувати файл server.conf за шляхои /etc/graylog/server/server.conf. Додаються наступні параметри конфігурації:

– telegram_api_token = YOUR_BOT_TOKEN,

де «YOUR_BOT_TOKEN» необхідно замінити на токен створеного бота;

– telegram_chat_id = YOUR_CHAT_ID,

де «YOUR_CHAT_ID» необхідно замінити на ID чату створеного бота.

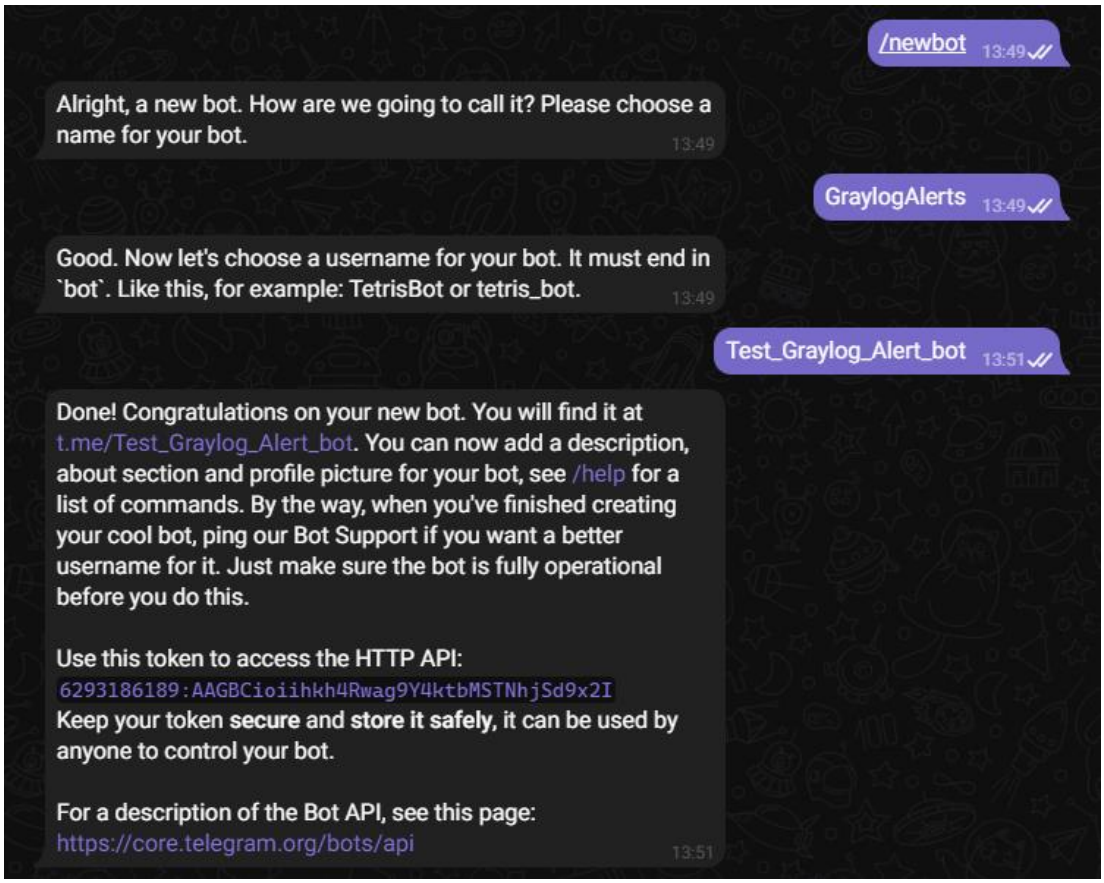


Рисунок 3.15 – Виконання алгоритму створення бота

Налаштування правил оповіщення у Graylog. За допомогою веб-інтерфейсу Graylog необхідно налаштувати правила оповіщення, що будуть спрацьовувати при виконанні певних умов або подій. У полі «Notification Type» необхідно обрати відповідний тип сповіщення, в даному випадку обрано сповіщення по Telegram. Після встановлення типу, вікно налаштувань зміниться відповідно до обраного типу. Результат налаштування сповіщень по телеграму зображено на рисунку 3.16.

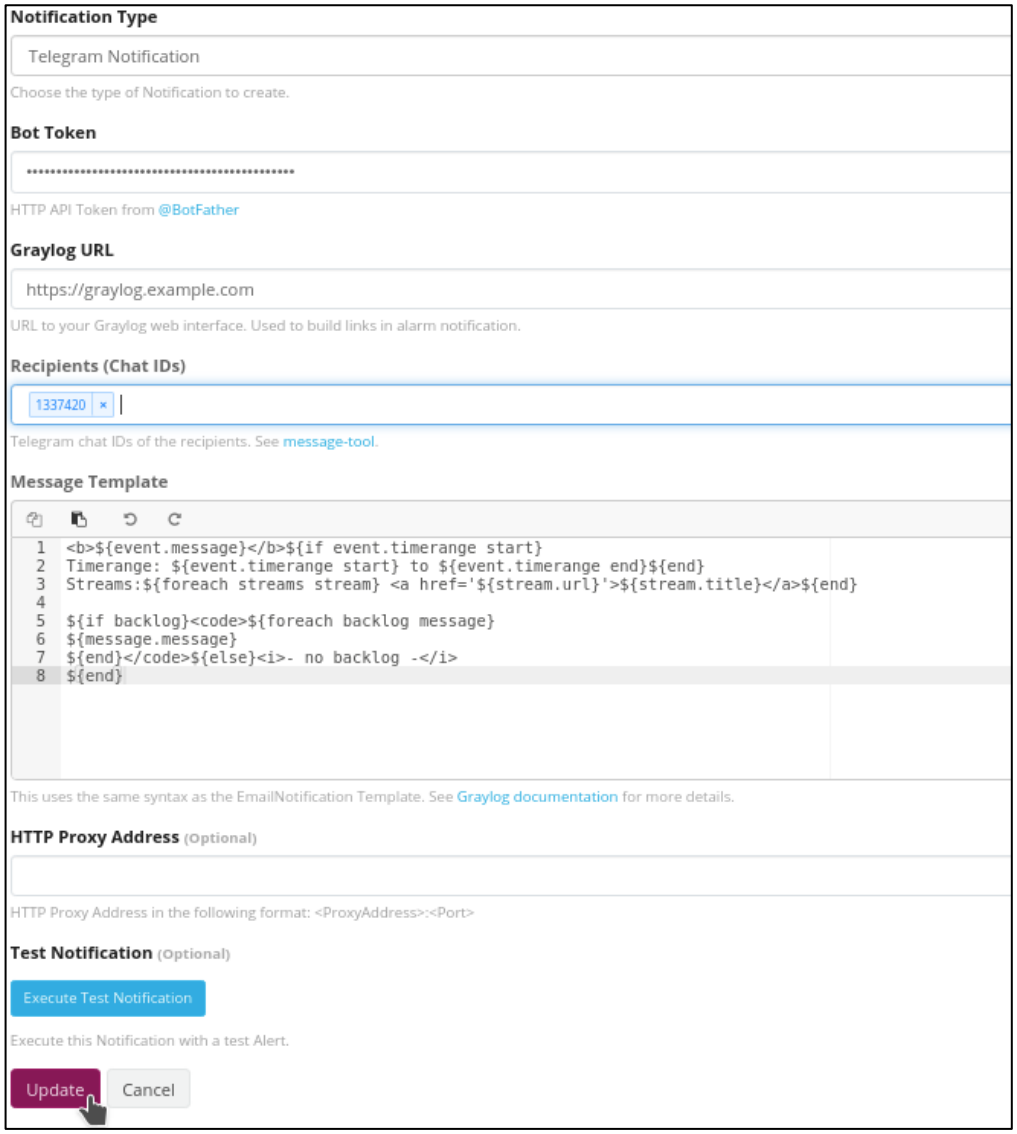


Рисунок 3.16 – Результат налаштування сповіщень по телеграму

З’явились поля для вводу бот токену та ID відповідного чату. В поле для токену встановлюється токен створеного бота, а в поле для чату встановлюємо відповідний ID, який можна дізнатися за допомогою існуючих ботів у телеграмі, чи за допомогою веб-сторінки телеграму, виділивши останню частину посилання, після решітки, при відкритому чату.

3.5.2 Налашутвання системи сповіщень Email

Для реалізації системи сповіщень за допомого поштового сервісу Email немає потреби у встановленні сторонніх розширень чи подібних файлі. Усі налаштування відбуваються безпосередньо через веб-інтерфейс Graylog. Вікно з налаштування системи сповіщень по поштовому сервісу Email зображено на рисунку 3.17.

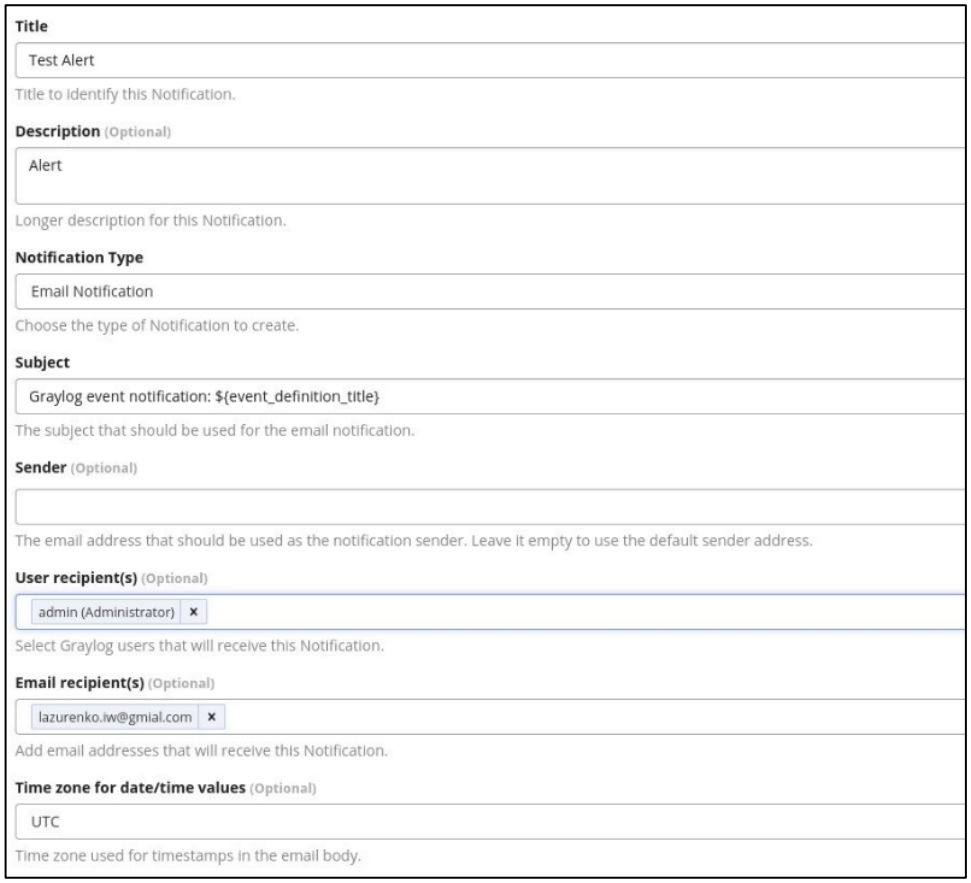


Рисунок 3.17– Вікно з налаштування системи сповіщень по поштовому сервісу Email

Першим етапом у налаштуванні системи сповіщень по Email є встановлення відповідного типу сповіщень, а саме «Email Notification».

Даний тип є одним із стандартних типів.

Наступним пунктом необхідно встановити адреси для відправки та прийому сповіщень. В якості відправника виступає будь-який налаштований почтовий сервер, або залишити дане поле пустим, що дасть змогу Graylog використовувати адресу за замовчуванням. Далі потрібно вказати користувачі, що будуть отримувати дані сповіщення. Одночасно сповіщення може бути відправлено декільком користувачам. Останнім встановлюється адреса електронної пошти, на яку буде відправлено сповіщення, одночасно може буде обрано декілька адрес.

Після проведення усіх налаштувань дану систему можливо протестувати натиснувши на відповідну кнопу в меню налаштування системи сповіщень.

Залишається тільки зберегти налаштування та прив’язувати його до різноманітних подій.

3.6 Висновки до 3 розділу

В результаті отримано працездатний кіберполігон на базі системи моніторингу Graylog.

Розглянуто та налаштовано методи фільтрації даних, що значно прискорять пошук конкретних лог-файлів. Створено потоки логів та правила відбору до відповідних потоків. Потоки допоможуть користувачеві розподілити логи за певними критеріями, що значно звузить пошук інформації та за необхідністю наддасть змогу розподілити обов’язки обробки певних потоків.

Розглянуто принципи роботи та налаштування системи сповіщень. Проаналізовано можливі типи відправки сповіщень, розглянуто алгоритм їх налаштування. Налаштування умов виникнення сповіщень та оформлення повідомлення, що необхідно відправити при спрацюванні умов.

Створено та налаштовано відповідне програмне забезпечення, у вигляді боту, для зв’язування з Graylog і подальшого використання в якості системи сповіщення.

ВИСНОВКИ

В результат бакалаврської роботи було спроектовано і побудовано кіберполігон на базі кафедри захисту інформації, та впроваджено система моніторингу Graylog до створеного кіберполігону.

Проведено аналіз існуючих кіберполігонів, визначено загальні принципи, що до його побудови, та необхідні вимоги до конфігурації створеної системи. Проаналізовано існуючі програмні рішення для реалізації моніторингу за лог-подіями.

Встановлено та налаштовано усі необхідні компоненти для коректного функціонування системи моніторингу.

Розглянуто та налаштовано доступні методи фільтрації лог-даних. Створено та налаштовано потоки лог-даний та встановлення правила для відповідних потоків. Проаналізовано принципи системи сповіщень, розглянути методи відправки повідомлень та налаштовано умови при яких необхідно відправляти сповіщення.

Результати даної бакалаврської роботи можливо в подальшому використовувати для проводження навчального практикуму студентів, шляхом виконання лабораторних робіт, покращенням навичок у побудові мереж та роботи з лог-даними, проведення практичних атак на створену систему та спроб захисту від відповідних атак, розширення існуючого кіберполігону.

В якості недоліку, що до створеного кіберполігону, необхідно відзначити недостатню потужність комп’ютера-сервера. Даний недолік значно підвищує можливість успішного проведення атаки та гальмує процес реагування на лог-події. При можливості, необхідно оновити конфігурацію серверної машини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. СИСТЕМА УПРАВЛІННЯ ЛОГАМИ «GRAYLOG» [Електронний ресурс]. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2023/paper/view/17969

2. Що таке логи [Електронний ресурс]. URL: https://hostiq.ua/wiki/ukr/log/

3. What is Graylog [Електронний ресурс]. URL: https://go2docs.graylog.org/5-0/what_is_graylog/what_is_graylog.htm

4. What is the ELK Stack? [Електронний ресурс]. URL: https://www.elastic.co/what-is/elk-stack

5. What Is Splunk & What Does It [Електронний ресурс]. URL: https://www.splunk.com/en_us/blog/learn/what-splunk-does.html

6. Централізований збір та обробка логів за допомогою ELASTICSEARCH, LOGSTASH та KIBANA [Електронний ресурс]. URL: https://freehost.com.ua/ukr/faq/articles/tsentralizovannij-sbor-i-obrabotka-logov-s-pomoschju-elasticsearch-logstash-i-kibana/

7. Elastic Beats and Where They Fit With ELK Stack [Електронний ресурс]. URL: https://www.instaclustr.com/blog/elastic-beats-and-where-they-fit-with-elk-stack/

8. Elasticsearch [Електронний ресурс]. URL: https://www.seotm.com/ua/technologies/elasticsearch-rozrobka.html

9. ЩО ТАКЕ KIBANA І ЯК ЦЕЙ ІНСТРУМЕНТ ВИКОРИСТОВУЄТЬСЯ В ТЕСТУВАННІ [Електронний ресурс]. URL: https://training.qatestlab.com/blog/technical-articles/what-is-kibana-and-how-to-use-this-tool/

10. What Is Splunk? [Електронний ресурс]. URL: https://www.edureka.co/blog/what-is-splunk/#:~:text=Splunk%20is%20a%20software%20platform,your%20IT%20infrastructure%20and%20business.

11. High Availability Log Processing with Graylog, MongoDB and ElasticSearch [Електронний ресурс]. URL: https://severalnines.com/blog/high-availability-log-processing-graylog-mongodb-and-elasticsearch/

12. Solarwinds Loggly Overview [Електронний ресурс]. URL: https://www.loggly.com/resource/solarwinds-loggly-overview/

13. ХМАРИ [Електронний ресурс]. URL: https://datapark.com.ua/ua/services/cloud/?gclid=cjwkcajwscgjbhaxeiwaswqqnik5z9uejqokm1bobjay6qpulvhsb00vksgatlz1pljrhvlsnxsm2rocsnyqavd_bwe

14. Ubuntu – опис ОС: актуальні версії, плюси, мінуси [Електронний ресурс]. URL: https://hyperhost.ua/info/uk/ubuntu-opis-os-aktualni-versii-plyusi-minusi

15. How To Install Java with Apt on Ubuntu 22.04 [Електронний ресурс]. URL: https://www.digitalocean.com/community/tutorials/how-to-install-java-with-apt-on-ubuntu-22-04

16. Install Elasticsearch on Ubuntu 22.04|20.04 [Електронний ресурс]. URL: https://computingforgeeks.com/install-graylog-on-ubuntu-with-lets-encrypt/

17. Найкращі інструменти для управління журналом та аналізу [Електронний ресурс]. URL: https://instagalleryapp.com/chistij-administrator-2/13-najkrashhih-instrumentiv-dlja-upravlinnja/

18. Oracle VM VirtualBox [Електронний ресурс]. URL: https://www.oracle.com/ua/virtualization/virtualbox/

19. Лог: що це, навіщо потрібен і де його знайти? [Електронний ресурс]. URL: https://hyperhost.ua/info/uk/log-shcho-tse-navishcho-potriben-i-de-yogo-znayti

20. Що таке файл журналу? [Електронний ресурс]. URL: https://ua.savtec.org/articles/howto/what-is-a-log-file-and-how-do-i-open-one.html

21. Що таке VirtualBox і як ним користуватися [Електронний ресурс]. URL: http://smartandyoung.com.ua/shho-take-virtualbox-i-jak-nim-koristuvatisja

22. Systems Monitoring and Big Data Analysis Using the Elasticsearch System [Електронний ресурс]. URL: https://ieeexplore.ieee.org/abstract/document/8745151

23. Аналіз роботи інструменту для управління та аналізу журналів Graylog [Електронний ресурс]. URL: https://elartu.tntu.edu.ua/bitstream/lib/40311/2/XNTK_2022_Humeniuk_O-Performance_analysis_of_75-76.pdf

24. Security monitoring tool system using threat intelligence vs threat hunting [Електронний ресурс]. URL: http://library.oum.edu.my/repository/1435/

25. Automated unearthing of dangerous issue reports [Електронний ресурс]. URL: https://dl.acm.org/doi/abs/10.1145/3540250.3549156

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ
БАКАЛАВРСЬКОЇ ДИПЛОМНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Кіберполігон для дослідження подій інформаційної безпеки. Частина 2. Обробка подій на основі Graylog

Автор роботи: Лазуренко Іван Дмитрович

Тип роботи: бакалаврська дипломна робота
(курс. зах.)

Підрозділ: кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 97.6%. Схожість – 2.4%.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Каплун В. А.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Лазуренко І.Д.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Васильєва О.І.
(підпис) (прізвище, ініціали)

Додаток Б

Методичні вказівки

Мета роботи: Ознайомитися з процесом встановлення та налаштування Graylog.

Порядок виконання:

Крок 1: Оновлення системи

Першим кроком перед встановленням Graylog потрібно провести оновлення операційної системи. Для того, щоб виконати цей крок необхідно виконати наступні команди:

```
sudo apt update && sudo apt -y full-upgrade
[ -f /var/run/reboot-required ] && sudo reboot -f
```

Ці команди оновлять пакети в системі та, якщо необхідно, перезавантажать систему для застосування оновлень.

Крок 2: Встановлення необхідних застосунків

Для успішної установки та налаштування Graylog потрібно встановити деякі необхідні залежності. Виконайте наступні команди для встановлення цих залежностей:

```
sudo apt update
sudo apt install vim apt-transport-https openjdk-11-jre-headless uuid-runtime pwgen curl dirmngr
```

Виконавши цей ряд команд, будуть встановлені необхідні пакети, включаючи Java Runtime Environment (JRE) і деякі інші утиліти, необхідні для роботи Graylog.

Крок 3: Встановлення та налаштування Elasticsearch

Після встановлення необхідних залежностей можна переходити до встановлення самої Elasticsearch. Виконайте наступні команди для встановлення та налаштування Elasticsearch:

```
sudo apt install curl

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg

echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update

sudo apt install elasticsearch

sudo nano /etc/elasticsearch/elasticsearch.yml
```

У першій команді встановлюється утиліта curl, яка використовується для завантаження необхідних ключів та пакетів. Наступні команди завантажують ключі та встановлюють пакет Elasticsearch з офіційного репозиторію Elastic. Після цього відкриється конфігураційний файл Elasticsearch для налаштування.

У відкритому файлі /etc/elasticsearch/elasticsearch.yml знайдіть наступні рядки та внесіть зміни:

```
cluster.name = graylog

network.host = localhost

action.auto_create_index = false
```

Ці налаштування встановлюють назву кластера Elasticsearch, обмежують доступ до Elasticsearch лише з локальної машини та вимикають автоматичне створення індексів. Після збереження змін в файлі, закрийте його. В результаті налаштування у файлі мають виглядати як на рисунку 1.

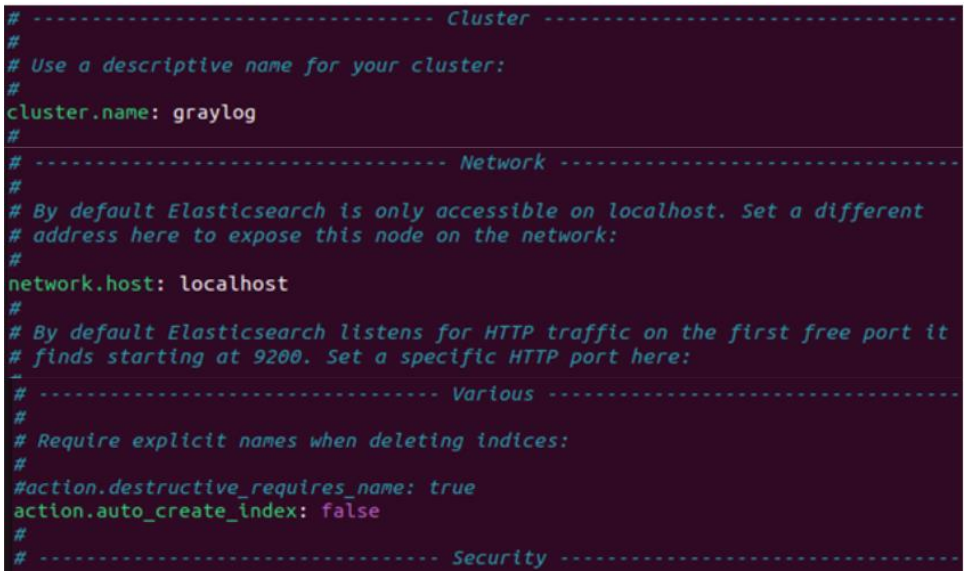


Рисунок 1 – Налаштування в конфігураційному файлі Elasticsearch

Крок 4: Запуск Elasticsearch

Для запуску Elasticsearch і налаштування його на автоматичний запуск при перезавантаженні системи. необхідно виконати наступну команду:

```
sudo systemctl start elasticsearch
```

```
sudo systemctl enable elasticsearch
```

Крок 5: Встановлення та налаштування MongoDB

Наступним кроком необхідно встановити документовану систему управління базами даних Mongodb. Для встановлення MongoDB необхідно скористатися наступною командою:

```
sudo apt install mongod
```

Використовуючи дану команду, відбудеться встановлення додатку. Додаткові налаштування непотрібні. Для перегляду статусу MongoDB необхідно виконати команду:

```
systemctl status mongodb
```

Результат виконання команди представлено на рисунку 2.

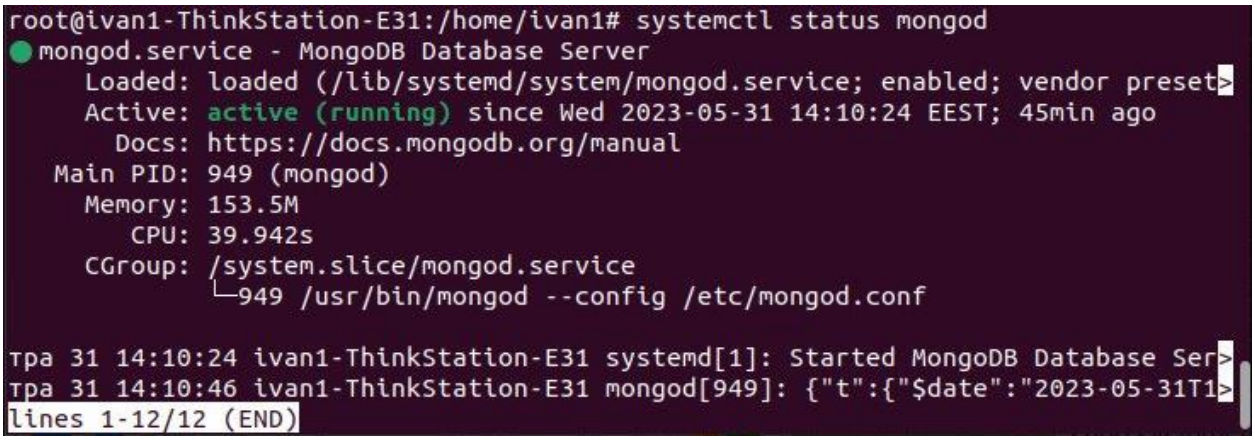


Рисунок 2 – Результат успішного встановлення Mongodb

Отримавши результати, можна зробити висновок, що Mongodb встановлено правильно та система готова до використання.

Крок 6: Встановлення та налаштування Graylog server

Для встановлення Graylog необхідно завантажити його з репозиторію за допомогою команд:

```
wget https://packages.graylog2.org/repo/packages/graylog-4.3-repository_latest.deb
```

```
sudo dpkg -i graylog-4.3-repository_latest.deb
```

Далі встановлюється Graylog server використовуючи спочатку команду для оновлення, а потім команду для встановлення самого серверу:

```
sudo apt update
```

```
sudo apt install graylog-server
```

Після встановлення Graylog server потрібно згенерувати спеціальний секретний пароль за допомогою команди: pwgen -N 1 -s 96. В результаті отримуємо унікальний секретній пароль розміром 96 символів.

Даний пароль необхідно занести до файлів конфігурації серверу. Файл конфігурації серверу знаходиться за шляхом /etc/graylog/server/server.conf і навпроти «password_secret = » приписується згенерований секретний пароль.

Для прив’язки веб-інтерфейсу до серверу необхідно зазначити IP адрему та порт. У файлі конфігурацій серверу знайти поле «http_bind_address» і встановити значення за таким патерном (IP:Port), у випадку коли сервер і веб-

інтерфейс знаходяться на одній машині можливо використовувати наступне значення: 0.0.0.0:9000.

Наступним кроком є створення хеш-паролю sha256 для адміністратора. Це пароль, який знадобиться для входу у веб-інтерфейс. Для його отримання використовуються команди:

```
echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1
```

```
Enter Password: password
```

В результаті буде отримано пароль котрий складається із 64 символів. Після отримання даного пароля необхідно занести його до файлу конфігурації у поле «root_password_sha2».

Останнім кроком буде перезапуск Graylog server, та Mongodb, використовуючи наступній ряд команд:

```
sudo systemctl daemon-reload
```

```
sudo systemctl restart mongodb graylog-server
```

```
sudo systemctl enable mongodb graylog-server
```

Щоб перевірити успішність налаштування Graylog server, потрібно перейти за посиланням наступного типу «http://<serverip_hostname>:9000». У випадку з проведеними налаштування посилання матиме такий вигляд «http://localhost:9000». Результат успішного налаштування Graylog server зображено на рисунку 3.

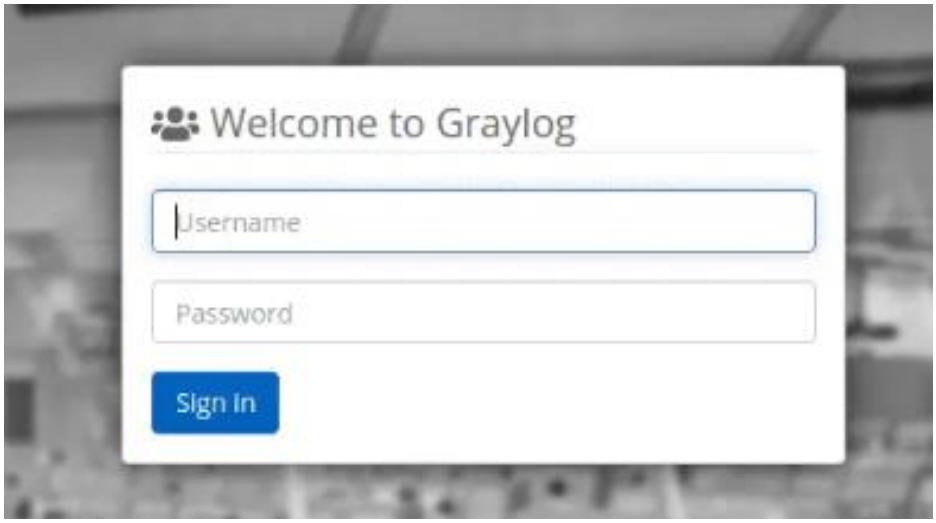


Рисунок 3 – Результат успішного налаштування Graylog server

ІЛЮСТРАТИВНА ЧАСТИНА

Кіберполігон для дослідження подій інформаційної безпеки. Частина 3. Обробка на основі Graylog

(Назва бакалаврської кваліфікаційної роботи)

Виконав: студент 4 курсу групи 1БС-21МС
спеціальності 125 Кібербезпека
_____ Іван Лазуренко
_____ 2023 р.

Керівник: к. т. н., доцент каф. ЗІ
_____Олеся ВОЙТОВИЧ
_____ 2023 р.

ТОПОЛОГІЯ МЕРЕЖІ

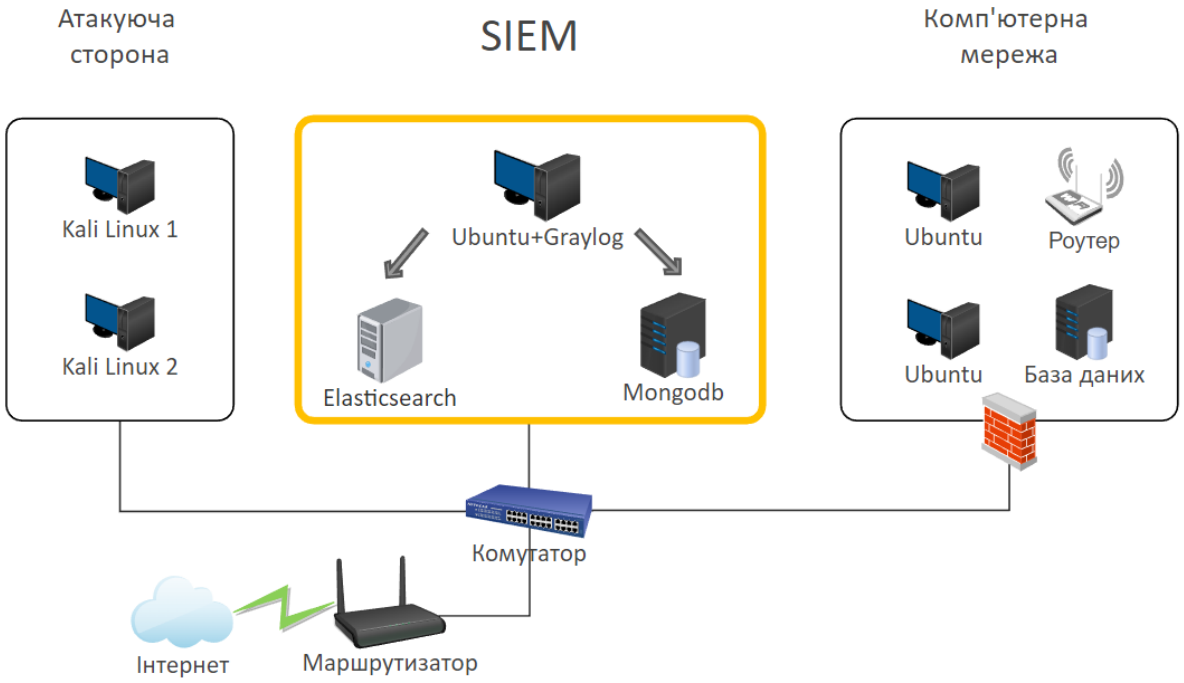


СХЕМА ВЗАЄМОДІЇ МІЖ КОМПОНЕНТАМИ GRAYLOG

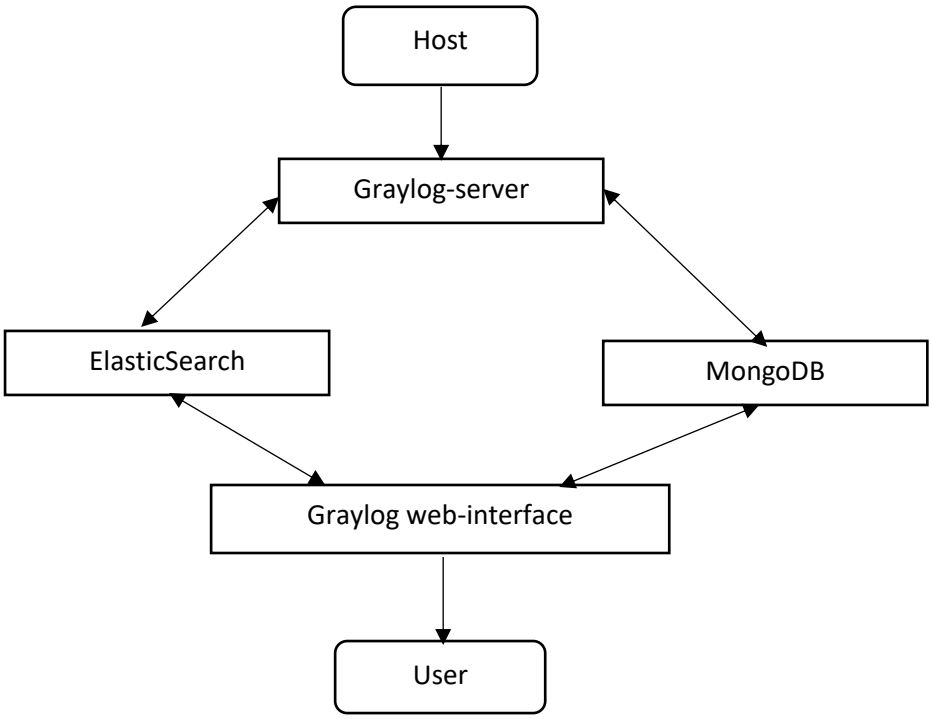
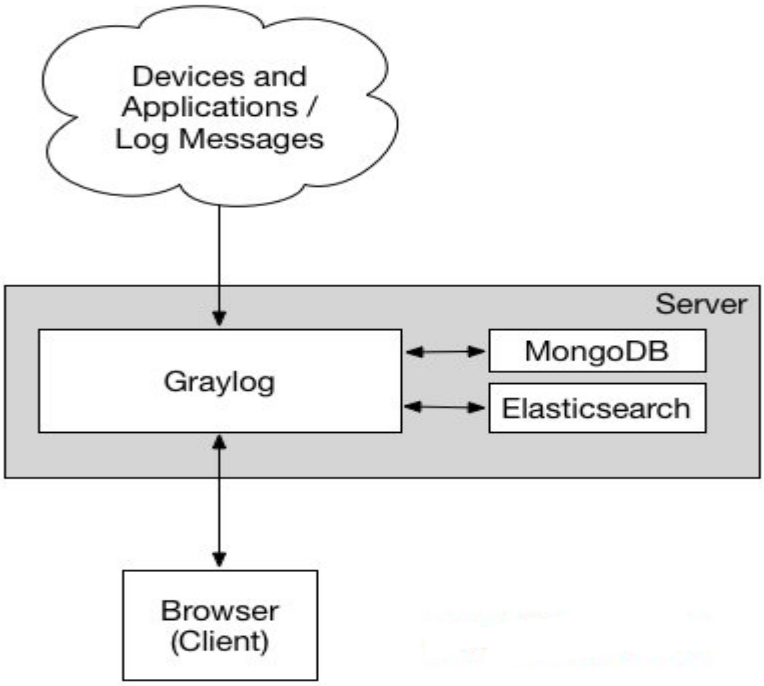


СХЕМА РОБОТИ СИСТЕМИ СПОВІЩЕНЬ

СХЕМА РОБОТИ МЕХАНІЗМУ ПОТОКІВ ЛОГ-ДАНИХ

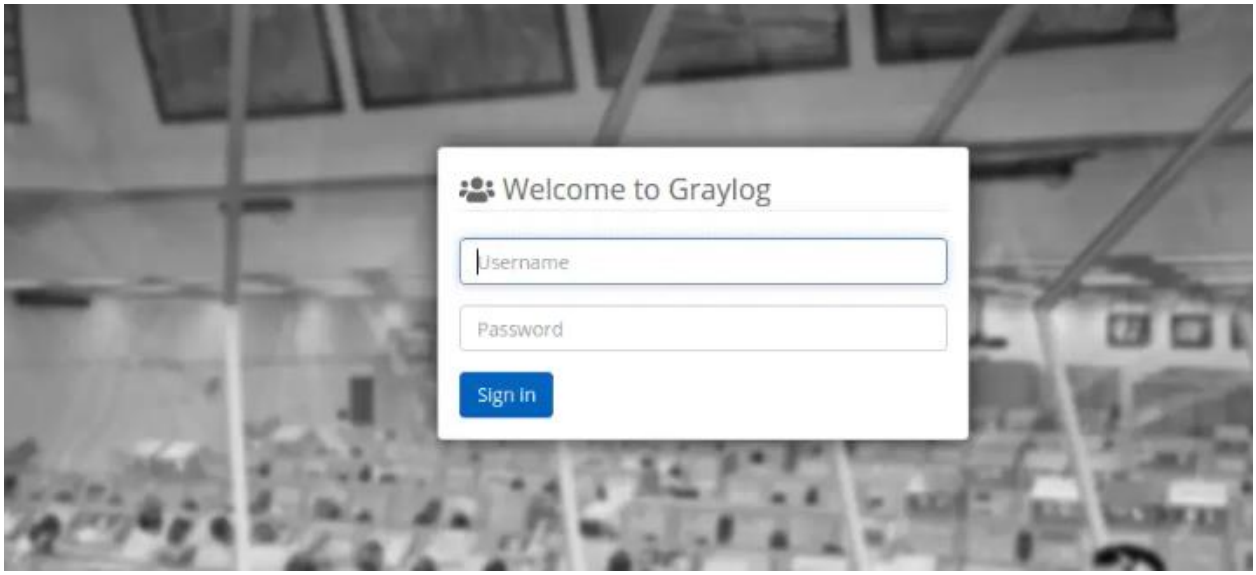
УЗАГАЛЬНЕНА СХЕМА GRAYLOG-СЕРВЕРУ



РЕЗУЛЬТАТИ АНАЛІЗУ ОСНОВНИХ ПАРАМЕТРІВ ДОДАТКІВ ДЛЯ РОБОТИ З ЛОГАМИ

Додаток	Опис	Тип додатка	Інтеграція
Elastic Stack	Потужний стек для збору, аналізу та візуалізації логів	Відкритий, self-hosted	Інтеграція з Logstash, Elasticsearch API, Kibana, Beats
Splunk	Інтегрована платформа для аналізу та моніторингу	Комерційна, self-hosted	Інтеграція з API та SDK, Universal Forwarder, різноманітні джерела даних
Graylog	Відкрите рішення для збору та аналізу логів	Відкрите, self-hosted	Інтеграція з ріними джерелами та агентами даних, Graylog API
Loggly	Хмарна платформа для збору та аналізу логів	Хмарна	Інтеграційні інструменти відсутні

РЕЗУЛЬТАТ УСПІШНОГО НАЛАШТУВАННЯ GRAYLOG SERVER



РЕЗУЛЬТАТ НАЛАШТУВАННЯ ФІЛЬТРАЦІЇ