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

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Методи та засоби дослідження подій дистрибутива PfSense

Виконав: студент VI курсу, групи СІм-61
спеціальності 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

_____ Василенко В.І.
(підпис) (прізвище та ініціали)

Керівник _____ Стадник Н. Б.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Луцик Н. С.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Осухівська Г. М.
(підпис) (прізвище та ініціали)

Рецензент _____ Петрик М. Р.
(підпис) (прізвище та ініціали)

Тернопіль
2022

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

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

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Осухівська Г.М.
(підпис) (прізвище та ініціали)
«____» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

Студенту Василенко Володимир Ігорович
(прізвище, ім'я, по батькові)

1. Тема роботи Методи та засоби дослідження подій дистрибутива PfSense

Керівник роботи Стадник Наталія Богданівна, к.т.н., старший викладач кафедри КС
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «__06__» __грудня___ 2022 року № __4/7-986____

2. Термін подання студентом завершеної роботи 20 грудня 2022р.

3. Вихідні дані до роботи журнали подій pfSense, ELK-стек, конфігураційний файл, методи аналізу логів

4. Зміст роботи (перелік питань, які потрібно розробити)
ЗМІСТ; ВСТУП; 1. АНАЛІЗ ПРЕДМЕТУ;. 2 АНАЛІЗ МЕТОДІВ ЗБОРУ ЛОГІВ;
3 РОЗРОБКА ТА ТЕСТУВАННЯ СИСТЕМИ;
4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ; ВИСНОВКИ;
ПЕРЕЛІК ДЖЕРЕЛ; ДОДАТКИ

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Методи та засоби дослідження подій дистрибутива PfSense
Схема роботи мережевого екрану PfSense
Кластер Elasticsearch та типовий пайплайн Logstash
Поєднання агентного та безагентного способу, схема роботи SNMP пастки
Схема встановлення X-Pack
Основна частина програми
Загальний вигляд логів у Kibana та вигляд окремого логу у Kibana
Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В. М., старший викладач		

7. Дата видачі завдання 15.11.2022

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Затвердження теми кваліфікаційної роботи	14.11.2022	Виконано
2	Аналіз літературних джерел	18.11.2022	Виконано
3	Обґрунтування актуальності дослідження	19.11.2022	Виконано
4	Аналіз предмету дослідження та предметної області	28.11.2022	Виконано
5	Проведення дослідження методів аналізу журналів	29.11.2022	Виконано
	подій		
6	Оформлення першого розділу роботи	07.12.2022	Виконано
7	Оформлення другого розділу роботи	08.12.2022	Виконано
8	Оформлення третього розділу роботи	09.12.2022	Виконано
9	Оформлення розділу «Охорона праці та безпека в»	10.12.2022	Виконано
	надзвичайних ситуаціях		
10	Нормоконтроль	19.12.2022	Виконано
11	Попередній захист роботи	19.12.2022	Виконано
12	Захист кваліфікаційної роботи	21.12.2022	

Студент _____ *Василенко В.І.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Стадник Н. Б.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи та засоби дослідження подій дистрибутива PfSense // Кваліфікаційна робота освітнього рівня «Магістр» // Василенко Володимир Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СІм-61 // Тернопіль, 2022 // С. 54, рис. – 27, табл. – , кресл. – , додат. – 1, бібліогр. – 28.

Ключові слова: дистрибутив, метод, логи, аналіз, журнал подій, PfSense.

Кваліфікаційна робота присв'ячена розробці конфігураційного файлу, в якому проводиться аналіз та структуризація журналів подій.

В першому розділі кваліфікаційної роботи описано дистрибутив pfSense та його можливості, проведено аналіз та огляд публікацій, що відображають задачі та напрямки досліджень які стосуються об'єкту дослідження. Вибрано та обґрунтувано методи вирішення поставленої задачі.

В другому розділі кваліфікаційної роботи проведено аналіз методів отримання логів.

В третьому розділі кваліфікаційної роботи описано програмне забезпечення системи. Спроектовано конфігураційний файл, в якому проводиться аналіз та структуризація журналів подій. Описано можливості роботи з Kibana.

ANNOTATION

Methods and tools for events investigating the PfSense distribution // Qualification work of the educational level "Master" // Vasylenko Volodymyr Ihorovych // Ternopil National Technical University named after Ivan Pulyu, Faculty of Computer Information Systems and Software Engineering, Department of Computer Sciences, Group of Computer Science -61 // Ternopil, 2022 // C. 54, fig. – 27, tab. - , chair. - , add. – 1, bibliography - 28.

Key words: distribution, method, logs, analysis, event log, PfSense.

The qualification work is devoted to the development of a configuration file in which the analysis and structuring of event logs is carried out.

In the first section of the qualification work, the pfSense distribution and its capabilities are described, an analysis and review of publications reflecting the tasks and directions of research related to the research object is carried out. Methods of solving the given task are selected and substantiated.

In the second section of the qualification work, the methods of obtaining logs were analyzed.

The software of the system is described in the third section of the qualification work. A configuration file is designed, in which the analysis and structuring of event logs is carried out. Features of working with Kibana are described.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Лог-файл (англ log-file) – спеціальний файл, у якому накопичується зібрана службова та статистична інформація про події в системі.

ELK – це абревіатура трьох проектів з відкритим кодом: Elasticsearch, Logstash і Kibana.

PDU – (Protocol data units) – це єдина одиниця інформації, що передається між одноранговими об’єктами комп’ютерної мережі.

API (Application Programming Interface) – прикладний програмний інтерфейс.

DHCP (Dynamic Host Configuration Protocol) – це стандартний протокол прикладного рівня, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі.

SSL (Secure Sockets Layer) – криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером.

ЗМІСТ

ВСТУП

Актуальність теми. Покращення безпеки мережевих систем зростає загрозливою швидкістю. Кожні 8 років кількість цифрових даних у світі збільшується в 10 разів. Передбачається, що глобальний обсяг даних досягне 175 зетабайт до 2025 року. Методи визначення захищеності інформаційних систем поділяються на кількісні та якісні. Індикаторами для кількісних підходів є вартість ресурсу, критичність ресурсу, захист від окремих загроз, ймовірність реалізації загрози шляхом експлуатації, ступінь втрати інформаційної цінності через зловмисні дії та величина залишкового ризику. Запобігання злочинній діяльності можна здійснити за допомогою методів збору даних про події в певній мережі. Адже завдяки аналізу подій можна дізнатись звідки стався напад.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи рівня «Магістр» є дослідження сучасних методів аналізу подій для дистрибутива операційної системи FreeBSD з відкритим кодом, під назвою PfSense. Для цього було здійнено:

– Проаналізувано і виділено основні властивості дестрибутиву PfSense.

– Здійснено дослідження існуючих на даний момент способів аналізу логів.

– Проаналізовано методи аналізу журналів подій.

– Розроблено алгоритм аналізу журналів подій.

Об’єкт дослідження. Процеси опрацювання та аналізу логів.

Предмет дослідження. Методи аналізу логів дистрибутиву PfSense.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, щоб покращити процес аналізу подій.

Практичне значення одержаних результатів. Виконано проектування та алгоритмізацію аналізу логів.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на X науково-технічній конференції

«Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2022 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додатки А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 20 найменувань та 1 додатку. Загальний обсяг кваліфікаційної роботи складає 60 сторінок, з них 41 сторінки основного тексту, який містить 33 рисунки.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ЛОГУВАННЯ PFSENSE

1.1. Опис та аналіз властивостей, характеристик, параметрів об’єкту дослідження

PfSense - дистрибутив для створення міжмережевого екрану/маршрутизатора, заснований на основі FreeBSD. PfSense призначений для встановлення на персональний комп'ютер, відомий своєю надійністю та пропонує функції, які часто можна знайти лише у дорогих комерційних міжмережевих екранах. Налаштування можна проводити через web-інтерфейс, що дозволяє використовувати його без знання базової системи FreeBSD. Мережеві пристрої з pfSense зазвичай застосовуються як периметрові брандмауери, маршрутизатори, сервери DHCP/DNS, і технології VPN як вузла топології hub/spoke.

PfSense можна інсталювати на більшості звичайних апаратних засобів, включаючи старі комп’ютери та вбудовані системи. Зазвичай pfSense налаштовується та працює через зручний веб-інтерфейс, що спрощує адміністрування навіть для користувачів із обмеженими знаннями в роботі з мережами. Як правило, для налаштування маршрутизатора ніколи не потрібно використовувати термінал або редагувати конфігураційні файли. Навіть оновлення програмного забезпечення можна запускати з веб-інтерфейсу [1].

PfSense здебільшого використовується як програмне забезпечення для маршрутизатора та брандмауера та зазвичай налаштовано як DHCP-сервер, DNS-сервер, точка доступу WiFi, VPN-сервер, усі вони працюють на одному апаратному пристрої. PfSense також дозволяє встановлювати сторонні пакунки з відкритим кодом, такі як Snort або Squid, через вбудований менеджер пакетів, що робить його вибором за замовчуванням для багатьох мережевих адміністраторів.

Крім того, що він є потужним і гнучким брандмауером і платформою маршрутизатора, він має довгий список функцій і систему пакетів, що є досить

вигідним. Ця система пакетів не тільки дає операційній системі гнучкість для розширення, але й запобігає прогалинам безпеки в розповсюдженні.

PfSense має гнучкий дизайн. Його можна використовувати на маленькому домашньому маршрутизаторі, а також керувати всією мережею великої корпорації. Сьогодні pfSense часто замінює CISCO та інші дорогі бренди у великих корпоративних середовищах не тому, що він безкоштовний, а тому, що це багатофункціональна та зріла платформа.

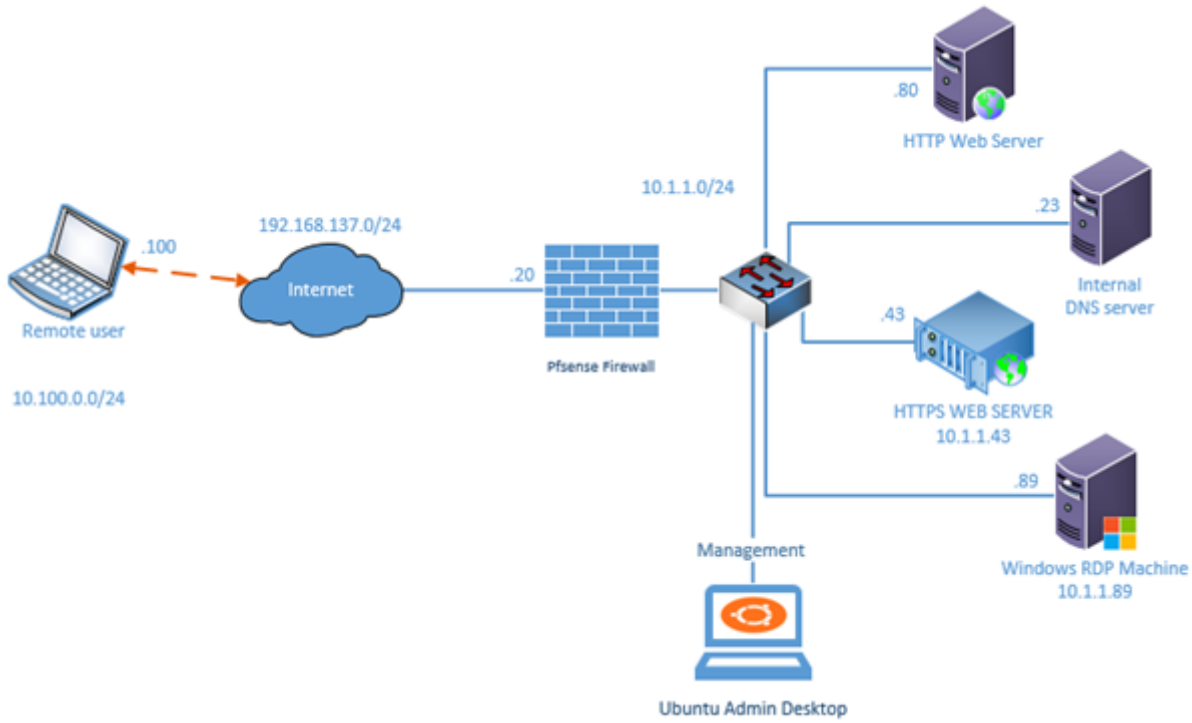


Рис. 1.1 Схема роботи мережевого екрану PfSense

PfSense можна встановити на будь-якому обладнанні - старий комп'ютер може стати новим маршрутизатором за умови, якщо є комп’ютер із принаймні 2 мережевими картами. Можна вибрати одну зі спеціалізованих апаратних платформ, таких як PC Engines APU, TekLager TLSense, Soekris, Netgate або інші.

Операційні системи з відкритим кодом, такі як pfSense, регулярно оновлюються та, як відомо, швидко виправляють проблеми безпеки. pfSense дає можливість повністю контролювати мережу [2].

1.2. Огляд та аналіз публікацій що стосуються об’єкту дослідження

Основна сторінка системи pfSense – це сторінка Статус системи (Status >> System). Вона містить деяку інформацію про базову систему, наприклад, ім'я маршрутизатора, версію pfSense, платформи, час роботи, розмір таблиці стану, використання MBUF, використання CPU, використання пам'яті, використання своп простору та використання диска. Лічильники на сторінці оновлюються автоматично, кожні кілька секунд, тому немає потреби в оновленні сторінки.

Інші опції меню Status >> Systems Logs на закладці Settings необхідні для налаштування демона syslog, що дозволяє копіювати записи журналів на віддалений сервер. Оскільки журнали pfSense, що зберігаються, на самому маршрутизаторі мають кінцевий (і досить малий) розмір, їх копіювання на syslog-сервер забезпечує як можливість пошуку і усунення несправностей, так і можливість тривалого зберігання записів у разі необхідності. Журнали маршрутизатора очищаються при перезавантаженні, а наявність видаленої копії журналів дозволяє діагностувати події, що відбуваються безпосередньо перед перезавантаженням. Деякі корпоративні та законодавчі політики визначають, скільки часу повинні зберігатися файли журналів брандмауерів або аналогічних пристроїв. Якщо організація вимагає довгострокового зберігання журналів, то доведеться зайнятися конфігуруванням syslog-сервера.

Для запуску віддаленого журналювання потрібно встановити Enable sysloging для віддаленого syslog-сервера та заповнити IP адресу для syslog-сервера Remote Syslog Server. Якщо потрібно вимкнути локальне журналування, можна відзначити «Вимкнути запис файлів журналу на диск локальної пам’яті», але зазвичай цього робити не рекомендується [3].

Зазвичай, syslog-сервер, це сервер безпосередньо з локальним інтерфейсом системи pfSense. Журналювання може здійснюватися на сервер через VPN, але для цього можуть знадобитися деякі додаткові налаштування. Але не варто передавати дані syslog безпосередньо через інтерфейс WAN, оскільки ці дані є простим текстом і можуть містити значну інформацію.

Варто встановити прапори для типів записів, які потрібно копіювати на syslog-сервер. Можна вибрати віддалену реєстрацію системних подій, подій брандмауера, подій служби DHCP, автентифікації, події VPN або всі види подій одночасно.

Системні журнали можна знайти на вкладці Status >> System Log, меню System. Вони містять записи журналу, безпосередньо згенеровані вузлом, деякими службами та пакетами, які перенаправляються інші вкладки системного журналу. Як показано на рис. 1.2, тут є записи демона SSH, пакета avahi та клієнта динамічного DNS. Тут же реєструються і безліч інших систем, але більшість сервісів не завантажуватиме системний журнал. Зазвичай, якщо служба веде об'ємний журнал, вона переміщує його власну вкладку.

Варто звернути увагу, що журнали налаштовуються і дозволяють відображати записи в порядку їхнього оновлення – тобто, нові записи з'являються на вершині списку.

Action	Time	Interface	Source	Destination	Protocol
✖	Aug 3 08:59:02	WAN	198.51.100.1:67	198.51.100.2:68	UDP
✖	Aug 3 15:02:10	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:02:10	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:14:02	WAN	198.51.100.108:138	198.51.100.255:138	UDP
✖	Aug 3 15:14:02	WAN	198.51.100.108:138	198.51.100.255:138	UDP

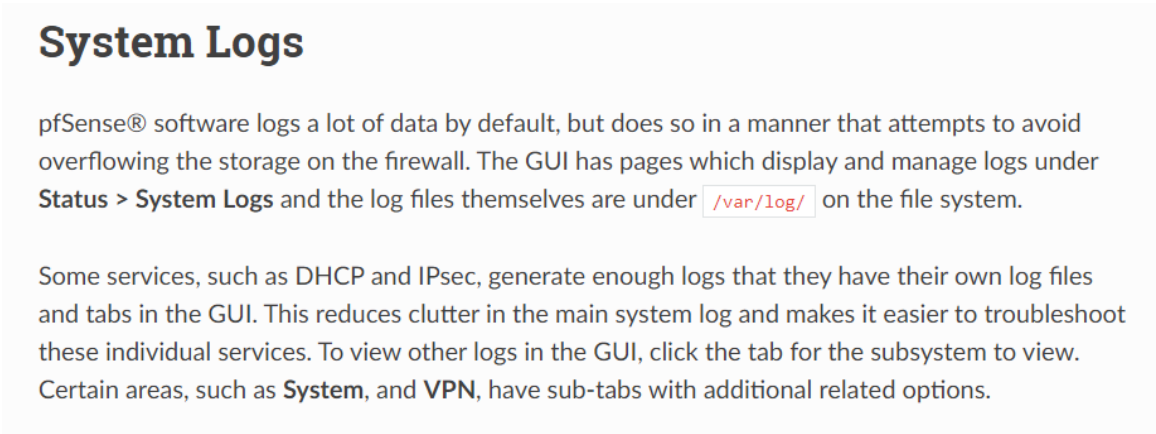
Рис. 1.2 Приклад логів системного журналу

За замовчуванням pfSense реєструє досить малий обсяг даних, який дозволяє уникнути переповнення сховища маршрутизатора. Журнали можна знайти на вкладці Status >> System Logs у web-інтерфейсі, і в каталозі /var/log файлової системи. Деякі компоненти, такі як DHCP та IPsec генерують досить об'ємну інформацію, тому винесені на окремі вкладки, з метою покращення читання журналів та пошуку необхідної інформації. Щоб переглянути ці журнали, слід вибрати вкладку відповідної підсистеми [4].

Журнали pfSense ведуться в циркулярному бінарному лозі або clog-форматі. Вони мають фіксовані розміри та ніколи не розростаються. Як наслідок

- журнал містить лише певну кількість записів, і застарілі записи видаляються з журналу з приходом нових.

Наразі єдиним методом яким можна переглянути журнали подій для дистрибутива PfSense є спосіб за замовчуванням від розробника, до того ж логуються, в основному, системні події.



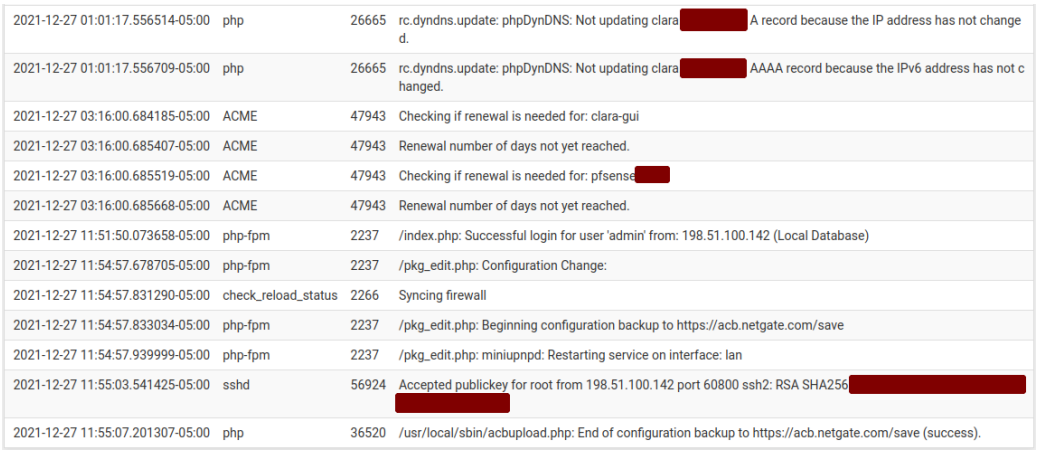
System Logs

pfSense® software logs a lot of data by default, but does so in a manner that attempts to avoid overflowing the storage on the firewall. The GUI has pages which display and manage logs under **Status > System Logs** and the log files themselves are under `/var/log/` on the file system.

Some services, such as DHCP and IPsec, generate enough logs that they have their own log files and tabs in the GUI. This reduces clutter in the main system log and makes it easier to troubleshoot these individual services. To view other logs in the GUI, click the tab for the subsystem to view. Certain areas, such as **System**, and **VPN**, have sub-tabs with additional related options.

Рис. 1.3 Опис доступу до файлів логів від розробника

Основною проблемою цього методу є те, що відображається надто мала кількість подій та вони не є чітко розбитими на складові.



2021-12-27 01:01:17.556514-05:00	php	26665	rc.dyndns.update: phpDynDNS: Not updating clara [redacted] A record because the IP address has not changed.
2021-12-27 01:01:17.556709-05:00	php	26665	rc.dyndns.update: phpDynDNS: Not updating clara [redacted] AAAA record because the IPv6 address has not changed.
2021-12-27 03:16:00.684185-05:00	ACME	47943	Checking if renewal is needed for: clara-gui
2021-12-27 03:16:00.685407-05:00	ACME	47943	Renewal number of days not yet reached.
2021-12-27 03:16:00.685519-05:00	ACME	47943	Checking if renewal is needed for: pfsense [redacted]
2021-12-27 03:16:00.685668-05:00	ACME	47943	Renewal number of days not yet reached.
2021-12-27 11:51:50.073658-05:00	php-fpm	2237	/index.php: Successful login for user 'admin' from: 198.51.100.142 (Local Database)
2021-12-27 11:54:57.678705-05:00	php-fpm	2237	/pkg_edit.php: Configuration Change:
2021-12-27 11:54:57.831290-05:00	check_reload_status	2266	Syncing firewall
2021-12-27 11:54:57.833034-05:00	php-fpm	2237	/pkg_edit.php: Beginning configuration backup to https://acb.netgate.com/save
2021-12-27 11:54:57.939999-05:00	php-fpm	2237	/pkg_edit.php: miniupnpd: Restarting service on interface: lan
2021-12-27 11:55:03.541425-05:00	sshd	56924	Accepted publickey for root from 198.51.100.142 port 60800 ssh2: RSA SHA256 [redacted]
2021-12-27 11:55:07.201307-05:00	php	36520	/usr/local/sbin/acbupload.php: End of configuration backup to https://acb.netgate.com/save (success).

Рис. 1.4 Вигляд журналу подій у середовищі перегляду від розробника

До того ж у налаштуваннях за замовчуванням відображатимуться не всі журнали подій, а лише найосновніші, що може бути небезпечним, оскільки

можна пропустити певну атаку і навіть не підозрювати про неї. Загалом PfSense може відображати події від датасетів зображених на рис. 1.5 [5].

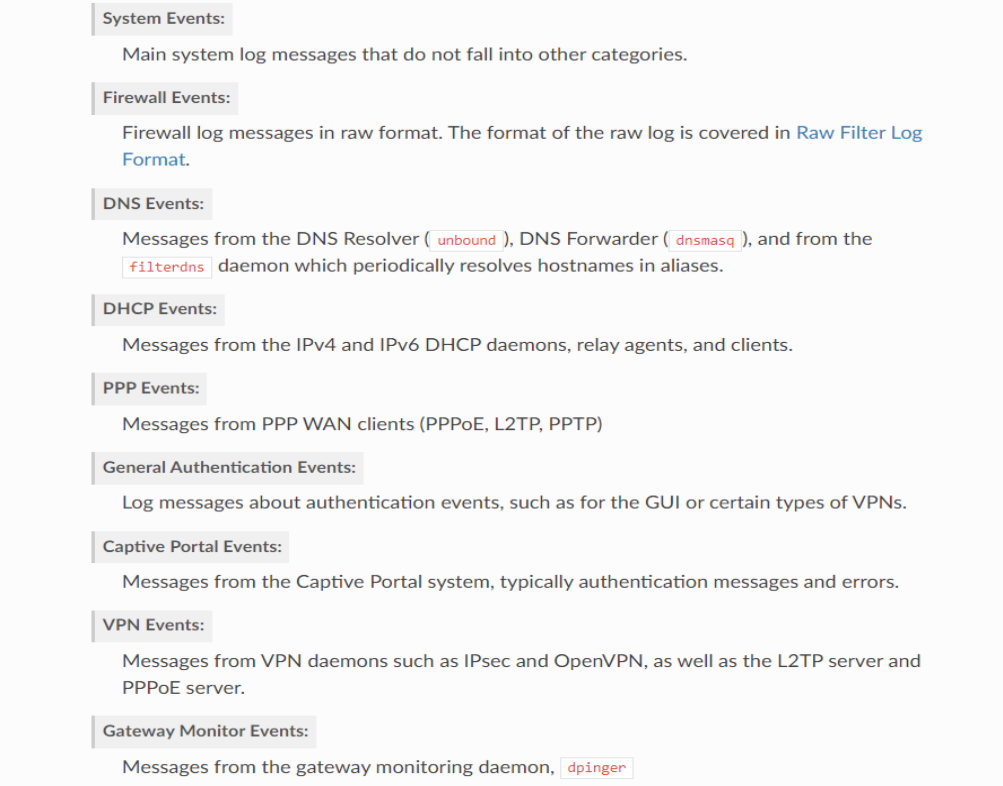


Рис. 1.5 Можливі датасети від яких є можливість отримувати записи у журналі подій

1.3. Обґрунтування та вибір методів вирішення поставленої задачі

Оскільки на даний час немає зручних методів перегляду та розбиття на категорії журналів подій для pfSense мною було запропоновано метод стягнення подій на спеціальний хост від провайдера [6].

First, configure the syslog server to accept remote connections which means running it with the `-a <subnet>` or similar flag.

On FreeBSD, edit `/etc/rc.conf` and add this line:

```
syslogd_flags=" -a 192.168.1.1 "
```

Where `192.168.1.1` is the IP address of the pfSense firewall.

More complex allow rules for syslog are also possible, like so:

```
syslogd_flags=" -a 10.0.10.0/24:*"
```

Using that parameter, syslog will accept from any IP address in the 10.0.10.0 subnet (mask 255.255.255.0) and the messages may come from any UDP port.

Now, edit `/etc/syslog.conf` and add a block at the bottom:

```
!*
+*

+pfsense
*.*             /var/log/pfsense.log
```

Рис. 1.6 Інструкція з отримання логів від постачальника

Where `pfSense` is the hostname of the pfSense firewall. An entry may also need to be added in **/etc/hosts** for that system, depending on the DNS setup. Logs may be split separate files. Use the **/etc/syslog.conf** file on the pfSense firewall for more details on which logging facilities are used for specific items.

```
192.168.1.1          pfsense     pfsense.example.com
```

The log file may also need to be created manually with proper permissions:

```
touch /var/log/pfsense.log
chmod 640 /var/log/pfsense.log
```

Now restart syslog:

```
/etc/rc.d/syslogd restart
```

Рис. 1.7 Завершення пересилання подій на хост

Файл журналу, у контексті комп’ютера, — це автоматично створена документація з часовими мітками про події, що стосуються системи. Практично всі програми та системи створюють файли журналу.

Файл журналу — це документація подій, які відбуваються в системі в певний час. Кілька прикладів журналів: журнал доступу, журнал транзакцій і журнал аудиту. На веб-сервері журнал аудиту містить список усіх файлів, які користувачі запитували на веб-сайті. З файлів журналу сервера адміністратор може отримати таку інформацію, як кількість відвідувачів, кількість запитів сторінки, домен відвідувачів тощо. У Microsoft Exchange журнал транзакцій — це запис усіх змін, внесених до бази даних Exchange. Інформація, яку потрібно додати до бази даних поштової скриньки, спочатку записується в журнал транзакцій Exchange, а потім вміст журналу транзакцій записується в базу даних Exchange Server. Журнал аудиту реєструє хронологічну документацію дій, таких як ресурси, до яких було отримано доступ, адреси призначення та джерела, позначку часу тощо, які могли вплинути на конкретну операцію чи подію. Кожна діяльність у системі, включаючи перезапуск і завершення роботи, документується як файл журналу. Журнали можна класифікувати наступним чином.

Журнали за замовчуванням: вони генеруються за замовчуванням, коли виконання проекту починається та закінчується, коли виникає помилка та виконання припиняється, а також коли параметри журналювання налаштовані на реєстрацію виконання кожної дії. У цій категорії реєструються події: початок виконання, кінець виконання, початок транзакції, кінець транзакції, журнал помилок і журнал налагодження.

Визначені користувачем журнали: вони створюються відповідно до процесу, розробленого користувачем.

Є журнали, які можна видалити за кілька днів, а деякі потрібно зберігати роками. Щоб зупинити величезне зростання журналів, можна скористатися «Обіг журналів». Обіг журналів надає засоби ротації, стиснення, видалення та альтернативного надсилання журналів, що полегшує адміністрування систем, які

генерують велику кількість журналів. Час ротації журналів можна вказати у файлі конфігурації журналу ротації відповідно до вимог користувача.

Дані журналу надають інформацію для виявлення та усунення несправностей обладнання, помилок конфігурації та збоїв обладнання. Журнали містять записи про всі транзакції. Отже, журналювання є критичним у будь-якій системі [7].

ELK — це абревіатура проектів з відкритим кодом Elasticsearch, Logstash і Kibana, як показано на рис. 1.8. Усе це об’єднано разом для перегляду синтаксичного аналізу, зберігання, пошуку та аналізу. Тепер це більш застосовується для візуалізації журналів у реальному часі. Журнали/документи від клієнта аналізуються для стеку на сервері під назвою Elasticsearch від Logstash. Потім Kibana візуалізує журнали/документи, присутні в Elasticsearch.

Рис. 1.8 ELK Stack

Elastic Stack забезпечує централізоване журналювання та дозволяє здійснювати централізований пошук у всіх журналах. Elastic Stack — це універсальна колекція інструментів програмного забезпечення з відкритим вихідним кодом, реалізованих на основі підходу розподіленого збирача журналів, що полегшує збір інформації з даних [8].

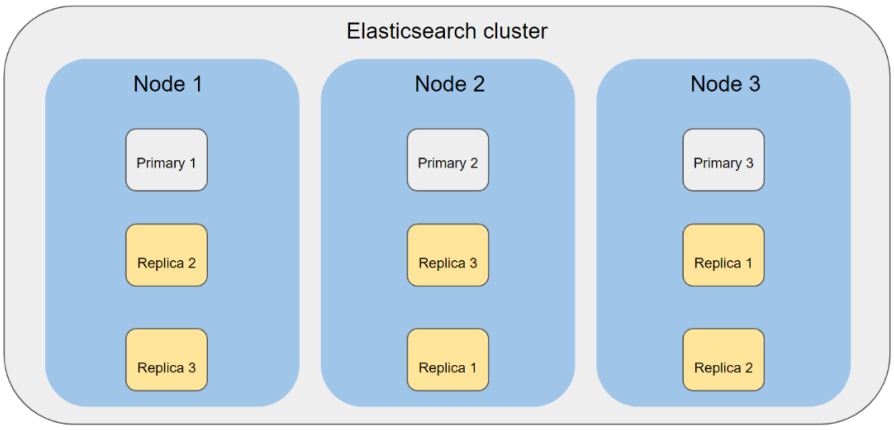


Рис. 1.9 Кластер Elasticsearch

Elasticsearch — це пакет із відкритим вихідним кодом, який є високомасштабованим повнотекстовим механізмом і механізмом аналітики. Це один із кращих пакетів для зберігання, пошуку, аналізу даних, малих і великих обсягів у режимі реального часу. Він містить багато концепцій, які використовуються для створення Elasticsearch.

Logstash це безкоштовний і відкритий конвеєр обробки даних на стороні сервера, який використовується як механізм збору даних із можливостями конвеєрної обробки в реальному часі. Це конвеєр обробки даних, який має здатність отримувати дані з кількох джерел одночасно, нормалізує їх, а потім надсилає в «сховище» під назвою Elasticsearch.

Logstash можна налаштувати різними способами для роботи з усіма форматами журналів. Коли дані переміщуються від джерела до схованки, цей пакет фільтруватиме записи журналу та аналізуватиме кожну подію, ідентифікуватиме поля імен для створення структури та перетворюватиме їх у нормалізуючий формат [9].

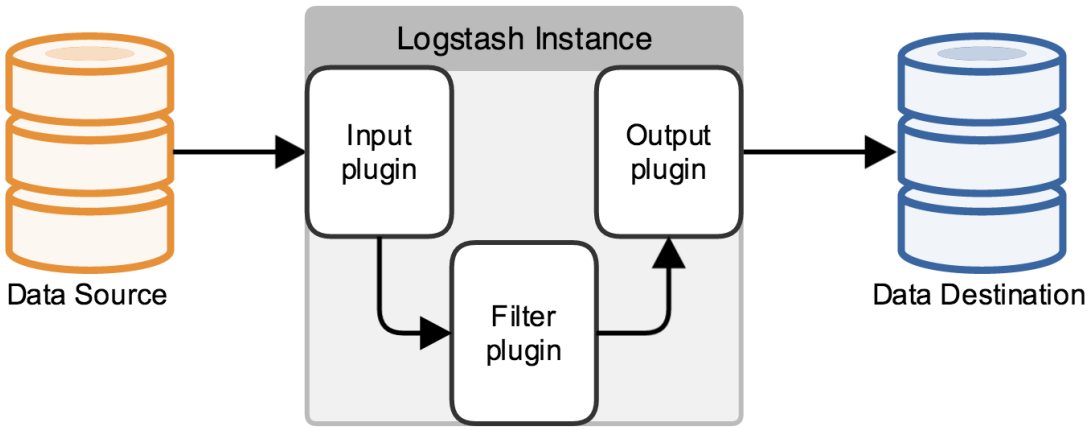


Рис. 1.10 Типовий пайплайн Logstash

Увімкнувши плагін введення HTTP, Logstash може отримувати однорядкові або багаторядкові події через HTTP(s). Події з додатків можуть надсилати їх за допомогою HTTP-запиту з тілом до кінцевої точки, розпочатої цим входом. Тоді Logstash перетворить вхідну подію та розбере її у нормалізований спосіб з усіма іншими подіями. Існують також інші способи використання цього плагіна, наприклад отримання запитів на веб-перехоплення для інтеграції з іншими службами та програмами. Цей плагін підтримує стандартні базові заголовки автентифікації HTTP для ідентифікації запитувача. Під час надсилання даних до Logstash додається набір імені користувача та пароля. Налаштування SSL – ще один варіант безпечного надсилання даних через HTTP.

Kibana — це платформа з відкритим кодом, яка пропонує функцію візуалізації. Тут це пов’язано з роботою з Elasticsearch. За допомогою Kibana користувач може переглядати, шукати, аналізувати та взаємодіяти з даними в Elasticsearch. За допомогою Kibana легко працювати з величезними даними, оскільки Kibana пропонує такі функції візуалізації, як графіки, таблиці, діаграми тощо, за допомогою яких ми можемо переглядати та розуміти дані в абстрактній формі.

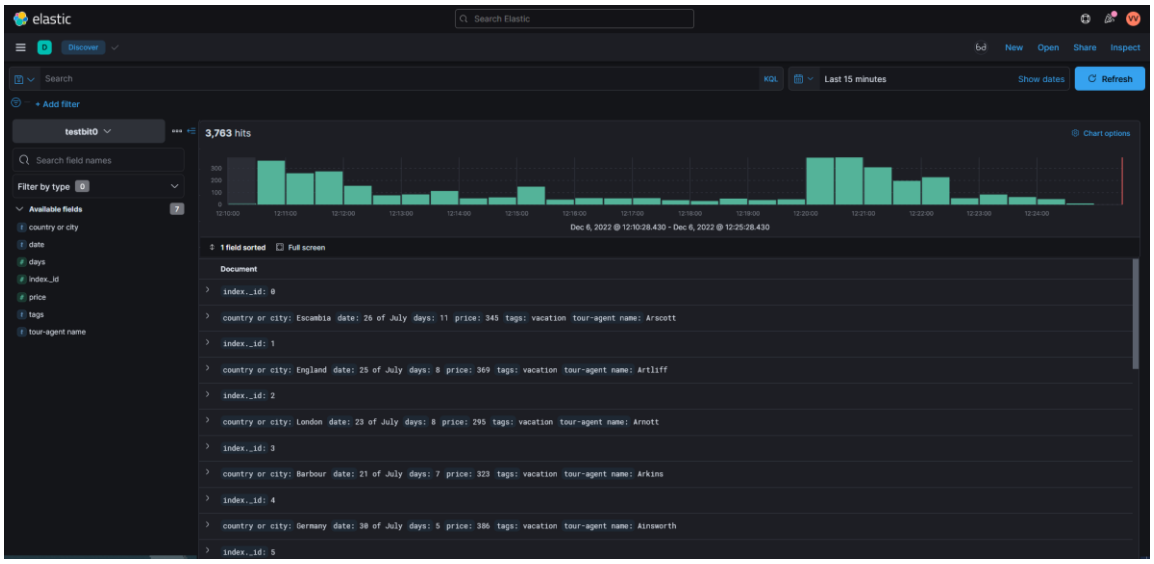


Рис. 1.11 Kibana

Kibana складається з бічної панелі навігації з різними розділами, як-от Discover, Visualize, Dashboard, Timelion, Management, Dev Tools. Усі ці інструменти описано нижче.

Discover: якщо позначити програму Discover, з’явиться можливість переглянути гістограми даних у Elasticsearch і самі дані в таблиці даних під гістограмами. Також є засіб вибору часу, де можна вибрати діапазон часу, протягом якого потрібно переглянути дані, а також вибрати час оновлення для Kibana. При необхідності є рядок пошуку для будь-яких запитів. Будь-які окремі дані всередині Elasticsearch можна візуалізувати на цій інформаційній панелі.

Visualize: програма Visualize дозволяє візуалізувати дані, що надходять у сховище. Він має багато варіантів для візуалізації даних, таких як лінії, зони та панельні чати.

Time Series Visual Builder — це візуалізатор даних часових рядів, який наголошує на тому, щоб дозволити використовувати всю потужність агрегаційної системи Elasticsearch. Time Series Visual Builder дозволяє об’єднувати нескінченну кількість агрегацій і конвеєрних агрегацій для відображення складних даних у змістовний спосіб.

Dashboard: відображає колекцію пошуків і візуалізацій кожного окремого типу даних. Інформаційну панель можна зберегти з параметрами впорядкування,

зміни розміру та редагування. Збереженою інформаційною панеллю можна поділитися. Якщо параметр візуалізації ввімкнено в Kibana, необроблені дані під візуалізацією відображатимуться за допомогою кнопки «Розгорнути/Згорнути».

Dev Tools: Ця сторінка містить інструменти розробки, які використовуються для взаємодії з даними в Kibana. Ця програма має консольний плагін, який забезпечує інтерфейс користувача з Rest API Elasticsearch. Він має дві основні області: панель редактора та панель відповідей. На панелі редактора до Elasticsearch виконуються такі запити, як пошук, редагування, читання, запис, видалення тощо, а на панелі відповідей відображатимуться вихідні дані/відповіді на запит, зроблений на панелі редактора.

Management: ця програма використовується для виконання конфігурацій Kibana під час виконання, включаючи як початкове налаштування, так і поточні конфігурації шаблонів індексів. Вона також виконує розширені параметри, які налаштовують саму поведінку Kibana та збережені об’єкти, такі як пошук, візуалізація та інформаційні панелі. Збережені пошукові запити, візуалізації та інформаційні панелі можна переглядати, редагувати, видаляти, експортувати та імпортувати з налаштувань керування.

У розділі «Visualize» можна візуалізувати дані у вигляді кругових діаграм, таблиць, графіків тощо. Інформаційна панель відображає колекцію всіх візуалізацій і пошуків. Розділ «Management» дозволяє виконувати налаштування Kibana під час виконання. Цей розділ змінюється, якщо до Kibana приєднано будь-які плагіни, такі як X-Pack. За наявності плагінів розділ «Management» надає додаткові функції. Dev Tools — це консоль, де можна надсилати будь-які запити.

Filebeat — це засіб відправлення даних журналу для локальних файлів. Він відстежує розташування, вказані користувачем, і пересилає їх до Elasticsearch, або Logstash, або Kafka, або Redis для індексування/зберігання залежно від конфігурації. Він читає та пересилає журнали рядок за рядком, коли його переривають, запам’ятовує точну позицію, де було перервано, і починає надсилати журнали знову з цієї конкретної позиції. Filebeat використовує

чутливий до зворотного тиску протокол під час надсилання журналів до Logstash або Elasticsearch. Це означає, що щоразу, коли Logstash зайнятий файлами журналів, Logstash надсилає сигнал Filebeat, щоб уповільнити його процес, а Filebeat уповільнює доставку журналів, доки Logstash не вирішить проблему. Коли Logstash звільниться для отримання нових файлів журналу, Filebeat продовжує процес доставки з попередньою швидкістю. Filebeat не має залежностей під час виконання [10].

1.4. Висновок до першого розділу

В першому розділі роботи описано дистрибутив pfSense та його можливості, проведено аналіз та огляд публікацій що відображають задачі та напрямки досліджень що стосуються об’єкту дослідження, вибрно та обґрунтовано методи вирішення поставленої задачі.

РОЗДІЛ 2
АНАЛІЗ МЕТОДІВ ЗБОРУ ЛОГІВ

2.1. Порівняння способу без агента та з агентом

Існує декілька методів збору журналів подій. В цьому розділі буде детально розглянуто основні з них.

Збір журналів без агентів: у збиранні журналів без агентів журнали, створені на кожному пристрої, збираються без агента. Пристрій або програма, де генерується журнал, безпосередньо надсилатиме дані журналу на центральний сервер. Передача буде захищена за допомогою таких протоколів, як TCP і HTTPS. Режим збору журналів, у якому події збираються віддалено без встановлення агента на джерело. Він використовується, коли збір журналів на основі агента неможливий через технічні, адміністративні або відповідні обмеження.

Як альтернативу інсталяції агента журнали можна збирати з кінцевих точок, налаштувавши утиліти Nxlog (Windows) і Rsyslog (Linux) на цільових кінцевих точках [11].

На дебати щодо того, чи моніторинг на основі агентів чи без агентів є «кращим», відповідали багато разів протягом багатьох років у журнальних/онлайнових статтях, публікаціях у блогах, офіційних документах постачальників тощо. На жаль, більшість із цих статей часто є неповними, неточними, упередженими чи поєднанням того й іншого.

Щоб трохи заплутати ситуацію, різні постачальники програмного забезпечення використовують різні методи моніторингу серверів і робочих станцій. Деякі використовують агентів, деякі ні, а деякі пропонують обидва методи.

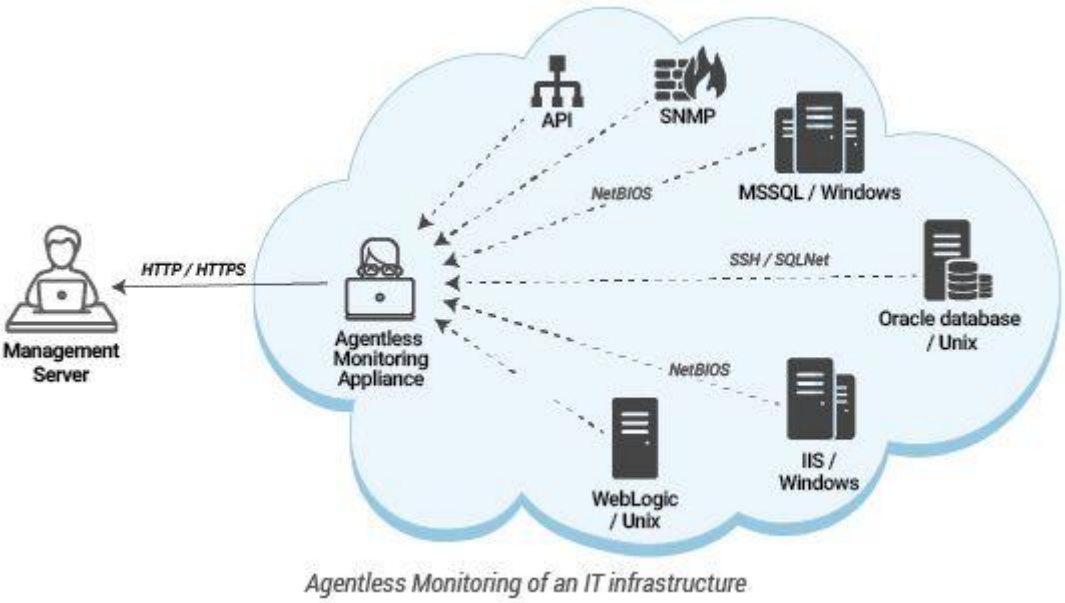


Рис. 2.1 Схема безагентного моніторингу

Спочатку важливо визначити, що відстежується, щоб визначити, чи підхід на основі агента чи без агента є кращим. Наприклад, збір системних показників, таких як дані про продуктивність, зазвичай створює менше проблем, ніж передача великої кількості даних журналу (подій). Крім того, моніторинг на основі агента не є варіантом для пристроїв, які працюють під керуванням власної вбудованої ОС (перемикач, принтер тощо), де неможливо встановити агента.

Програмне забезпечення для моніторингу, звичайно, не єдиний тип програмного забезпечення, яке використовує агентів, багато іншого корпоративного програмного забезпечення (резервне копіювання, розгортання, A/V ...) також використовує агенти. Нижче наведено деякі з міфів щодо того, що передбачає (моніторинг) використання агентів:

- Агенти можуть використовувати забагато ресурсів на контрольованих хостах і сповільнювати роботу контрольованих машин.
- Агенти можуть стати нестабільними та негативно вплинути на ОС хоста.
- Розгортання агентів і керування ними — справа трудомістка та трудомістка.

- Встановлення агентів може вимагати встановлення та розгортання залежностей, необхідних агентам (.NET, Java, …).
- Встановлення стороннього програмного забезпечення знизить безпеку контрольованого хоста.

Цілком зрозуміло, що програмне забезпечення, яке встановлюється на потенційно кожному сервері та робочій станції в мережі, проходить певний рівень перевірки, але агенти досягають успіху в наступних сферах. Безпека: краща безпека, оскільки агенти надсилають дані до центрального компонента, замість того, щоб контрольований сервер налаштовувався на віддалений збір. Надійність: агенти можуть тимчасово зберігати та кешувати відстежувані журнали, якщо з'єднання з центральним сервером моніторингу втрачено, навіть якщо локальні журнали більше не доступні. Агенти також можуть швидше вживати коригувальних заходів, оскільки вони можуть працювати ізольовано (офлайн). Мобільні пристрої неможливо відстежувати за допомогою безагентних рішень, оскільки до них недоступний центральний компонент моніторингу. Продуктивність: агенти можуть застосовувати локальні правила фільтрації та передавати лише цінні дані, таким чином збільшуючи пропускну здатність і одночасно зменшуючи використання мережі. Функціональність: вони пропонують більше можливостей, оскільки фактично немає обмежень щодо того, яку інформацію може збирати агент, оскільки він має повний доступ до контрольованої системи.

Розробка агентів разом із простим у використанні механізмом розгортання вимагає багато часу та ресурсів, тому не дивно, що багато постачальників віддають перевагу моніторингу хостів без агентів. Щоб компенсувати нестачу, ISV, які повинні покладатися виключно на підхід без агентів, зроблять усе можливе, щоб наголосити, що вони не використовують агентів, переконати, що моніторинг без агентів є кращим.

Але, навіть так звані безагентні рішення насправді використовують і агента – єдина різниця полягає в тому, що агент (зазвичай) інтегрований у Windows. Windows не просто чарівним чином обслуговує віддалених клієнтів, які

запитують навантаження даних WMI – вона обробляє ці запити через службу WMI, яка, за всіма намірами і цілями, є агентом. Наприклад, доступ до журналів подій Windows через WMI охоплює значно більше рівнів, ніж прямий доступ до журналів подій [12].

За винятком мережевих пристроїв, на яких неможливо встановити агента, рішення на основі агента забезпечать більш ретельний моніторинг у 9 із 10 випадках.

Деякі постачальники моніторингу журналів подій намагаються переконати, що моніторинг без агентів кращий і легший, але не варто повністю вірити в це. Бувають ситуації, коли неможливо розгорнути повномасштабне рішення моніторингу за допомогою агентів, наприклад, коли доручено контролювати мережу третьої сторони, де встановлення будь-якого програмного забезпечення неможливе. Рішення моніторингу без агентів може заповнити прогалину в цьому випадку.

Наприклад, EventSentry пропонує один із найдосконаліших та найефективніших агентів Windows для моніторингу журналів на ринку. Розробити надійного, безпечного та швидкого агента важко, але це єдиний розумний підхід, який не зрізає кути.

EventSentry також використовує SNMP (без агента) для збору інвентаризації, показників продуктивності, а також інших системних даних з пристроїв, відмінних від Windows, включаючи хости Linux. Цей метод збору страждає від наведених вище обмежень, але оскільки дані журналу надсилаються з пристроїв, відмінних від Windows, через протокол Syslog, це прийнятний компроміс.

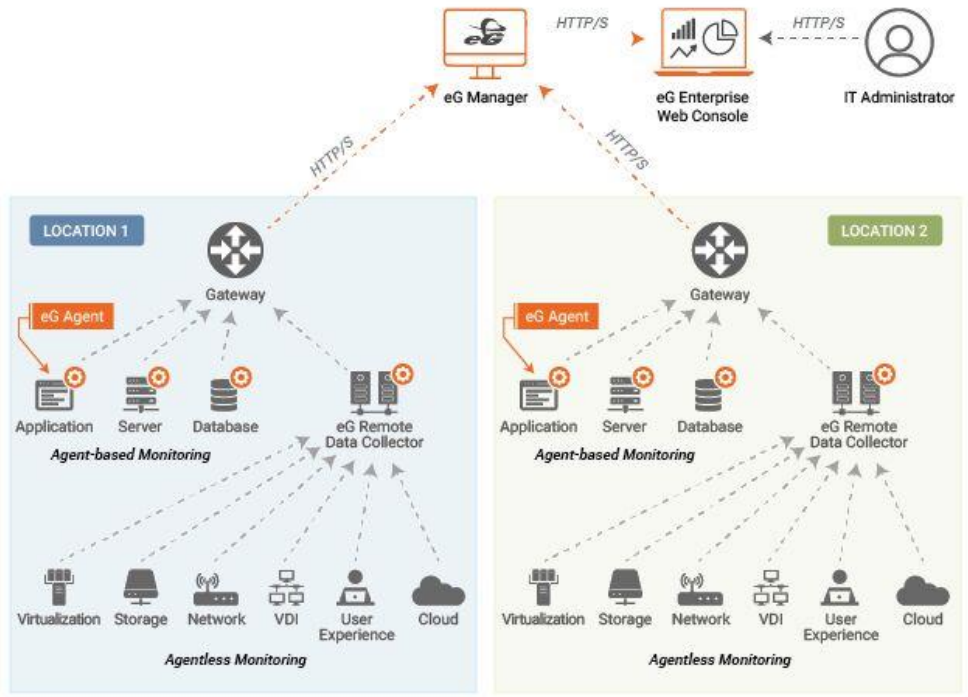


Рис. 2.2 eG Enterprise використовує поєднання агентного та безагентного моніторингу

Застарілі операційні системи, такі як Windows і Unix, не підтримують типи API, які мають нові технології, такі як віртуалізація, контейнери та хмарні платформи. Отже, для моніторингу платформ Windows і Unix і запущених на них додатків краще використовувати агентний підхід. Агент, що працює в системі, також пропонує інші переваги. Наприклад, віддалені дії на сервері ефективніше виконуються за допомогою агента в системі. Точне автоматичне виявлення програм і екземплярів програм, запущених на сервері, можливе лише за допомогою агента в системі (агент може локально отримувати доступ до файлів конфігурації програми, записів реєстру тощо) [13].

2.2. Збір журналів на основі API

У цьому методі API використовується для запитів і передачі даних журналу на безпечний сервер. Також можна використовувати API для збору

журналів і надсилання їх торонньому інструменту аналізу журналів для аналізу даних журналу.

Логування є критично важливим компонентом будь-якої стратегії API. Він надає цінну інформацію про те, як використовується API, і може допомогти виявити проблеми та потенційні сфери вдосконалення.

Існує кілька різних підходів до журналювання, і найкращий підхід для певного API залежатиме від конкретних потреб організації. Однак є деякі загальні найкращі практики, яких слід дотримуватися під час впровадження журналювання для API.

Логування слід проводити централізовано. Якщо є кілька серверів API, може бути важко отримати чітке уявлення про те, що відбувається, якщо всі журнали зберігаються в різних місцях. Централізувавши ведення журналів, можна легше шукати та аналізувати свої журнали, щоб знаходити помилки та відстежувати проблеми.

Є кілька способів централізувати журналювання. Одним із варіантів є використання агента журналювання, який працює на кожному сервері та пересилає журнали на центральний сервер журналу. Крім того, можна налаштувати веб-сервер для запису своїх журналів у центральне розташування.

Слід використовувати правильний рівень журналювання для кожного типу повідомлень журналу. Якщо вивикористовувати неправильний рівень журналювання, то є ризик запису завеликої кількості інформації та перевантаження системи реєстрації, не реєструвати достатньо інформації та не не буде можливості вирішити помилки [14].

Ось короткий огляд різних рівнів реєстрації:

- DEBUG: повідомлення про налагодження, корисні для розробників, які працюють над кодом.
- INFO: інформаційні повідомлення, які можуть бути корисними для операторів або адміністраторів.
- WARNING: попереджувальні повідомлення, які вказують на можливі проблеми.

- ERROR: повідомлення про помилки, які вказують на те, що щось пішло не так.
- CRITICAL: критичні повідомлення, які вказують на те, що щось пішло дуже не так.

Слід зберігати журнали в безпечному місці. Журнали містять велику кількість інформації про трафік і використання API. Їх можна використовувати для відстеження та діагностики проблем і навіть для покращення дизайну API.

Однак усі ці дані платні. Файли журналу можуть швидко стати занадто великими та громіздкими, що ускладнює керування ними. І якщо ними не керувати належним чином, вони можуть становити загрозу безпеці.

Ось чому важливо зберігати свої журнали в безпечному місці, наприклад у корзині S3. Це забезпечить доступ до них лише авторизованим користувачам і захистить їх від випадкового видалення.

Якщо не видаляти свої старі журнали, з часом вони стануть настільки великими, що почнуть впливати на продуктивність API. Це не тільки ускладнить налагодження проблем, але й може призвести до втрати даних, якщо файли журналів будуть пошкоджені.

Щоб уникнути цих проблем, слід налаштувати API на регулярну автоматичну ротацію файлів журналу. Таким чином можна контролювати розмір файлів журналу та завжди мати доступ до точної інформації [15].

2.3. WMI логування

Журналювання подій інструменту керування Windows (WMI) — це метод, який використовується для збору журналів із середовища Windows. Відстеження подій для Windows (ETW) виконується журналом подій WMI. Вони збирають подробиці про події, діагностичні дані, помилки та різні інші дії у мережі.

WMI використовує трасування подій (ETW), і події можна отримати через інтерфейс користувача Event Viewer або інструмент командного рядка Wevtutil.

Активність служби WMI записується у файл WMITracing.log. Постачальники моделі драйверів Windows (WDM) продовжують входити у файл Wbemprov.log.

Файли журналів, створені WMI та різними постачальниками, записують події, дані трасування або діагностики, помилки та різні дії. Лише адміністратори мають доступ для читання папки журналу WMI, яка знаходиться за адресою %windir%\system32\wbem\logs.

Лише основні компоненти WMI або постачальники WMI записують у файли журналу. Можна читати або переглядати дані в цих журналах лише з метою діагностики. Також можна створювати та зберігати власні файли журналу в каталозі журналу WMI.

Файл WMITracing.log містить події, які відстежує WMI. Однак це двійковий файл. Щоб переглянути ці події у форматі, доступному для читання людьми, слід скористатися Event Viewer [16].

За замовчуванням події WMI не відстежуються. Щоб увімкнути трасування подій WMI та знайти події WMI слід виконати певні операції за допомогою інструмента командного рядка wevtutil.

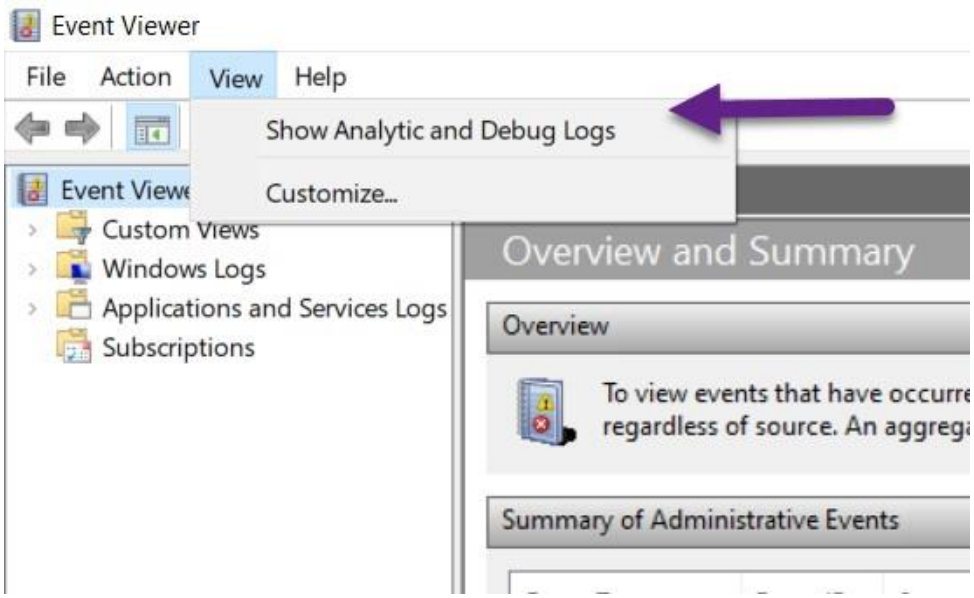


Рис. 2.3 Показ журналів подій в Event Viewer

В операційних системах Windows, починаючи з Windows Vista, WMI створює активний канал трасування під час процесу завантаження. Назва каналу WMI_Trace_Session. На каналі реєструються лише помилки.

Програмний препроцесор трасування Windows (WPP) записує інформацію у двійковий файл. Щоб прочитати файл, слід спочатку перевести його в читабельний текстовий формат. Використовується інструмент під назвою tracefmt.exe з Windows Driver Kit (WDK), щоб виконати переклад. Інструменту потрібна інформація, яка зберігається в деяких пов’язаних файлах. Файли розташовані в каталозі %SystemRoot%\System32\wbem\tmf і мають розширення імені файлу .tmf. Інструменту насправді потрібен один файл .tmf. При створенні цього єдиного файлу об’єднуються всі файли .tmf в інший файл .tmf [17].

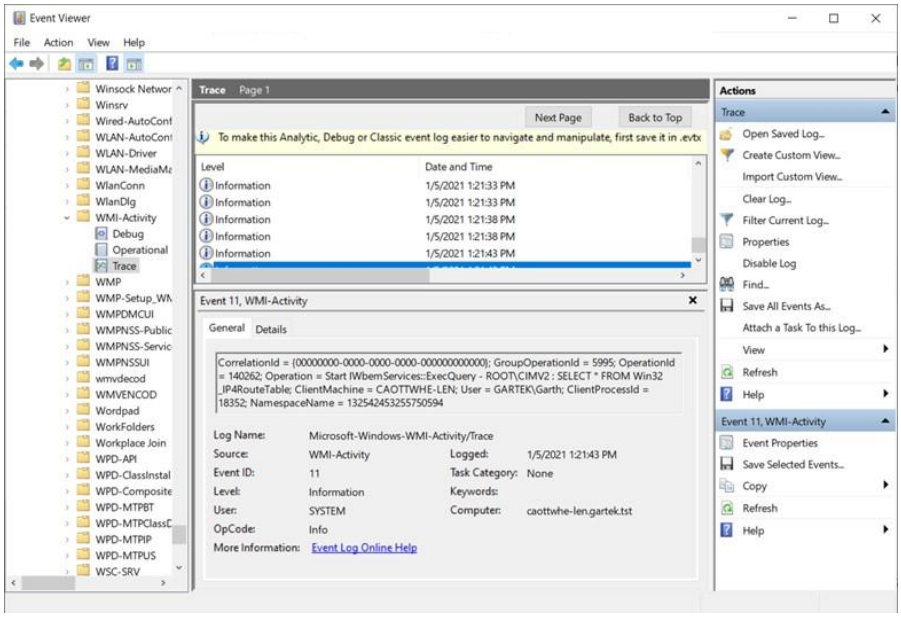


Рис. 2.4 Вигляд логів в Event Viewer

2.4. SNMP пастки

Пастка SNMP – це тип блоку даних протоколу SNMP (PDU). На відміну від інших типів PDU, за допомогою перехоплення SNMP агент може надіслати незапитане повідомлення менеджеру, щоб повідомити про важливу подію.

Перехоплення SNMP створюється пристроєм із підтримкою SNMP, який є агентом, і надсилається до збирача. Колекціонер отримує інформацію в режимі реального часу за допомогою пастки SNMP про кожну важливу подію, насамперед збір подій для керування та моніторингу.

Простий протокол керування мережею (SNMP) — широко використовуваний протокол у моніторингу мережі. Стратегія моніторингу мережі за допомогою SNMP складається з чотирьох ключових компонентів:

- Група з однієї або кількох адміністративних машин, відомих як менеджери.
- Пристрої, які контролюються або керуються за допомогою SNMP, відомі як керовані пристрої. Зазвичай керовані пристрої – це компоненти IT-мережі, наприклад модеми, комутатори, концентратори, маршрутизатори, тощо.
- Агент SNMP, програмний модуль, що працює на керованих пристроях.
- Програмна система SNMP, що працює в менеджері SNMP, відома як система керування мережею (NMS).

Агент знає інформацію про керування своїм керованим пристроєм і перетворює цю інформацію у форму, що підтримується SNMP, і надає інформацію у вигляді змінних [18].

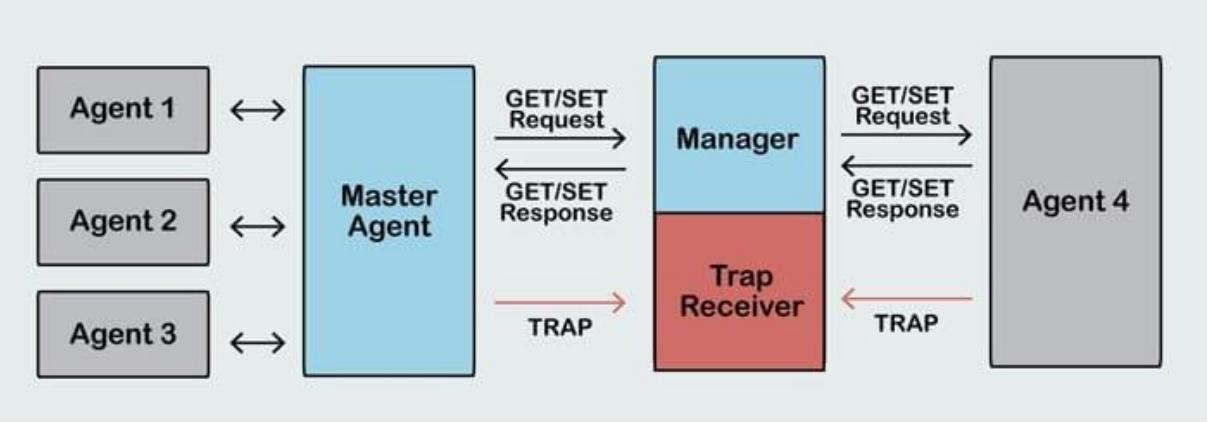


Рис. 2.5 Схема роботи SNMP пастки

Зазвичай менеджер запитує інформацію в агента, надсилаючи запит із підтримкою SNMP у формі PDU, щоб отримати та змінити певні змінні або знайти доступні змінні та відповідні значення.

Проте перехоплення SNMP — це спеціальний тип PDU, за допомогою якого агент надсилає незапитане повідомлення або сповіщення менеджеру про критичні події щодо об’єктів у керованому пристрої.

Переваги пасток SNMP. Розглянемо сценарій, у якому менеджер відповідає за величезну кількість пристроїв у IT-мережі організації, і кожен пристрій, який контролюється під керівництвом менеджера, містить багато об’єктів. Для менеджера може стати майже неможливим або непосильним запитувати інформацію про керування для кожного об’єкта на всіх пристроях для виявлення та зміни топології. Крім того, надсилання запитів у такий спосіб може мати значний вплив на продуктивність мережі.

Повідомлення перехоплення SNMP вирішує це, дозволяючи агенту надсилати незапитане оновлення про важливу подію в об’єкті пристрою. Такий підхід економить ресурси мережі, а також дозволяє уникнути негативного впливу на продуктивність агента.

Пастка SNMP — це популярний механізм, який використовується для керування та моніторингу активності пристроїв у невеликій або глобальній мережі. Платформи маршрутизації здатні генерувати низку подій, які можуть бути дуже корисними для мережевих адміністраторів. Крім того, оперативна група має вибрати та налаштувати сповіщення для кожної події [19].

2.5. Висновок до другого розділу

В другому розділі роботи проведено аналіз методів отримання логів. Детально описано та проведено порівняльний аналіз таких методів збору логів – з агентом та без агента, WMI логування та SNMP пастки.

РОЗДІЛ 3
РОЗРОБКА ТА ТЕСТУВАННЯ СИСТЕМИ

3.1. Використання ELK-стеку для оброблення даних

У цій кваліфікаційній роботі було вирішено використати спосіб через API, оскільки він є доволі зручним та надійним.

Перш за все, слід встановити Elasticsearch. Elasticsearch встановлюється за допомогою менеджера пакетів шляхом додавання списку джерел пакетів Elastic. Спочатку треба імпортувати відкритий ключ GPG ElasticSearch в apt. Потім список джерел ElasticSearch додається до Cloud-Storage. Нарешті, із стороннього пакета встановлюється пакет ElasticSearch. Після встановлення ElasticSearch змінюються конфігурації, щоб отримати доступ до локального сервера. Потім запускається ElasticSearch і додається до ініціалізації для запуску під час завантаження системи [20].

Kibana встановлюється за допомогою менеджера пакетів шляхом додавання списку джерел пакетів Elastic. Далі список Kibana Source додається до Cloud-Storage. Потім з пакета іншого виробника встановлюється пакет Kibana. Файл конфігурації Kibana за шляхом /etc/kibana/kibana.conf змінено таким чином, що він слухає локальний хост. Подібно до ElasticSearch, Kibana також додається до ініціалізації для запуску під час завантаження системи.

Оскільки відкритий ключ уже встановлено для Elasticsearch і такий самий для Logstash, немає необхідності встановлювати ключ з того самого репозиторію, потім Logstash додається до списку джерел і встановлюється з вторинної сторони.

Оскільки цей підхід стеку ELK передає журнали з одного сервера на інший, існує потреба створити сертифікат SSL і пару ключів для надійного та безпечного обміну. Сертифікат розподілятиметься між двома серверами та

підтверджуватиме, що сервери кожного іншого можуть надсилати й отримувати журнали.

На сервері Cloud-Storage створюється каталог для додавання сертифіката SSL і ключів. Оскільки на цьому сервері не налаштовано DNS, немає можливості створити запис і надати спільний доступ до сертифікатів. Отже, тут у файлі OpenSSL.conf поле під поле subjectAltName (SAN) розділу [v3_ca] сертифіката SSL додається з приватною адресою сервера.

Тепер сертифікат SSL і закритий ключ створено у відповідному каталозі. Потім сертифікат, створений на сервері Cloud-Storage, безпечно копіюється в FSB і зберігається в каталозі.

У файлі конфігурації Logstash у розділі «Сертифікати» додано шлях до сертифіката та приватного ключа, щоб між ними був правильний і точний спільний доступ до журналів [21].

Пакет X-pack завантажується як zip-файл і додається до модулів Elasticsearch, Logstash-plugin і Kibana-plugin і вносить необхідні зміни в їхні конфігураційні файли, як-от увімкнення безпеки X-Pack і надання облікових даних для входу для Elasticsearch і Kibana. Після завершення інсталяції, якщо відкрити Kibana, він попросить увійти, і слід увійти, використовуючи ім’я користувача за замовчуванням «Kibana» або «elastic» і пароль «XXXXX» [22].

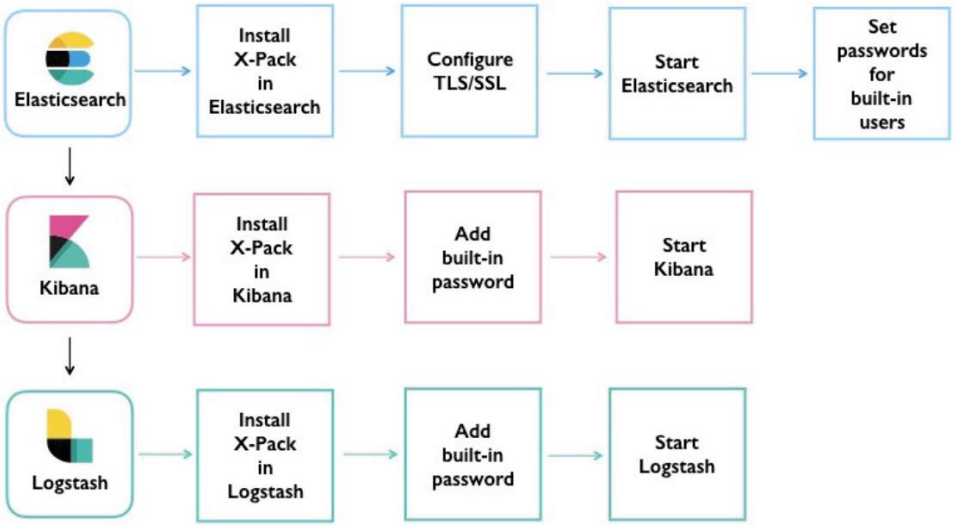


Рис. 3.1 Встановлення X-Pack

Підхід до забезпечення безпеки полягає у створенні різних користувачів і призначенні їм різних ролей, щоб лише користувач, який має дозвіл на доступ до певного файлу журналу, міг переглядати його та вносити зміни, якщо він бажає. На рис. 1.13 показані користувачі за замовчуванням, які були визначені у вузлі Elasticsearch, за винятком першого, створеного з метою тестування. Користувач може вносити лише ті зміни, на які він також має «привілей». Тобто можливо надати користувачеві такі привілеї, як «читати», «записувати», «видалити», тощо, на вкладці користувача. Якщо користувачеві надано лише право «читати», він не може «записати» щось у файл журналу, до якого він має доступ.

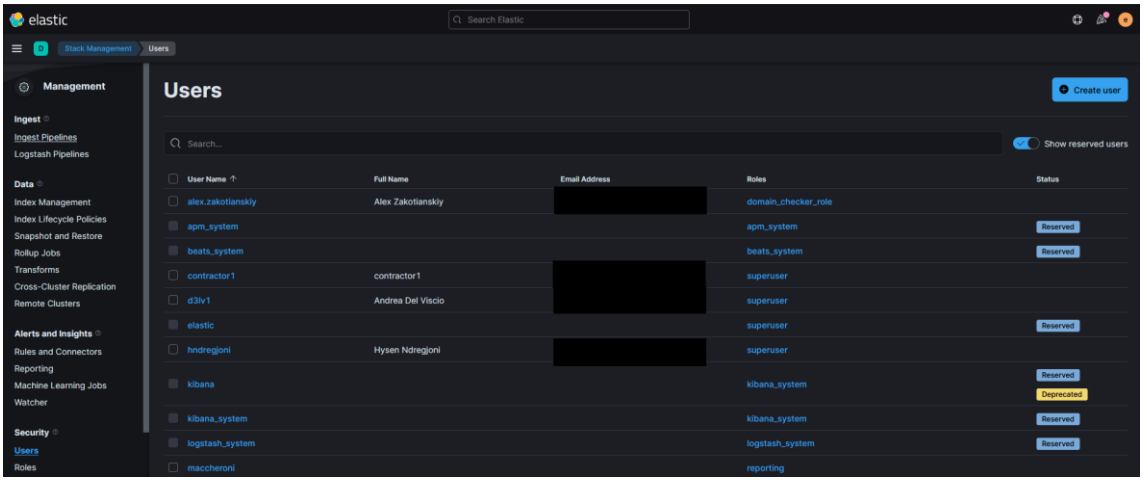


Рис. 3.2 Користувачі у Kibana

Вкладка ролей показує ролі за замовчуванням, створені у вузлі Elasticsearch. Вкладка «Roles» визначає, які дії може виконувати користувач із роллю як на рівні вузла, так і на рівні індексу. Користувач може мати кілька ролей. У Kibana «Dev Tools» — це консоль, де можна задавати запити для створення користувачів, призначати ролі та надавати привілеї користувачам. Це також можна зробити безпосередньо в розділі «Management» Kibana замість написання запитів у консолі Dev Tools.

Можливо забезпечити два види безпеки журналів. Це безпека на рівні документа та безпека на рівні поля. Обидва рівні безпеки надаються на основі

кожного індексу. Безпека на рівні документів забезпечує доступ користувача до певних документів.

Безпека на рівні поля надає користувачеві доступ до певного файлу журналу та обмежує його доступ лише до певних полів, таких як «час», «дата» тощо у файлі журналу. У цій дипломній роботі для журналів у Elasticsearch використовується безпека на рівні документа, оскільки безпека захищена лише для користувачів [23].

Кожен автентифікований GET, PUT, POST або DELETE, отриманий під час пошукового запиту, запиту аналітики, створення документа – будь-якої події Engine будь-якого роду – буде записано в журналі API.

Навіть запити до самого журналу API реєструються в журналі API.

Для автентифікації кінцева точка API Logs вимагає:

- Назву вашого пристрою: [ENGINE].
- Приватний ключ API: [PRIVATE_API_KEY].

```
curl -X GET '<ENTERPRISE_SEARCH_BASE_URL>/api/as/v1/engines/[ENGINE]/logs/api' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer [PRIVATE_API_KEY]'
```

Рис. 3.3 Введення даних для авторизації

Для кожного розгортання Elastic базова URL-адреса Enterprise Search є частиною URL-адреси Enterprise Search, яка передує шляху. Він містить схему, доменне ім’я та порт. У всіх документах це скорочено <ENTERPRISE_SEARCH_BASE_URL>.

Для розгортання Elastic Cloud перейдіть до Elastic Cloud → Розгортання → розгортання. Поруч із Enterprise Search слід вибрати «Копіювати кінцеву точку», щоб скопіювати базову URL-адресу Enterprise Search у буфер обміну.

```
https://my-enterprise-search-deployment.ent.europe-west1.gcp.cloud.es.io
```

Рис. 3.4 URL-адреса Enterprise Search у Cloud

У разі самостійного розгортання треба знайти параметр ent_search.external_url у налаштуваннях конфігурації Enterprise Search.

```
http://localhost:3002
```

Рис. 3.5 Базова URL-адреса самокерованого Enterprise Search

За замовчуванням буде отримано 10 результатів на сторінку в порядку зростання. Результат включатиме:

- Мітку часу.
- Метод HTTP.
- Повний шлях запиту.
- Код стану.
- Тіло запиту та відповідь.
- Запит агенту користувача.

```
// An example JSON payload from the logs/api endpoint.
{
  "results": [
    {
      "timestamp": string,
      "http_method": string,
      "path": string,
      "full_request_path": string,
      "status": number,
      "request_body": string,
      "response_body": string,
      "user_agent": string
    }
  ],
  "meta": {
    "query": string,
    "filters": {
      "date": {
        "from": string,
        "to": string
      }
    },
    "page": {
      "current": number,
      "size": number
    }
  }
}
```

Рис. 3.6 Результат на виході

Щоб відфільтрувати журнали, необхідно вказати часові рамки. Можна комбінувати всі параметри в об’єкті фільтрів. Наприклад, можна надіслати запит GET для отримання всіх подій журналу API з 1 по 5 лютого з кодом статусу 400.

```
curl -X GET '<ENTERPRISE_SEARCH_BASE_URL>/api/as/v1/engines/national-parks-demo/logs/api' \
-H 'Content-Type: application/json' \
-H 'Authorization: Bearer private-xxxxxxxxxxxxxxxxxxx' \
-d '{
  "filters": {
    "date": {
      "from": "2019-02-01T00:00:00+00:00",
      "to": "2019-02-05T00:00:00+00:00"
    },
    "status": "400"
  }
}'
```

Рис. 3.7 Команда для фільтрації за часом

За допомогою запитів в json-форматі можна отримати всю доступну корисну інформацію, але це можна зробити значно зручніше в Kibana – адже там

знаходяться всі необхідні фільтри, зі зручним інтерфейсом, які можна застосувати для перегляду цікавих логів [24].

3.2. Написання зразку програми аналізу

Типова конфігурація logstash являє собою файл(и), який складається з вхідного потоку інформації (input), декілька фільтрів для цієї інформації (filter) і вихідного потоку (output). Виглядає це як один або кілька конфігураційних файлів, які у найпростішому варіанті (який не робить взагалі нічого) виглядає так, як зображено на рис. 3.8.

```
input{

}

filter {

}

output {

}
```

Рис. 3.8 Проста структура конфігураційного файлу

В input налаштовується на який порт будуть приходити логи і за яким протоколом, або з якої папки читати нові файли, що постійно дозаписуються. У FILTER налаштовується парсер логів: розбір полів, редагування значень, додавання нових параметрів чи видалення. Filter це поле для керування повідомленням, яке приходить на Logstash з масою варіантів редагування. У output налаштовується куди відправляється вже розібраний лог, у разі якщо це elasticsearch відправляється JSON запит, у якому відправляються поля зі

значеннями, або ж в рамках дебага можна виводити в stdout чи записувати в файл.

Перш за все, Elasticsearch (іноді його називають ES) — це сучасна пошукова та аналітична система, яка базується на Apache Lucene. Elasticsearch — це база даних NoSQL, повністю відкрита й побудована на Java. Це означає, що він зберігає дані в неструктурований спосіб і не має можливості використовувати SQL для запиту до них.

Кожне повідомлення, індексується як “документ” – це аналог таблиці в реляційних SQL. Також, усі документи зберігаються в індексі – аналогу бази даних SQL [25].


```
{
  "_index": "checkpoint-2019.10.10",
  "_type": "_doc",
  "_id": "yvNZcWwBygXz5W1aycBy",
  "_version": 1,
  "_score": null,
  "_source": {
    "layer_uuid": [
      "dae7f01c-4c98-4c3a-a643-bfbb8fcf40f0",
      "dbee3718-cf2f-4de0-8681-529cb75be9a6"
    ],
    "outzone": "External",
    "layer_name": [
    "TSS-Standard Security",
    "TSS-Standard Application"
    ],
    "time": "1565269565",
    "dst": "103.5.198.210",
    "parent_rule": "0",
    "host": "10.10.10.250",
    "ifname": "eth6",
    ]
}
```


Рис. 3.9 Приклад документу в базі

Перш за все треба виставити правильний input – частина коду яка відповідає за отримання даних з зовнішнього джерела.

```
input {
    elasticsearch {
        hosts => "localhost"
        query => '
            "match_all": {}
        '
    }
}
```

Рис. 3.10 input для отримання журналів подій

На рис. 3.10 зображено input, в якому отримуються всі дані з локального хоста та використовуються для подальшого аналізу.

Після цього слід написати частину filter, в якій буде знаходитись основний код для аналізу та структуризації усіх журналів подій.

Grok фільтр надає можливість фільтрувати та структурувати дані. Цей інструмент ідеально підходить для журналів syslog, журналів apache та інших веб-серверів, журналів mysql і взагалі будь-якого формату журналу, який зазвичай пишеться для людей, а не для використання комп'ютером [26].

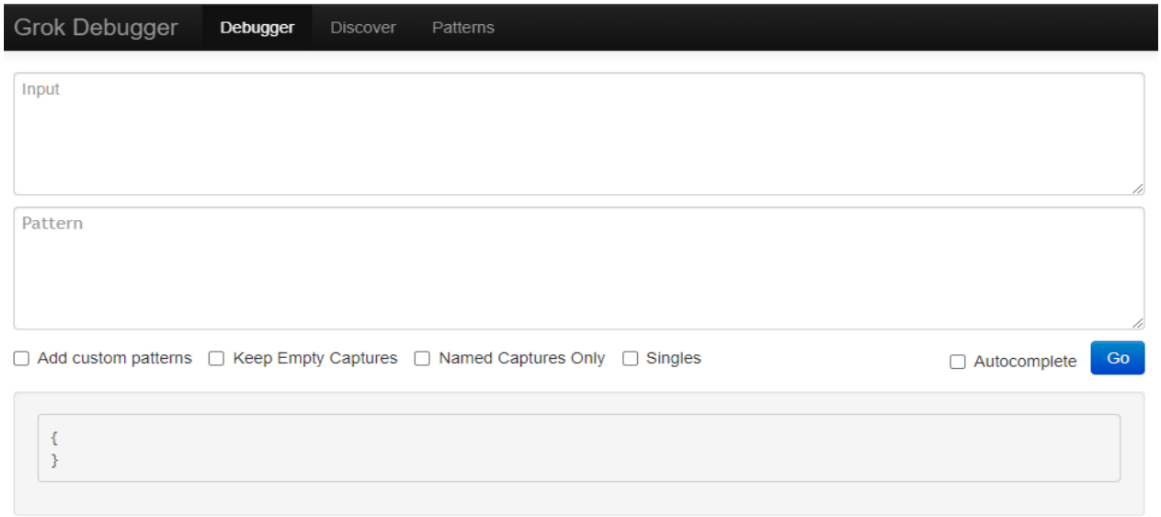


Рис. 3.11 "Grok Debugger" від heroku

Далі пишеться основна частина програми.

3.3. Висновок до третього розділу

В третьому розділі кваліфікаційної роботи описано програмне забезпечення системи. Спроектовано конфігураційний файл, в якому проводиться аналіз та структуризація журналів подій. Описано можливості роботи з Kibana.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Метою кваліфікаційної роботи магістра є дослідження сучасних методів аналізу подій для дистрибутива операційної системи FreeBSD з відкритим кодом, під назвою PfSense. Оскільки, проведення робіт з розробки та використання системи передбачає використання комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з розробки ПЗ комп'ютерних систем, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до наступних вимог. Переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005). Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від

28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

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

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

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

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

При розробці методичного підходу, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп’ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп’ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи [27].

4.2 Підвищення стійкості роботи об’єктів приладобудівної галузі в воєнний час

На основі вивчення факторів, які впливають на стійкість роботи об'єктів приладобудівної діяльності, та оцінки стійкості елементів і галузей виробництва проти уражаючих факторів ядерної, хімічної і біологічної зброї, стихійних лих і виробничих аварій, необхідно завчасно організувати і провести організаційні, інженерно-технічні й технологічні заходи для підвищення стійкості роботи.

Здійснення організаційних заходів передбачає завчасну підготовку всіх структур цивільного захисту, служб і формувань до надзвичайних ситуацій, в тому числі і військових дій.

Вжиттям технологічних заходів підвищується стійкість роботи об'єктів шляхом змінювання технологічних процесів, режимів, можливих в умовах різних надзвичайних ситуацій.

Інженерно-технічні заходи мають забезпечити підвищену стійкість виробничих споруд, технологічних ліній, устаткування, комунікацій об'єкта до впливу уражаючих факторів під час військових дій.

При проведенні цих заходів необхідно враховувати конкретні умови об'єкта народного господарства. Проте є загальні організаційні інженерно-технічні заходи, які мають проводитись на всіх об'єктах.

Підвищення стійкості роботи промислових підприємств в умовах НС мирного і воєнного часів досягається завчасним проведенням комплексу інженерно-технічних, технологічних і організаційних заходів.

Інженерно-технічні заходи (ІТЗ) включають комплекс робіт по підвищенню міцності і надійності будинків, споруд комунально-енергетичних систем, матеріально-технічних запасів.

Технологічні заходи спрямовані на підвищення стійкості виробництва шляхом заміни існуючого технологічного режиму роботи на такий, що виключає можливість виникнення вторинних вражаючих факторів.

Організаційні заходи передбачають розробку і планування дій в умовах НС керівного складу об’єкту, штабу, служб та невоєнізованих формувань ЦЗ по захисту робітників і службовців, проведення рятувальних робіт та відновлення порушеного виробництва.

Одним з найбільш важливих завдань в умовах воєнного часу і надзвичайних ситуацій є забезпечення захисту людей та їх життєдіяльності.

Для підвищення стійкості об’єктів приладобудівної галузі та захисту людей необхідно:

- створити на об'єкті надійну систему оповіщення про загрози нападу противника, радіоактивне забруднення, хімічне і біологічне зараження, загрозу стихійного лиха і виробничої аварії;
- організувати розвідку і спостереження за радіоактивним забрудненням, хімічним і біологічним зараженням;
- організувати гідрометеорологічне спостереження за рівнем води, напрямком і швидкістю вітру, рухом і поширенням хмари радіоактивного забруднення, сильнодіючих отруйних речовин і отруйних речовин;
- створити фонд захисних споруд ЦО, запасів засобів індивідуального захисту і забезпечення своєчасної видачі їх населенню;
- завчасно підготуватись до масової санітарної обробки населення і знезаражування одягу;

– організувати взаємодію з установами охорони здоров'я для медичного обслуговування населення в умовах воєнного часу.

Також в умовах воєнного часу необхідно провести підготовку до евакуації населення, розміщеного в зонах можливих руйнувань і катастрофічного затоплення. Це передбачає завчасну підготовку місць евакуації, організацію прийому евакуйованого населення на територію населених пунктів обслуговування населення в умовах воєнного часу.

Також в умовах воєнного часу необхідно провести підготовку до евакуації населення, розміщеного в зонах можливих руйнувань і катастрофічного затоплення. Це передбачає завчасну підготовку місць евакуації, організацію прийому евакуйованого населення на територію населених пунктів.

Окрім цього, необхідно забезпечити постачання продуктів харчування, питної води, предметів першої необхідності та провести заходи щодо морально-психологічної підготовки населення до виживання в умовах воєнного часу, забезпечити процес чіткого інформування про обстановку та правила дій і поведінки населення в надзвичайних ситуаціях воєнного часу.

Для забезпечення стійкості роботи об'єктів повинні проводитись інженерно-технічні заходи на мережах об’єктів приладобудівної галузі з метою захисту джерел тепла із заглибленням у ґрунт комунікацій. Котельні слід розміщувати в спеціальному окремо розміщеному приміщенні.

Якщо об'єкт одержує тепло з міської теплоцентралі, необхідно провести заходи для забезпечення стійкості трубопроводів і розподільних пристроїв, підведених до об'єкта.

Теплова мережа має будуватися за кільцевою системою з прокладанням труб у спеціальних каналах зі з'єднанням паралельних ділянок. Для відключення пошкоджених ділянок мають бути встановлені запірно-регулюючі засувки, вентилі та ін. Ці пристосування необхідно розміщувати в оглядових колодязях, на території, що не завалюється при руйнуванні будівель.

Система каналізації має будуватись окремо: одна для дощових, друга для промислових вод. На об'єкті має бути не менше двох виводів з підключенням до

міських каналізаційних колекторів, а також виводи і колодязі з аварійними засувками на об'єктових колекторах з інтервалом 50 м на території, що не завалюється, для аварійного скидання неочищеної води в найближчі штучні та природні заглиблення.

На деяких промислових об'єктах є системи для забезпечення технології виробництва: для подання кисню, аміаку, стиснутого повітря та інших рідких і газових реактивів. Для цих систем розробляють заходи для попередження виникнення вторинних факторів зброї, стихійних лих та виробничих аварій і катастроф.

Створення резерву енергетичних потужностей за рахунок автономних пересувних електростанцій, а також місцевих джерел електроенергії. Підготовка автономних електростанцій до роботи за спеціальним режимом (графіком) для забезпечення технологічних процесів виробництва, для яких неможливі тривалі перерви в електропостачанні.

З метою попередження аварій на електричних мережах необхідно установити автоматичну систему відключення при виникненні перенапруги. Повітряні лінії електропостачання замінити на підземно-кабельні [28].

ВИСНОВКИ

В першому розділі кваліфікаційної роботи освітнього рівня «Магістр» детально описано про дистрибутив pfSense та його можливості, проведено огляд та аналіз публікацій що відображають задачі та напрямки досліджень що стосуються об’єкту дослідження, вибрано та обґрунтовано методи вирішення поставленої задачі.

В другому розділі кваліфікаційної роботи проведено порівняння способів отримання журналів подій безагентним способом та за допомогою агента, проведено аналіз методу збору журналів подій за допомогою API, проведено аналіз WMI логування та проведено аналіз SNMP пастки.

В третьому розділі кваліфікаційної роботи описано використання ELK-стеку для оброблення даних та виконано написання зразку програми аналізу.

У дипломній роботі обгрунтовано вирішення наукового завдання щодо впровадження сучасних технологій веб-програмування в поєднанні з онтоорієнтованими засобами електронного навчання. Метою наукових результатів є дослідження методів аналізу подій для дистрибутива PfSense. В ході дослідження методів та засобів розробки таких програмних систем були зроблені наступні висновки.

Розроблено метод швидкого та зручного аналізу подій дистрибутива pfSense для подальшого використання у корпоративних цілях для захисту мережі від можливих атак кіберзлочинців.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 pfSense® - World's Most Trusted Open Source Firewall URL: https://www.pfsense.org (дата звернення: 10.10.2022).

2 What is pfSense® software? URL: https://www.sunnyvalley.io/docs/network-security-tutorials/pfsense (дата звернення: 10.10.2022).

3 System Monitoring URL: https://docs.netgate.com/pfsense/en/latest/monitoring/logs/settings.html (дата звернення: 12.10.2022).

4 Configure pfSense Firewalls URL: https://www.manageengine.com/products/firewall/help/configure-pfsense-firewalls.html (дата звернення: 15.10.2022).

5 Ship logs from pfSense URL: https://docs.logz.io/shipping/security-sources/pfsense.html (дата звернення: 18.10.2022).

6 pfSense 2 Cookbook by Matt Williamson URL: https://www.oreilly.com/library/view/pfsense-2-cookbook/9781849514866/apas05.html (дата звернення: 22.10.2022).

7 Що таке файл журналу (і як відкрити один)? URL: https://ua.savtec.org/articles/howto/what-is-a-log-file-and-how-do-i-open-one.html (дата звернення: 25.10.2022).

8 What is the ELK Stack? URL: https://www.elastic.co/what-is/elk-stack (дата звернення: 25.10.2022).

9 Logstash 101: Using Logstash in a Data Processing Pipeline URL: https://www.bmc.com/blogs/logstash-using-data-pipeline/ (дата звернення: 27.10.2022).

10 ELK Stack Tutorial: What is Kibana, Logstash & Elasticsearch? URL: https://www.guru99.com/elk-stack-tutorial.html (дата звернення: 30.10.2022).

11 Agent vs Agentless Log Collection URL: https://www.snaresolutions.com/wp-content/uploads/2020/03/Snare-Agents-vs-Agentless-1.pdf (дата звернення: 02.11.2022).

12 Agent vs Agentless: Why you should monitor (event) logs with an agent-based log monitoring solution URL: https://www.eventsentry.com/blog/2017/03/agent-vs-agentless-why-you-should-monitor-event-logs-with-an-agent-based-log-monitoring-solution.html (дата звернення: 02.11.2022).

13 Agent vs Agentless Monitoring Pros and Cons URL: https://www.eginnovations.com/blog/agentless-vs-agent-based-monitoring/ (дата звернення: 02.11.2022).

14 Use Logstash to stream logs with HTTP Data Collection API (legacy) URL: https://learn.microsoft.com/en-us/azure/sentinel/connect-logstash (дата звернення: 05.11.2022).

15 API for Logs URL: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/API-for-Logs.htm (дата звернення: 05.11.2022).

16 Tracing WMI Activity URL: https://learn.microsoft.com/en-us/windows/win32/wmisdk/tracing-wmi-activity (дата звернення: 09.11.2022).

17 How to Enable WMI Logging in Windows URL: https://www.recastsoftware.com/resources/how-to-enable-wmi-logging-in-windows/ (дата звернення: 09.11.2022).

18 What is an SNMP Trap? All About SNMP Traps URL: https://www.solarwinds.com/resources/it-glossary/snmp-traps (дата звернення: 09.11.2022).

19 SNMP Traps Explained – A Full Breakdown of What it Does! URL: https://www.pcwdld.com/snmp-trap (дата звернення: 19.11.2022).

20 Set up Elasticsearch URL: https://www.elastic.co/guide/en/elasticsearch/reference/8.5/install-elasticsearch.html#install-elasticsearch (дата звернення: 22.11.2022).

21 Kibana set up URL: https://www.elastic.co/guide/en/kibana/8.5/install.html (дата звернення: 25.11.2022).

22 Install X-Pack URL: https://www.elastic.co/downloads/x-pack (дата звернення: 25.11.2022).

23 Configure security in Kibana URL: https://www.elastic.co/guide/en/kibana/current/using-kibana-with-security.html (дата звернення: 25.11.2022).

24 API logs API URL: https://www.elastic.co/guide/en/app-search/current/api-logs.html (дата звернення: 25.11.2022).

25 The complete guide to the elk stack URL: https://logz.io/learn/complete-guide-elk-stack/ (дата звернення: 25.11.2022).

26 Grok Constructor URL: https://grokconstructor.appspot.com/do/match (дата звернення: 25.11.2022).

27 Горбаченко С.А., Дикий О.В., Флюнт М.О., методичні вказівки з дисципліни «Охорона праці та безпека життєдіяльності», (2020): (дата звернення: 8.12.2022).

28 Стручок В.С., Методичні вказівки з дисципліни «Охорона праці та безпека життєдіяльності» стор. 135-144, м. Тернопіль, (2022) (дата звернення: 14.12.2022).

Додаток А

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

УДК 004.062
В. Василенко, Н. Стадник
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ СТАКУ ELK ДЛЯ ДОСЛІДЖЕННЯ ПОДІЙ

UDC 004.062
V. Vasylenko, N. Stadnyk

USING ELK STACK TO RESEARCH OF EVENTS

Logstash – це засіб для збору, фільтрації та структуризації log-файлів (подій). Це безплатний та open source додаток, створений на базі Apache Lucene. Додаток Logstash входить до стаку ELK - Elasticsearch, Logstash і Kibana, де Elasticsearch – пошукова і аналітична система, Logstash – серверний конвеєр для обробки даних, який може отримувати дані одночасно з декількох джерел, переробляти їх та відправляти на сервер, в нашому випадку – це Elasticsearch. Kibana – засіб для візуального подання інформації, який дозволяє створювати різні діаграми та графіки з інформації, яка знаходиться в Elasticsearch.

Рисунок 1. Схема роботи стаку ELK

Logstash використовує спеціальні вирази, які називаються грок патерни (grok-patterns) для розбору log-файлів. Grok – це фільтр всередині Logstash, який використовується для структуризації неструктурованих даних. Він знаходиться поверх регулярного виразу (regex), і використовує текстові шаблони для зіставлення рядків у файлах журналів. Logstash постачається з більш ніж 100 вбудованих шаблонів, які можна використати для загальних системних журналів apache, linux, haproxy, aws тощо. Також є можливість написання свого власного патерну, за яким буде розбиратись лог. Для цього можна використати спеціалізовані сервіси для написання патерну, одним з найкращих є грок дебагер «herokuapp», в якому можна знайти приклади для різних частин логу. Синтаксис шаблону патерну виглядає наступним чином – %{SYNTAX:SEMANTIC}.

Після написання патерну, який буде проходитись по всіх рядках log-файлу, потрібно відправити структуровані файли на Elasticsearch. Після цього отримані дані можна буде візуалізувати за допомогою багатьох вбудованих засобів та візуалізацій, до яких входять різноманітні графіки і таблиці.

Література

1. What is the ELK Stack? URL: https://www.elastic.co/what-is/elk-stack.
2. The complete guide to the elk stack. URL: https://logz.io/learn/complete-guide-elk-stack/.
3. ELK Stack Tutorial: What is Kibana, Logstash & Elasticsearch? URL: https://www.guru99.com/elk-stack-tutorial.html.

УДК 004.062
В. Василенко, Н. Стадник
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЛОГУВАННЯ – ЩО ЦЕ І В ЧОМУ ЙОГО КОРИСТЬ

UDC 004.062
V. Vasylenko, N. Stadnyk

LOGGING – WHAT IS IT AND WHAT IS ITS BENEFIT

Якщо в роботі сервера, комп'ютера або програмного забезпечення виникла невідома помилка, насамперед дивляться логи. Лог – це текстовий файл з інформацією про дії програмного забезпечення або користувачів, який зберігається на комп'ютері або сервері. Це хронологія подій та їх джерел, помилок та причин, з яких вони сталися. Читати та аналізувати логи можна за допомогою спеціального ПЗ.

Логуванням називають запис логів. Воно дозволяє відповісти на питання, що відбувалося, коли і за яких обставин. Без логів складно зрозуміти, через що з'являється помилка, якщо вона виникає періодично і лише за певних умов. Записується інформація не тільки про помилки, але і про причини їх виникнення.

Існують різні рівні та різні подробиці логування. Якщо помилка унікальна, використовують максимально докладні логи; якщо це не потрібно, збирають лише ключову інформацію. Для роботи з логами та пошуком інформації у великих текстових даних використовують спеціалізовані інструменти. Для зручної роботи з логами їх ділять на типи. Це допомагає швидше знаходити потрібні та вибирати правильні інструменти для роботи з ними. Наприклад, виділяють:

- системні логи, тобто ті, які пов'язані із системними подіями;
- серверні логи, що реєструють звернення до сервера і помилки, що виникли при цьому;
- поштові логи, що стосуються вхідних/вихідних листів та відслідковують помилки, через які листи не були доставлені;
- логи аутентифікації.

Лог файли можуть знадобитися у багатьох ситуаціях під час роботи зі сайтами, ПК або сервером. Але зверніть увагу, що логи не зберігаються вічно, тому якщо виникла потреба перевірити їх, слід це робити своєчасно. Наприклад, часто хостинг-провайдери зберігають логи до 14 днів, а далі вони видаляються та записуються нові.

Отже, якщо сайт зламали більше кількох тижнів тому, встановити причину по логах не можливо, при умові, що логи вже видалені.

Література

1. Usage logging. URL: https://www.ibm.com/docs/en/csfdcd/7.1?topic=ult-usage-logging/
2. Logging. URL: https://en.wikipedia.org/wiki/Logging_(software).
3. An introduction to logging for programmers. URL: https://www.freecodecamp.org/news/you-should-have-better-logging-now-fbab2f667fac/.
4. The Log: What every software engineer should know about real-time data's unifying abstraction. URL: https://engineering.linkedin.com/distributed-systems/log-what-every-software-engineer-should-know-about-real-time-datas-unifying.