Лабораторна робота №9

Розгортання Wazuh Server та Dashboard.

Мета: Набути практичних навичок розгортання та початкового налаштування системи безпекового моніторингу Wazuh, ознайомитися зі структурою її основних компонентів (Server, Dashboard) і принципами їх взаємодії. Навчитися розгортати готове середовище Wazuh Appliance у VirtualBox, перевіряти коректність роботи основних служб та доступність вебінтерфейсу Wazuh Dashboard, готуючи систему до подальшого підключення агентів у наступних лабораторних роботах.

Інструменти: гіпервізор VirtualBox, модель комп'ютерної мережі.

Теоретичні відомості

У попередніх лабораторних роботах було створено віртуалізоване стендове середовище у VirtualBox, що складається з чотирьох хостів:

Serv-G-N-1 (Windows Server 2022) – контролер домену з ролями AD DS, DNS і DHCP, на якому встановлено Icinga 2 Agent для локального моніторингу ресурсів.

Serv-G-N-3 (Ubuntu Server 24.04) – сервер моніторингу з Icinga 2, веб-інтерфейсом Icinga Web 2, базою даних Icinga DB, Icinga Director для централізованого керування конфігураціями, а також інтеграцією з Graphite та Grafana для збору та візуалізації метрик.

WS-G-N-1 (Windows 10) – робоча станція, включена до внутрішнього домену, з встановленим Icinga 2 Agent; додана до системи моніторингу через Icinga Director.

Serv-G-N-5 (Ubuntu Server 24.04) – сервер з Icinga 2 Agent для локального моніторингу ресурсів.

Мережеве середовище забезпечує взаємодію між вузлами, а система Icinga 2 інтегрована з доменною інфраструктурою для подальшого моніторингу її елементів.

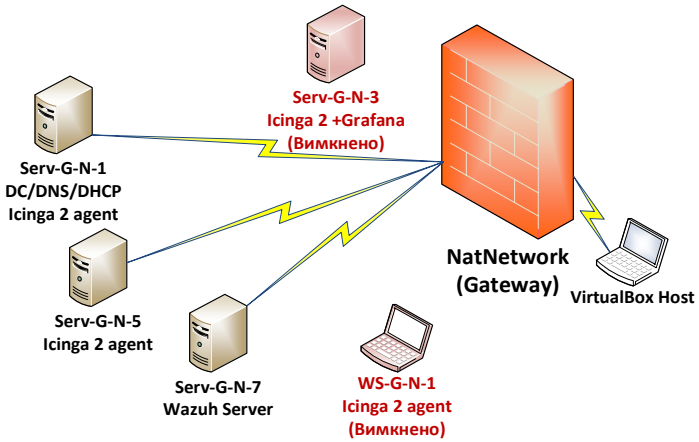

Рис. 9.1. Топологія мережі

У зв'язку із завершенням вивчення системи моніторингу Icinga 2 та переходом до наступного етапу курсу — розгортання і дослідження систем безпекового моніторингу Wazuh та Splunk, із метою оптимізації використання обчислювальних ресурсів стенду, прийнято рішення вимкнути віртуальні машини Serv-G-N-3 (Ubuntu Server з Icinga 2) та WS-G-N-1 (Windows 10 робоча станція).

Це дозволяє вивільнити ресурси процесора, пам'яті та дискового простору, необхідні для розгортання нових компонентів, що будуть використовуватися у наступних лабораторних роботах.

Для виконання поточної роботи до мережі додається сервер Serv-G-N-7, на якому розгортається Wazuh Appliance — окрема віртуальна машина, що містить компоненти Wazuh Server (Manager, API) та Elasticsearch + Kibana (Dashboard). Serv-G-N-7 функціонально замінює сервер Serv-G-N-3 у частині моніторингу систем (але тепер для безпекового моніторингу) та забезпечує ізоляцію середовища для проведення лабораторної роботи.

Підготовка Wazuh Appliance у VirtualBox

Для розгортання серверу Wazuh використаємо один з найпростіших методів – імпорт віртуальної машини з шаблону розробника. Завантажуємо з сайту розробника актуальний файл wazuh-4.14.0.ova. Виконуємо імпорт віртуальної машини. У меню VirtualBox – File - Import Appliance... обираємо завантажений файл. Під час імпорту можна одразу змінити назву віртуальної машини на Serv-G-N-7 (Wazuh Appliance). Після

завершення імпорту змінюємо параметри ВМ, щоб ресурси відповідали невисоким вимогам до стенду. CPU 1 ядро, RAM 8 ГБ.

Після завершення імпорту ВМ виконуємо налаштування мережевого підключення імпортованого хосту. У Settings – Network для ВМ, у налаштуваннях Adapter 1 обираємо тип підключення — NAT Network, і вказуємо ту саму мережу, що використовується іншими вузлами стенду (наприклад, SNM-N). Це забезпечить взаємодію між Wazuh Server і рештою вузлів (наприклад, Windows Server 2022 або Ubuntu Agent).

Запускаємо віртуальну машину. Зазвичай Wazuh Appliance базується на Linux-servers.

Поточна (версія 4.14) на момент написання цього документу ВМ побудована на Amazon Linux 2023. Це власна збірка Amazon, що базується на Fedora (точніше — на Fedora Rawhide / RHEL-подібній системі). У неї своя репозиторна система і dnf як менеджер пакетів. Тобто вона не базується на Debian або Ubuntu, а належить до Red Hat-сімейства.

Після завантаження системи — входимо у консоль з дефолтними обліковими даними:

user: wazuh-user
password: wazuh

Дефолтні облікові дані можуть змінюватись залежно від версії збірки. Їх можливо перевірити на сайті, звідки завантажується OVA-файл апплайнсу.

Рис. 9.2. Welcome to the Wazuh OVA version.

Змінюємо ім'я серверу, щоб він відповідав структурі стенду на Serv-G-N-7, де G — номер навчальної групи (двозначний), а N — номер варіанту:

sudo hostnamectl set-hostname Serv-G-N-7

Редагуємо файл /etc/hosts, змінивши локальний запис 127.0.0.1 serv-G-N-7 та перезавантажуємо ВМ:

sudo reboot

Після перезавантаження нове ім'я набуде чинності.

Якщо сервер успішно підключений до мережі, він отримує поточну, динамічну IP-адресу від DHCP-серверу Serv-G-N-1. Переглядаємо отриману адресу:

ip a

або

hostname -I

Найбільш зручним інтерфейсом та безпечним для роботи з Linux-серверами є ssh-підключення. Налаштуємо переадресацію, або «прокидання порту» для організації SSH доступу до Ubuntu серверу з фізичної машини – хосту VirtualBox.

Пункт виконується у меню **[Oracle VirtualBox Manager] – [File] – [Tools] – [Network Manager] – [Nat Network] – [Properties] – [Port Forfarding] – [IPv4]**.

Назва правила NAT – "Serv-G-N-7 SSH",

де G – група,

N – варіант, що Ви виконуєте, протокол – "TCP".

У якості Guest IP задаємо IP-адресу сервера, яку ми отримали за допомогою команди ***ip a*** , Port – 22 – порт «за замовчуванням» для SSH доступу.

У якості Host IP задаємо IP-адресу нашого фізичного ПК (хоста VirtualBox), який можна переглянути через ***ipconfig /all***, у якості Host Port – «вільний», або неіснуючий для обраного IP порт. Обираємо порт за допомогою команди ***netstat -an | findstr "IP_Hosts"***. Наприклад, для стандартної робочої станції Windows порти з 2200 не зайняті.

Робочий ПК (хост VirtualBox), як правило, підключається до мережі на динамічній адресації.
IP адресою Host Port резервуємо адреса мережі **VirtualBox Host-Only Ethernet Adapter**.

На хості VirtualBox виконуємо команди (рис.1.11):

ipconfig /all | Select-String -Context 0,10 "VirtualBox Host-Only Ethernet Adapter"

netstat -an | findstr "Знайдена IP-адреса"

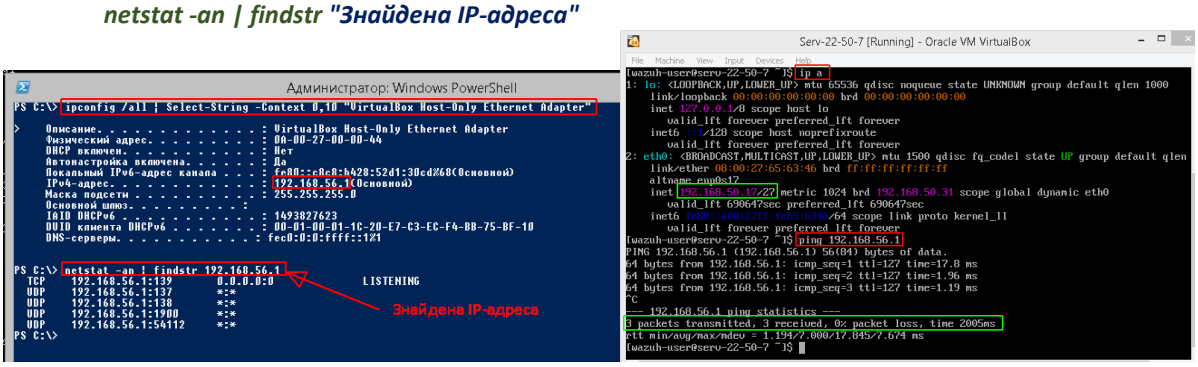

Рис. 9.3. Визначення на хості VirtualBox Host IP та «вільних» портів, та перевірка доступності Gateway мережі ВМ Ubuntu server Serv-22-50-7.

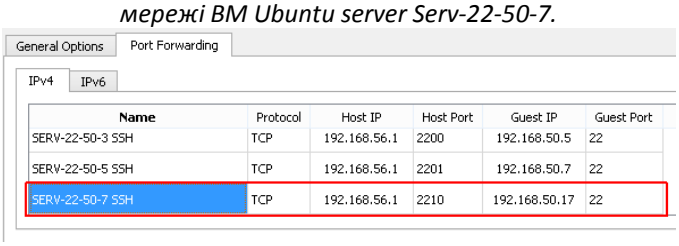

Рис. 9.4. Налаштування правила переадресації порту для SSH до серверу Serv-22-50-7.

У результаті, конфігурація NAT Network Port Forwarding для забезпечення SSH-доступу з фізичного хосту до ВМ Serv-G-N-7 (Wazuh Server) має вигляд, зображений на рис. 9.4. У якості порту переадресації обрано 2210.

Всі подальші дії з командним рядком Ubuntu рекомендовано виконувати за допомогою SSH-клієнта.

Не забуваємо, що зараз Serv-G-N-7 сконфігуровано на динамічну адресацію і адресу він отримує від доменного DHCP на сервері Serv-G-N-1. Сервери, зазвичай, працюють на статиці. Для зміни налаштування динамічної адреси на статичну в Amazon Linux 2023 (systemd-networkd), перевіряємо назву інтерфейсу:

ip link

Вивід команди ***ip link*** для поточної версії серверу показує, що це – eth0.

У Wazuh Appliance, побудованому на Amazon Linux 2023, за замовчуванням використовується система cloud-init — універсальний механізм автоматичної ініціалізації хмарних віртуальних машин. Її основне призначення — забезпечити автоматичне налаштування мережевих параметрів (зазвичай через DHCP), створення користувачів, ключів SSH, hostname тощо під час першого запуску інстансу у хмарних середовищах AWS, Azure або GCP.

Проте у випадку локального розгортання у VirtualBox, cloud-init не має доступу до хмарних метаданих, але все одно виконує базові скрипти конфігурації. У результаті — під час кожного старту системи вона примусово створює DHCP-конфігурацію інтерфейсу eth0, навіть якщо адміністратор задав статичну IP-адресу через systemd-networkd. Це призводить до конфлікту налаштувань: після перезапуску система знову отримує динамічну адресу.

Щоб забезпечити стабільність мережевої конфігурації та можливість використання фіксованої адреси (що є типовою практикою для серверів моніторингу), необхідно відключити мережеву частину cloud-init і перевести керування мережею повністю під контроль systemd-networkd.

Вимикаємо службу cloud-init (щоб вона не перезаписала знову)

sudo mkdir -p /etc/cloud/cloud.cfg.d

echo -e "network:\n config: disabled" | sudo tee /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg

sudo systemctl disable cloud-init

sudo systemctl mask cloud-init

Перейменовуємо файл, який зараз керує мережею

sudo mv /etc/systemd/network/10-cloud-init-eth0.network /etc/systemd/network/10-cloud-init-eth0.network.bak

Створюємо конфігураційний файл для мережевого інтерфейсу eth0 з найвищим (99-тим) пріоритетом ***/etc/systemd/network/99-eth0-static.network.***

Вставляємо у файл наступний вміст:

```
[Match]
Name=eth0

[Network]
Address=192.168.50.9/27
Gateway=192.168.50.1
DNS=192.168.50.3
DNS=192.168.50.1
```

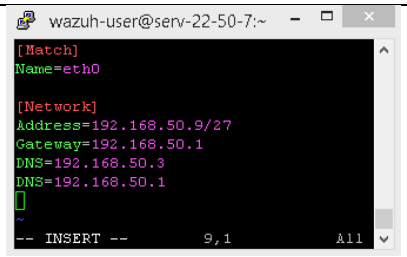

Рис. 9.5. 99-eth0-static.network

Перезапускаємо службу мережі. При цьому «зникає» наше SSH-підключення, бо налаштована у правилі переадресації портів для SSH до серверу Serv-22-50-7 адреса має змінитися на вказану у новому файлі конфігурації (рис.9.5)

```
sudo systemctl restart systemd-networkd
```

Перевіряємо у консолі серверу, чи застосувалась адреса та змінюємо правило переадресації.

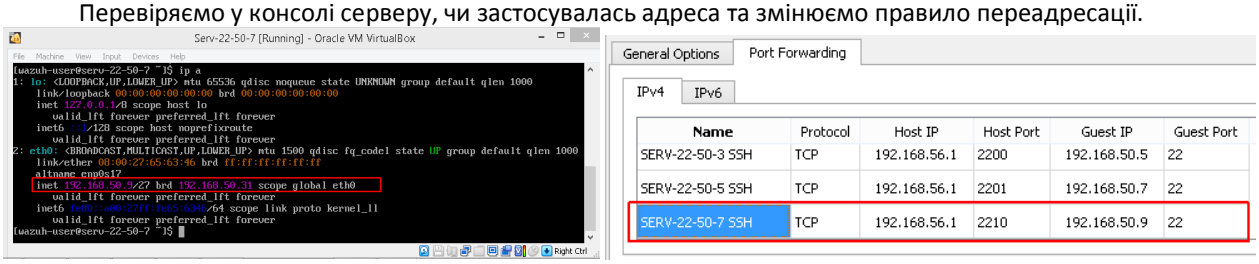

Рис. 9.6. Налаштування правила переадресації порту для SSH до серверу Serv-22-50-7

Налаштування мережі хосту Wazuh server Serv-G-N-7 завершено.

Перевірка стану сервісів Wazuh та взаємодії між компонентами.

Appliance Wazuh — це готова віртуальна машина, побудована розробниками, але після імпорту в VirtualBox вона не завжди автоматично стартує всі служби, а служба Elasticsearch (OpenSearch) вбудована у Wazuh і не має окремого systemd-сервісу elasticsearch.service (це нормально). Деякі компоненти можуть бути disabled, доки адміністратор не увімкне їх вручну.

Отже, активуємо служби вручну. Для цього послідовно вмикаємо основні сервіси Wazuh:

```
sudo systemctl enable --now wazuh-manager
sudo systemctl enable --now wazuh-dashboard
sudo systemctl enable --now wazuh-indexer
```

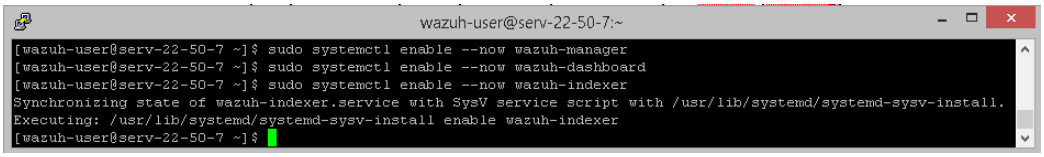

Рис. 9.7. Вмикання основних сервісів Wazuh

Перевіряємо статуси служб. Усі три мають бути active (running).

```
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-dashboard
sudo systemctl status wazuh-indexer
```

Після запуску сервісів та перевірки статусів їх служб, переглядаємо чи система слухає відповідні порти. Іншими словами -перевіряємо доступність веб-інтерфейсу Wazuh. Починаючи з версії 4.4, вебінтерфейс Wazuh Dashboard працює через HTTPS на порту 443.

```
sudo ss -tulnp | grep -E "443|9200"
```

У разі успішної конфігурації сервер має слухати порти 443 (Dashboard) і 9200 (Indexer) – рис.9.8.

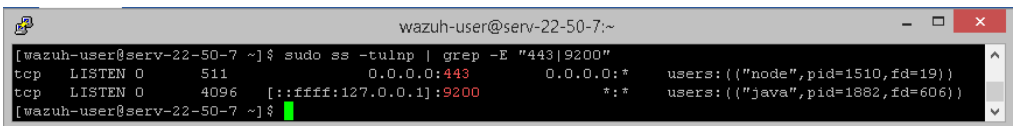

Рис. 9.8. Порти сервісів Wazuh, що «прослуховуються».

Вебінтерфейс відкривається у браузері за адресою https://<IP-адреса-сервера> , але маючи у стендовій мережі єдиний хост з браузером, а саме контролер домену, Windows Server 2022. Щоб не порушувати безпекові налаштування контролеру домену, налаштуємо NAT-переадресацію порту у VirtualBox.

HTTPs-доступ з фізичного хосту до ВМ Serv-G-N-7 (Wazuh Server) має вигляд, зображений на рис. 9.9. У якості порту переадресації обрано нативний порт протоколу 443.

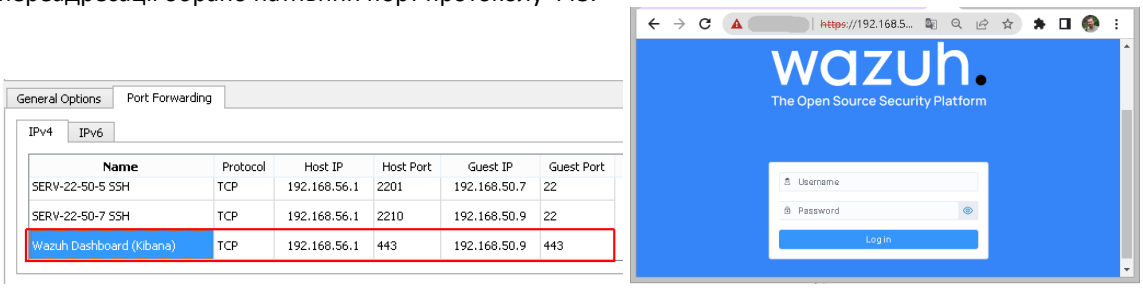

Рис. 9.9. Налаштування правила переадресації порту 443 для https та підключення до серверу Serv-22-50-7.

За замовчуванням у Wazuh Appliance використовуються такі облікові дані адміністратора:

user: admin
password: admin

Після авторизації відкривається головна панель керування Wazuh, що містить зведену інформацію про стан компонентів системи: Manager, Indexer та Dashboard.

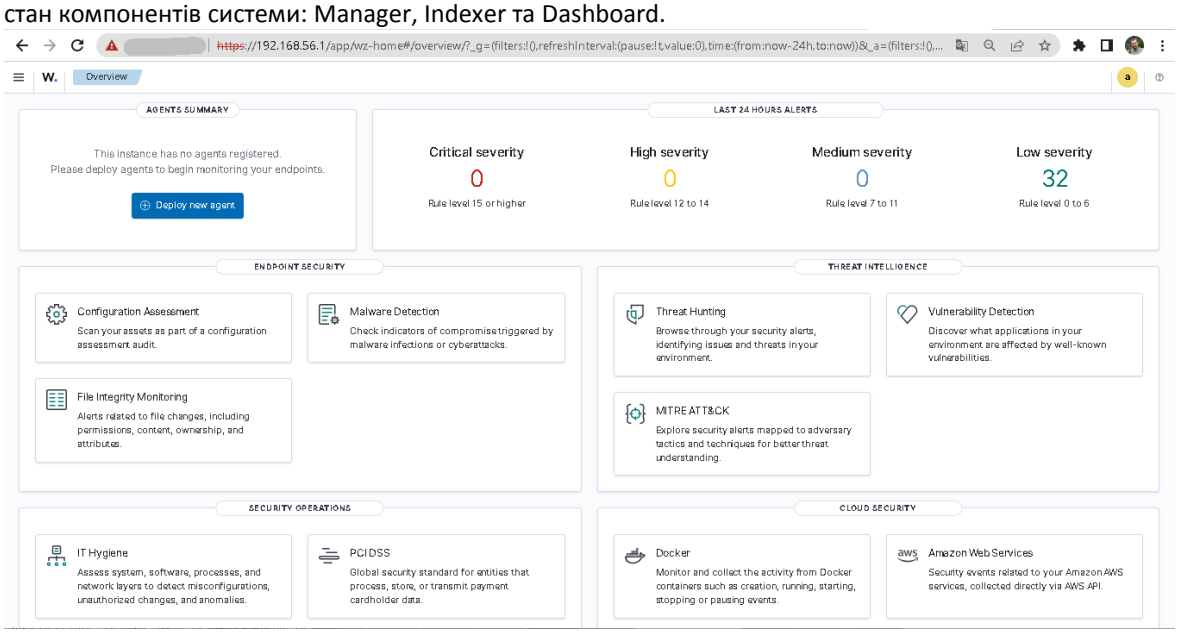

Рис. 9.10. Головна панель керування Wazuh

Перевірка працездатності Wazuh Dashboard.

Після успішного входу до вебінтерфейсу Wazuh Dashboard переконуємось, що сервер функціонує коректно. Після першого успішного входу до Wazuh Dashboard, користувач потрапляє на стартову сторінку “Home – Overview” (рис. 9.10). На цій сторінці відображається зведена інформація про стан системи моніторингу. У разі, якщо сервер щойно розгорнуто, відображається повідомлення:

“This instance has no agents registered. Please deploy agents to begin monitoring your endpoints.”

Це означає, що сервер успішно працює, але ще не підключено жодного агента для збору логів і подій безпеки. Також на цій сторінці можна побачити блоки з попередньо створеними розділами моніторингу:

- Configuration Assessment — аудит конфігурацій безпеки;
- Malware Detection — виявлення шкідливого ПЗ;
- File Integrity Monitoring — контроль цілісності файлів;
- Vulnerability Detection — пошук відомих вразливостей;
- MITRE ATT&CK — відображення подій за матрицею технік атак.

Це підтверджує, що Wazuh Dashboard повністю функціонує, усі його компоненти активні, і сервер готовий до підключення клієнтських систем.

Завдання до лабораторної роботи

1. Імпортувати віртуальну машину Wazuh Appliance у VirtualBox та налаштувати мережеве підключення.
2. Активувати основні служби Wazuh Server і перевірити їхній стан у консолі.
3. Відкрити вебінтерфейс Wazuh Dashboard і переконатися у його працездатності.
4. Перевірити відображення стану компонентів системи та зробити висновок про готовність серверної частини Wazuh до подальшої роботи.

Додаток 1.

Параметри для розрахунку IP-адрес у завданнях.

Таблиця 9.1

№ (N) варіанта	IP-адреса мережі	№ (N) варіанта	IP-адреса Мережі	№ (N) варіанта	IP-адреса мережі
1	192.168.N.0 /27	14	192.168.N.160 /27	27	192.168.N.64 /27
2	192.168.N.32 /27	15	192.168.N.192 /27	28	192.168.N.96 /27
3	192.168.N.64 /27	16	192.168.N.224 /27	29	192.168.N.128 /27
4	192.168.N.96 /27	17	192.168.N.0 /27	30	192.168.N.160 /27
5	192.168.N.128 /27	18	192.168.N.32 /27	31	192.168.N.192 /27
6	192.168.N.160 /27	19	192.168.N.64 /27	32	192.168.N.224 /27
7	192.168.N.192 /27	20	192.168.N.96 /27	33	192.168.N.0 /27
8	192.168.N.224 /27	21	192.168.N.128 /27	34	192.168.N.32 /27
9	192.168.N.0 /27	22	192.168.N.160 /27	35	192.168.N.64 /27
10	192.168.N.32 /27	23	192.168.N.192 /27	36	192.168.N.96 /27
11	192.168.N.64 /27	24	192.168.N.224 /27	37	192.168.N.128 /27
12	192.168.N.96 /27	25	192.168.N.0 /27	38	192.168.N.160 /27
13	192.168.N.128 /27	26	192.168.N.32 /27	39	192.168.N.192 /27

Додаток 2.

Контроль ресурсів (RAM/Swap/Disk) та розширення диску (Linux)

1. Перевірка оперативної пам'яті (RAM) та Swap
   1.1 Загальна інформація
   free -h
   Ключові поля: total — загальний обсяг RAM, used — зайнято, available — реально доступно, Swap total/used — стан файлу/розділу підкачки
   1.2 Детально по пам'яті
   cat /proc/meminfo | head -n 20
   1.3 Перевірка, чи є swap
   swapon --show
   1.4 Поточна "напруга" системи (Load Average + використання пам'яті)
   uptime
   top

2. Перевірка дискового простору
   2.1 Загальний стан файлових систем
   df -h
   Для кореневого розділу:
   df -h /
   2.2 Пошук, що "з'їдає" місце
   sudo du -xhd1 / | sort -h
   Детальніше по /var:
   sudo du -xhd1 /var | sort -h
   2.3 Найбільші каталоги/файли
   sudo du -ah /var | sort -rh | head -n 20
   2.4 Вільні inode (інколи проблема саме в них)
   df -ih

3. Створення файлу підкачки (Swap file). Рекомендовано, коли RAM не вистачає або важкі сервіси (OpenSearch/Wazuh Indexer) падають через нестачу пам'яті.
   3.1 Створення swap-файлу 4 GB
   sudo fallocate -l 4G /swapfile
   sudo chmod 600 /swapfile

```
sudo mkswap /swapfile
sudo swapon /swapfile
```

Перевірка:

```
swapon --show
free -h
```

3.2 Додати swapfile назавжди (persist)

```
echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
```

3.3 Оптимізація swappiness (щоб swap використовувався рідше)

```
sudo sysctl vm.swappiness=10
echo 'vm.swappiness=10' | sudo tee /etc/sysctl.d/99-swappiness.conf
```

4. Розширення дискових розділів (збільшення диску). Залежить від платформи.

```
lsblk
```

Детально:

```
sudo fdisk -l
```

Перевірити тип FS:

```
df -Th
```

5. Розширення розділу + файлової системи (найтиповіші випадки)

Випадок A: XFS (часто в Amazon Linux / RHEL)

Розширити розділ (наприклад /dev/sda1):

```
sudo growpart /dev/sda 1
```

Розширити файлову систему XFS:

```
sudo xfs_growfs /
```

Перевірка:

```
df -h /
```

Якщо growpart відсутній:

```
sudo dnf install -y cloud-utils-growpart
```

Випадок B: ext4

Розширити розділ:

```
sudo growpart /dev/sda 1
```

Розширити ext4:

```
sudo resize2fs /dev/sda1
```

Перевірка:

```
df -h /
```

Випадок C: LVM (логічні томи)

Перевірити:

```
lsblk
sudo pvs
sudo vgs
sudo lvs
```

Розширити фізичний том (якщо диск збільшили):

```
sudo pvresize /dev/sda2
```

Розширити логічний том (наприклад root):

```
sudo lvextend -l +100%FREE /dev/mapper/<VG>-<LV>
```

Розширити FS:

для XFS:

```
sudo xfs_growfs /
```

для ext4:

```
sudo resize2fs /dev/mapper/<VG>-<LV>
```

6. Під час роботи Wazuh (особливо Wazuh Indexer / OpenSearch) може виникнути ситуація, коли диск майже заповнений. У такому випадку Indexer автоматично переходить у “захисний режим”: він блокує запис у індекси, щоб уникнути повного падіння системи та пошкодження даних.

Це проявляється повідомленнями типу:

```
disk usage exceeded flood-stage watermark
```

індекси стають read-only-allow-delete (тобто тільки читання, запис заборонено)

Через це перестають створюватися/оновлюватися індекси Wazuh, не з'являються алерти в Dashboard а веб-інтерфейс може показувати помилки (наприклад Check alerts index pattern)

Порядок відновлення роботи

Крок 1. Звільнити місце або розширити диск

Потрібно забезпечити, щоб на розділі (зазвичай /) було достатньо вільного простору.

Наприклад видалити зайві журнали (logs) та очистити старі дані, або збільшити розмір диску ВМ (правильний варіант для лабораторних)

Крок 2. Зняти блокування "read-only" з індексів

Після того як місце звільнено, індекси можуть залишатися заблокованими. Тому потрібно вручну зняти обмеження запису командою:

```
curl -k -u admin:admin -X PUT "https://127.0.0.1:9200/_all/_settings" \
-H 'Content-Type: application/json' \
-d '{"index.blocks.read_only_allow_delete": false}'
```

Після виконання цієї команди Indexer знову дозволяє запис, і система повертається до нормальної роботи. Якщо диск не звільнити — блокування повернеться знову, бо це захисний механізм OpenSearch.

Корисні посилання

- Wazuh. Installation alternatives. Virtual machine (VM)

https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

- Step-by-step setup of Wazuh SIEM on Ubuntu 22.04.3 LTS.

https://medium.com/@akobeajiboluemmanuel/step-by-step-setup-of-wazuh-siem-on-ubuntu-22-04-3-lts-4663104fe69b

- Getting started with WazuhArchitecture

https://documentation.wazuh.com/current/getting-started/architecture.html

- VirtualBox & NAT network configuration tutorial

https://www.dedoimedo.com/computers/virtualbox-nat-networks.html

- NAT Port Forwarding in VirtualBox

https://superuser.com/questions/725318/nat-port-forwarding-in-virtualbox