Лабораторна робота №10

Підключення агентів до Wazuh Server.

Мета: Набути практичних навичок інсталяції та налаштування агентів Wazuh Agent на операційних системах Windows Server та Ubuntu Server, зареєструвати їх на раніше розгорнутому сервері Wazuh Server і перевірити коректність з'єднання. Ознайомитися з відображенням подій у Wazuh Dashboard та підготувати середовище для подальшого виконання лабораторних робіт з безпекового моніторингу системних логів та виявлення інцидентів.

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 буде розгорнуто Wazuh Agent для локального моніторингу ресурсів.

Serv-G-N-5 (Ubuntu Server 24.04) – сервер на якому буде встановлено Wazuh Agent для локального моніторингу ресурсів.

Serv-G-N-7 (Amazon Linux 2023) – сервер Wazuh Appliance, що містить компоненти Wazuh Server (Manager, API) та Elasticsearch + Kibana (Dashboard)

Мережеве середовище забезпечує взаємодію між вузлами з доменною інфраструктурою для подальшого моніторингу її елементів.

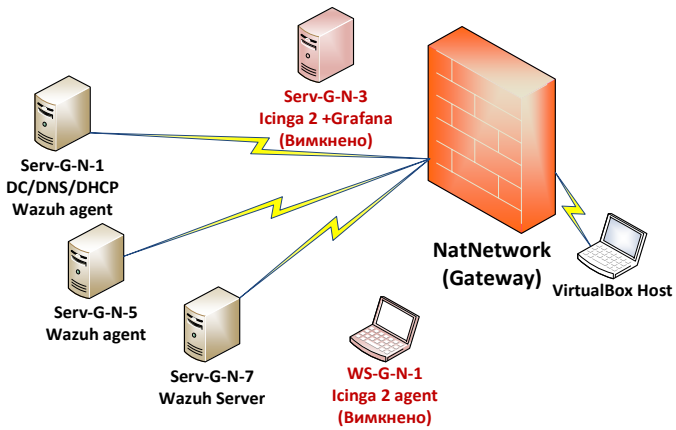

Рис. 10.1. Топологія мережі

Розгортання Wazuh Agent на Ubuntu Server 24.04

Для підключення Linux-вузла до системи безпекового моніторингу Wazuh використовується агент Wazuh Agent, який забезпечує збір подій із локальної системи та їх передачу на сервер Wazuh Manager. Входимо до Wazuh Dashboard під обліковим записом адміністратора та у головному меню обираємо пункт "Home – Overview – Deploy new agent". У формі розгортання вказуємо:

Select the package to download and install on your system: Linux (DEB amd64)

Server address: IP-адреса сервера Wazuh (192.168.50.9) та відмічаємо Remember server address

Optional settings: Assign an agent name: Вказуємо ім'я хосту на якому буде розгорнуто агент.

У цьому ж вікні (пункт 4 "Linux installation command") після заповнення попередніх полів автоматично генерується готовий набір команд для встановлення агента на цільовий хост Ubuntu.

Приклад команди для Ubuntu Server 24.04:

wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.14.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.50.9' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='serv-22-50-5' dpkg -i ./wazuh-agent_4.14.0-1_amd64.deb

Ця команда завантажує інсталяційний пакет агента, задає параметри підключення до сервера Wazuh (WAZUH_MANAGER, WAZUH_AGENT_GROUP, WAZUH_AGENT_NAME) та виконує інсталяцію пакета і автоматичну реєстрацію агента на сервері (рис.10.2).

Після успішного встановлення виконуємо послідовність команд із пункту 5 цього ж вікна для активації служби агента:

sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent

Після запуску служби перевіряємо її стан:

sudo systemctl status wazuh-agent

У результаті статус має бути active (running), що підтверджує успішне розгортання агента та його готовність до з'єднання з Wazuh Server.

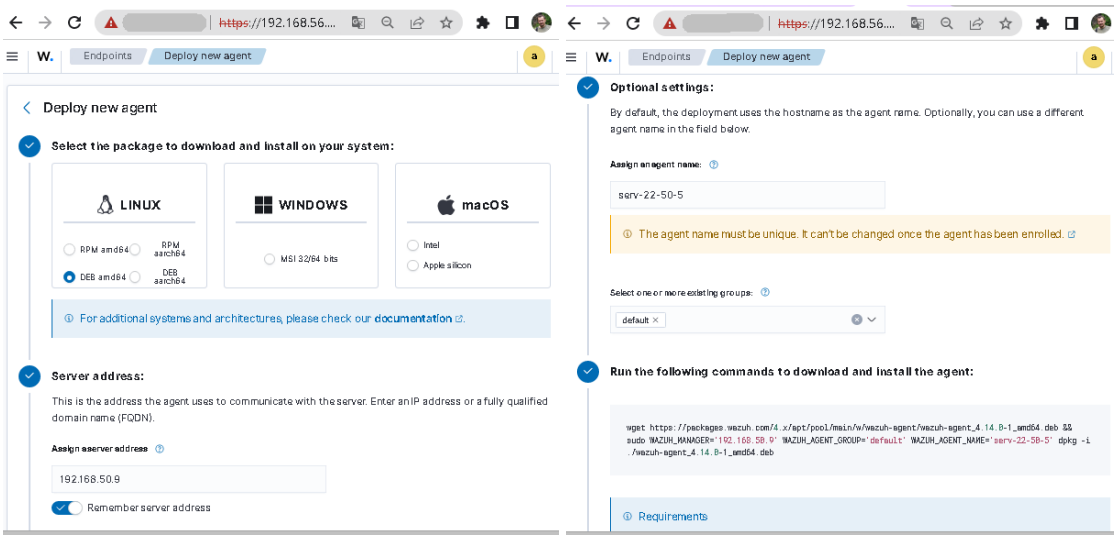

Рис. 10.2. Генерація набору команд для встановлення агента на цільовий хост Ubuntu

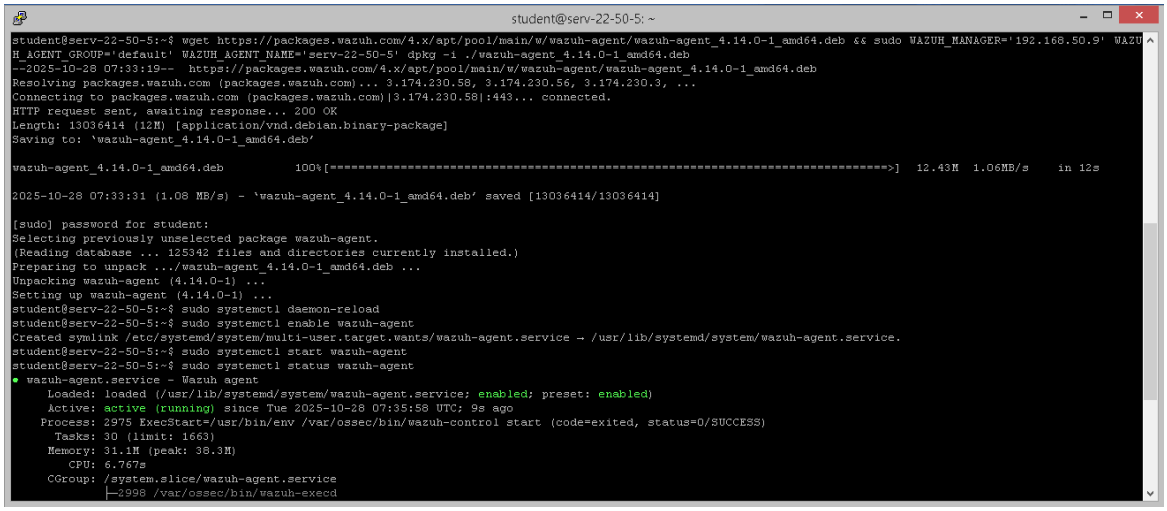

Рис. 10.3. Встановлення агента на цільовому хості Ubuntu

Повертаємося у Wazuh Dashboard, де новий агент має з'явитися у списку. Після короткої затримки (1–2 хвилини) його статус зміниться на Active, що свідчить про коректне з'єднання з Wazuh Manager. Надалі, «деплой» агентів виконується у пункті меню "Home – Agent Management – Summary – Deploy new agent"

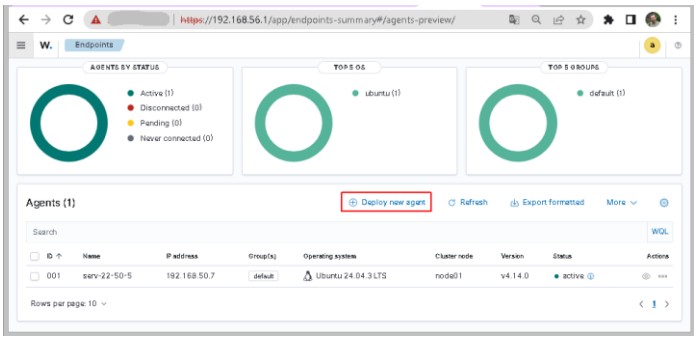

Рис. 10.4. Меню Home – Agent Management – Summary

Розгортання Wazuh Agent на Windows Server 2022

Для підключення Windows-вузла до системи безпекового моніторингу Wazuh також використовується агент Wazuh Agent, який забезпечує збір подій із локальної системи та їх передачу на сервер Wazuh Manager. Входимо до Wazuh Dashboard під обліковим записом адміністратора та у головному меню обираємо пункт Home – Agent Management – Summary – Deploy new agent (рис.10.4). У формі розгортання вказуємо:

Select the package to download and install on your system: Windows (MSI 32/64 bits)

Server address: IP-адреса сервера Wazuh (192.168.50.9) та залишаємо Remember server address

Optional settings: Assign an agent name: Вказуємо ім'я хосту на якому буде розгорнуто агент.

У цьому ж вікні (пункт 4 " Run the following commands to download and install the agent:") після заповнення попередніх полів автоматично генерується готовий набір команд для встановлення агента на цільовий хост Windows. Приклад команди Power Shell для завантаження та встановлення агента:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.0-1.msi -
OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q
WAZUH_MANAGER='192.168.50.9' WAZUH_AGENT_NAME='Serv-22-50-1'
```

Ця команда, аналогічно команді для Linux-хосту, завантажує інсталяційний пакет агенту, задає параметри підключення до сервера Wazuh (WAZUH_MANAGER, WAZUH_AGENT_GROUP, WAZUH_AGENT_NAME) та виконує інсталяцію пакета і автоматичну реєстрацію агента на сервері (рис.10.6).

Після успішного встановлення виконуємо команду NET START Wazuh. Повертаємося до веб-інтерфейсу Wazuh Dashboard. Новий агент має з'явитися у списку зареєстрованих вузлів зі статусом Active.

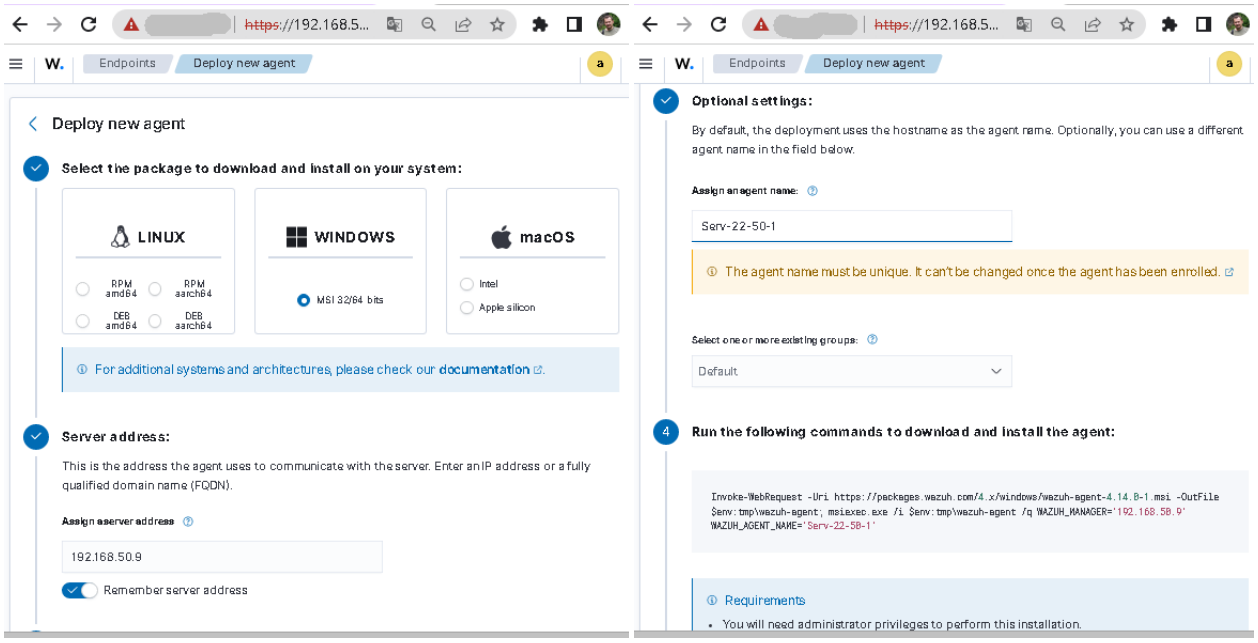

Рис. 10.5. Генерація набору команд для встановлення агента на цільовий хост Windows

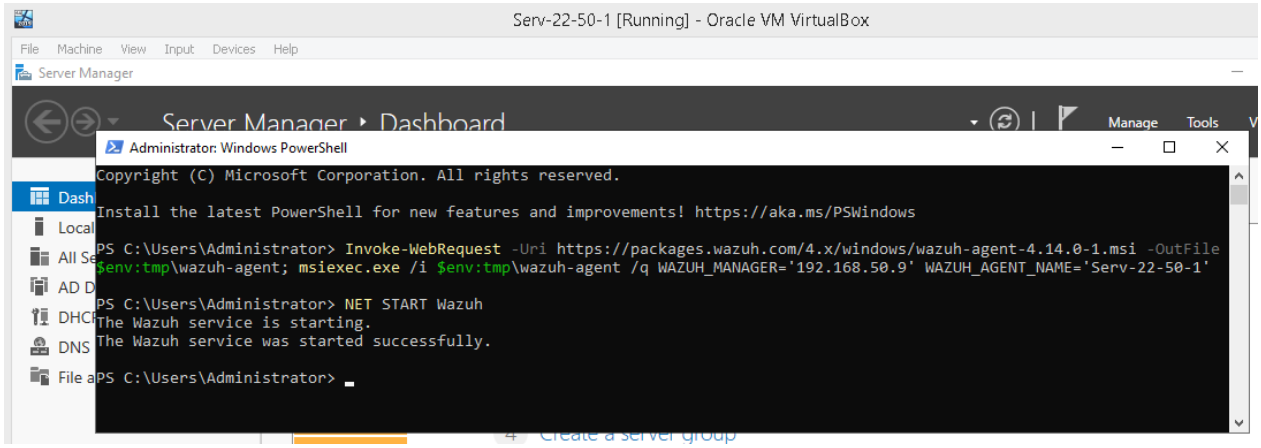

Рис. 10.6. Встановлення агента на цільовому хості Windows

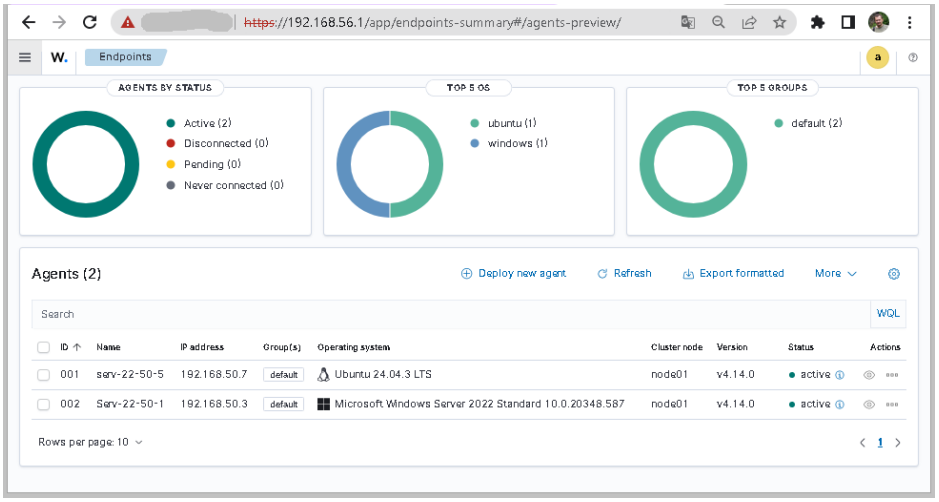

Рис. 10.7. Меню Home – Agent Management – Summary

Перевірка підключення агентів до Wazuh Server.

У розділі меню Wazuh Dashboard Home – Agent Management – Summary (рис.10.7) відображається список усіх агентів, зареєстрованих на сервері Wazuh. Для кожного встановленого агента (наприклад, Serv-G-N-1 та Serv-G-N-5) у стовпці Status має бути зазначено Active. Якщо агент перебуває у стані Disconnected або Never connected, варто перевірити налаштування мережі, IP-адресу сервера або параметри WAZUH_MANAGER.

Переглянути журнали агента на Linux можна командою:

sudo systemctl status wazuh-agent

sudo tail -f /var/ossec/logs/ossec.log

Те ж саме на Windows виконується через Event Viewer – Applications and Services Logs – Wazuh.

Для перевірки надходження подій рекомендується виконати певні системні дії на хостах. Наприклад, вхід користувача, запуск сервісів, перезавантаження хосту, тощо. Результатом цих дій має бути поява відповідних повідомлень у Home – Threat Intelligence – Threat Hunting. Це буде свідчити про успішну комунікацію між агентом і сервером Wazuh.

Завдання до лабораторної роботи

1. Перевірити доступність у мережі існуючого серверу Wazuh Appliance Serv-G-N-7.
2. Розгорнути агент Wazuh Agent на хості Ubuntu Server 24.04 (Serv-G-N-5) із використанням інструменту Deploy new agent у Wazuh Dashboard.
3. Встановити та налаштувати агент Wazuh Agent на Windows Server 2022 (Serv-G-N-1), виконавши інсталяцію через PowerShell-команду, згенеровану у Dashboard.
4. Перевірити підключення обох агентів до сервера Wazuh, переконатися у їхньому статусі Active та у надходженні подій до Wazuh Dashboard.
5. Розглянути аналітичну інформацію меню Threat Intelligence – Threat Hunting та Threat Intelligence – Vulnerability Detection для перевірки роботи системи безпекового моніторингу

Корисні посилання

- Wazuh. Installation alternatives. Virtual machine (VM)

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

- Installation guide / Wazuh agent

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html

- Getting started with Wazuh / Architecture

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

- Wazuh Agent Install —Endpoint Monitoring

https://socfortress.medium.com/part-4-wazuh-agent-install-endpoint-monitoring-f24f6a0464ac

- User manual / Wazuh dashboard

https://documentation.wazuh.com/current/user-manual/wazuh-dashboard/index.html