11. ?????????? ?????????? ????????? ?????

11.1 ?????????? ?? ???????????? ???????????? ???????????? ??????????

Оператор (або Суб'єкт електронної взаємодії, якщо він самостійно встановлює та адмініструє локальні компоненти) має можливість встановити та налаштувати сервер аналізу транзакцій, який може збирати та відображати відомості щодо кількості здійснених запитів, що пройшли через ШБО.

Також Оператор (або Суб'єкт електронної взаємодії, якщо він самостійно встановлює та адмініструє локальні компоненти) має можливість встановити та налаштувати сервер моніторингу за працездатністю власного ШБО, який може збирати та відображати відомості щодо використання апаратних ресурсів ШБО в процесі функціонування.

Мінімальні апаратні характеристики віртуальних машин (або фізичних серверів), необхідні для роботи компонентів локального моніторингу, наведено у таблиці 5.1.

З метою економії апаратних ресурсів можна встановлювати програмне забезпечення сервера аналізу транзакцій та сервера моніторингу за працездатністю на одній віртуальній машині. При цьому, необхідно враховувати, що об’єднане програмне забезпечення може використовувати більше оперативної пам’яті.

Сервер аналізу журналів подій та моніторингу за працездатністю функціонують на базі операційної системи Ubuntu Server 18.04.4 x64, процес інсталяції якої наведено в Інструкції з інсталяції операційної системи Ubuntu Server 18.04.4 x64.

Також на дані віртуальні машини рекомендовано встановити антивірусне програмне забезпечення (наприклад, Falcon).

11.2 ?????????? ?? ?????????? ??????? ??????? ??????????

Сервер аналізу транзакцій складається з наступних програмних компонентів:

- Elasticsearch, що збирає та накопичує відомості про здійснені транзакції;

- Kibana, що виконує функції інтерфейсу користувача та відображає накопичені відомості за критеріями пошуку користувача.

Схема мережевої взаємодії сервера аналізу транзакцій наведена на рисунку 11.1.

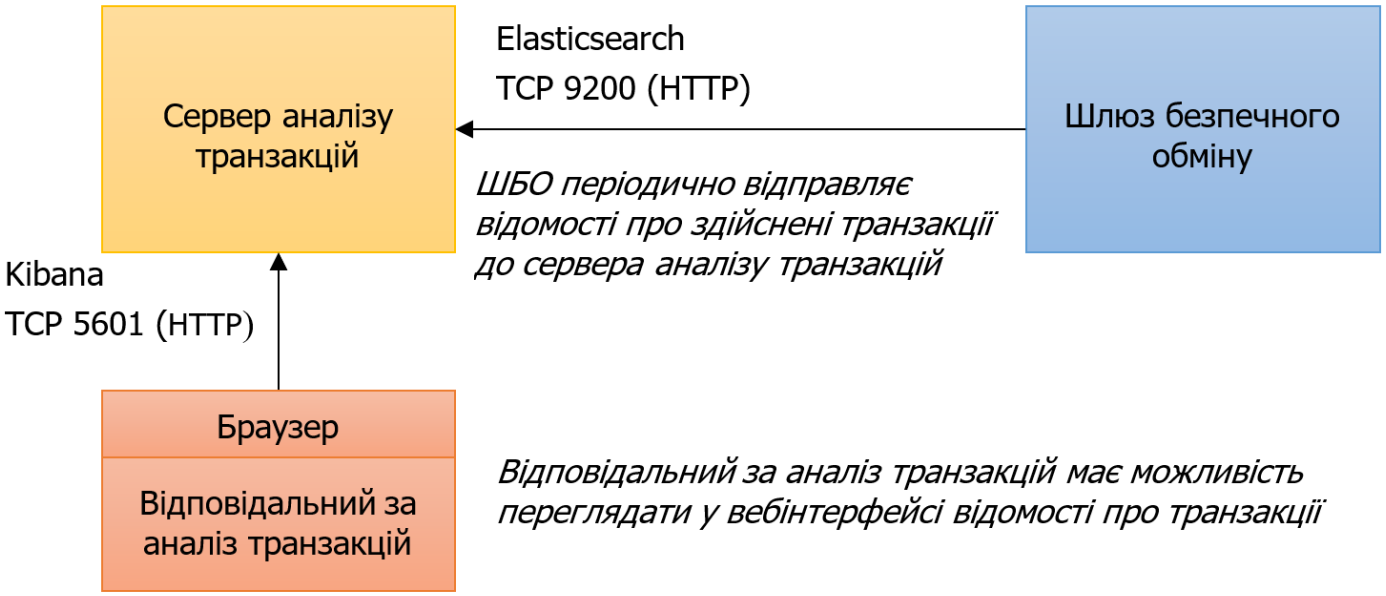


Рисунок 11.1 – Схема мережевої взаємодії сервера аналізу транзакцій

З метою організації мережевої взаємодії Оператор (або Суб'єкт електронної взаємодії, якщо він самостійно встановлює та адмініструє локальні компоненти) має забезпечити можливість мережевого з’єднання ШБО з сервером аналізу транзакцій на порт TCP 9200 (у тому числі, налаштувати вбудований міжмережевий екран на шлюзі безпечного обміну, якщо він був увімкнений).

Також Адміністратор локальних компонентів (системний адміністратор) повинен мати можливість підключатися до серверу аналізу транзакцій на порт TCP 5601, на якому розміщена служба вебінтерфейсу аналізу транзакцій.

Під час встановлення, сервер аналізу транзакцій повинен мати підключення до мережі Інтернет з метою встановлення програмних пакетів з програмного репозиторію системи «Трембіта».

Встановлення та всі відповідні налаштування виконуються Адміністратором локальних компонентів. Кінцевим користувачем, що працюватиме з сервером аналізу транзакцій через вебінтерфейс є користувач з роллю "Відповідальний за аналіз транзакцій".

11.2.1. ?????????? ??????? ??????? ??????????

Інсталяційні пакети Elasticsearch і Kibana входять в комплект компоненту uxp-monitor-analytics.

Щоб встановити uxp-monitor-analytics потрібно виконати наступні дії на сервері аналізу транзакцій:

1. Закрити доступ до сторонніх репозиторіїв за допомогою виконання наступної команди:

```
sudo sed -i 's/^[A-Za-z0-9]/#&/' /etc/apt/sources.list
```

2. Додати у операційну систему репозиторій з пакетами системи «Трембіта» за допомогою виконання наступної команди:

```
echo 'deb https://project-repo.trembita.gov.ua:8081/repository/trembita-member_archive/
certified main' | sudo tee -a /etc/apt/sources.list
```

Перевірити результат виконання команд можна за допомогою текстового редактора nano, відкривши файл на редагування, за допомогою виконання наступної команди:

```
sudo nano /etc/apt/sources.list
```

3. Додати GPG ключ репозиторію за допомогою виконання наступної команди:

```
sudo wget -O - https://project-repo.trembita.gov.ua:8081//public-keys/public.key.txt | sudo
apt-key add -
```

Якщо команду виконано успішно, буде виведено повідомлення «OK».

4. Провести системне очищення та оновити списки доступних пакетів за допомогою послідовного виконання наступних команд:

```
sudo apt autoremove && sudo apt clean && sudo apt autoclean
sudo apt update
```

5. Встановити пакет uxp-monitor-analytics на сервері аналізу транзакцій за допомогою виконання наступної команди:

```
sudo apt install -y uxp-monitor-analytics
```

6. Додати Elasticsearch і Kibana до автозапуску після встановлення за допомогою послідовного виконання наступних команд:

```
sudo systemctl enable kibana
sudo systemctl enable elasticsearch
```

7. Вперше служби потрібно запустити вручну за допомогою послідовного виконання наступних команд:

```
sudo service kibana start
sudo service elasticsearch start
```

11.2.2. ???????????? Elasticsearch ? Kibana

Перед початком роботи служби Elasticsearch і Kibana повинні бути налаштовані Адміністратором локальних компонентів наступним чином:

1. Відкрити на редагування файл /etc/elasticsearch/elasticsearch.yml на сервері аналізу транзакцій зі встановленим програмним забезпеченням пакету uxp-monitor-analytics за допомогою виконання наступної команди:

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

2. Перевірити наявність наступних рядків в даному файлі:

```
cluster.name: uxp
node.name: ${HOSTNAME}
network.host: 0.0.0.0
cluster.initial_master_nodes: ["${HOSTNAME}"]
search.max_buckets: 20000
```

3. Закрити редактор, натиснувши комбінацію клавіш «Ctrl+X», далі буде відображено повідомлення про підтвердження на збереження змін – необхідно натиснути «Y», а потім «Enter» для збереження.

4. Відкрити на редагування файл /etc/kibana/kibana.yml за допомогою виконання наступної команди:

```
sudo nano /etc/kibana/kibana.yml
```

5. Замінити наступний рядок:

```
#server.host: «localhost»
```

на:

```
server.host: 0.0.0.0
```

6. Закрити редактор, натиснувши комбінацію клавіш «Ctrl+X», далі буде відображено повідомлення про підтвердження на збереження змін – необхідно натиснути «Y», а потім «Enter» для збереження.

7. Перезавантажити служби elasticsearch та kibana шляхом послідовного виконання наступних команд:

```
sudo service elasticsearch restart
sudo service kibana restart
```

Для перевірки працездатності компоненту Адміністратору локальних компонентів необхідно перейти до вебінтерфейсу серверу аналізу транзакцій за посиланням: http://<YOUR-EK-SERVER-IP>:5601/,

де **<YOUR-EK-SERVER-IP>** – адреса відповідного сервера, на якому встановлено ПЗ серверу аналізу транзакцій.

11.2.3. ???????????? ???????????? ????? ?????????? ?????? ?? ??????? ??????? ??????????

Конфігурація підключення шлюзу безпечного обміну до серверу аналізу транзакцій налаштовується на ШБО у файлі /etc/uxp/monitor-agent.ini.

Для налаштування підключення Адміністратору локальних компонентів (системному адміністраторові) необхідно виконати наступні дії на ШБО:

1. Відкрити на редагування файл /etc/uxp/monitor-agent.ini за допомогою виконання наступної команди:

```
sudo nano /etc/uxp/monitor-agent.ini
```

2. Розкоментувати наступні рядки (видаливши символ «#» на початку рядку) і встановити наступні параметри:

```
[elasticsearch]
address = <YOUR-EK-SERVER-IP>
```

```
port = 9200
cluster_name = uxp
index = uxp
```

де **<YOUR-EK-SERVER-IP>** – адреса відповідного сервера, на якому встановлено програмне забезпечення серверу аналізу транзакцій.

3. Закрити редактор, натиснувши набір клавіш «Ctrl+X», після чого буде відображено повідомлення-підтвердження збереження змін – необхідно натиснути «Y», а потім «Enter» для збереження відомостей.

Для застосування нової конфігурації Elasticsearch на ШБО потрібно виконати наступну команду:

```
sudo reload-monitor-agent
```

11.2.4. ???????????? ???????????? ?????????? ?? ??????? ??????? ??????????

11.2.4.1. ???????????? ??????? ???????

Налаштування шаблону індексу на сервері аналізу транзакцій здійснюється Відповідальним за аналіз транзакцій.

Примітка. Індекс в Elasticsearch з'явиться не одразу, а тільки після початку обміну повідомленнями між ШБО Учасника та іншими ШБО. Про це необхідно пам’ятати під час налаштувань.

Для налаштування шаблону Відповідальному за аналіз транзакцій необхідно виконати наступні дії в вебінтерфейсі серверу аналізу транзакцій, відкривши його за посиланням: http://<YOUR-EK-SERVER-IP>:5601/:

1. Перейти в розділ «Management –> Index Patterns»;

2. В полі «Index pattern» ввести: uxp*;

В полі «Time Filter field» name має з’явитися значення: monitoring_data_ts;

3. Натиснути на кнопку «Create».

Примітка. Якщо після введення «uxp*» з’являється повідомлення «Unable to fetch mapping. Do you have indices matching the pattern» – це означає, що до сервера аналізу транзакцій від ШБО ще не надходило відомостей про виклики сервісів. Потрібно здійснити обмін інформацією через ШБО, після чого він має надіслати статистику здійснених транзакцій.

Індикатором успішного створення індексу може бути повідомлення, що містить поле «Creating index (uxp) for Elasticsearch» у файлі журналу /var/log/uxp/proxymonitoragent.log на ШБО.

Після цього необхідно повторити процедуру створення індексу на сервері аналізу транзакцій. Статистика відправляється з ШБО не одразу, а через певні інтервали часу.

Подивитись останні отримані відомості у простому форматі можна на вкладці «Discover» інструменту Kibana.

11.2.4.2. ???????????? ????????????

Пакет uxp-monitor-analytics містить деякі приклади візуалізації транзакцій. Ці приклади знаходяться в директорії /usr/share/doc/uxp-monitor-analytics/examples/kibana-7.x/operational-data, а саме:

- request-total-by-security-server.json – візуалізує загальну кількість запитів, здійснених ШБО;

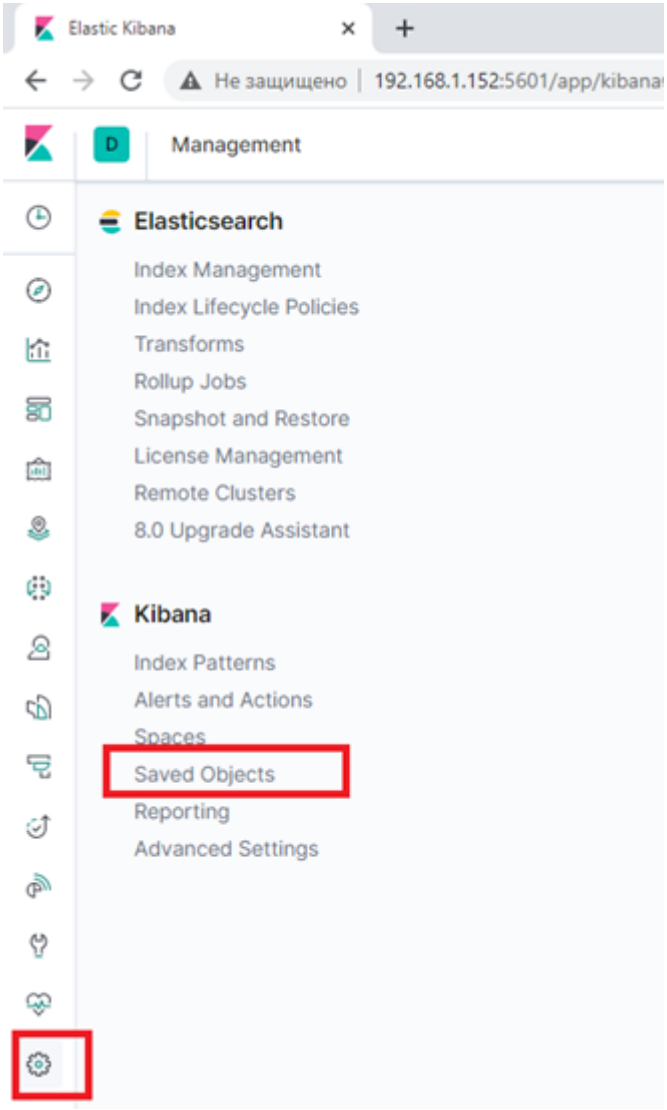
- request-total-by-security-server-by-service.json – візуалізує загальну кількість запитів, здійснених через певний ШБО і певний сервіс;

- succeeded-requests-by-service.json – візуалізує кількість вдалих запитів до сервісу.

Для налаштування візуалізації необхідно виконати наступні дії в вебінтерфейсі серверу аналізу транзакцій:

1. Скопіювати зазначені вище файли із сервера аналізу транзакцій в зручну директорію на робочій станції Відповідальної особи за аналіз транзакцій, використовуючи WinSCP або іншу програму .

2. Зайти в розділ «Management –> Saved Objects» вебінтерфейсу Kibana:



3. Натиснути на кнопку «Import», щоб імпортувати файли в Kibana.

4. Обрати збережений на диску потрібний файл. У діалоговому вікні натиснути на кнопку «Yes, overwrite all», а в наступному вікні - «Confirm all changes». Імпортований файл повинен з'явитися на вкладці «Visualizations».

11.2.4.3. ????????? ????????????

Для перевірки візуалізації на сервері аналізу транзакцій необхідно зробити наступні дії:

1. Відкрити вебінтерфейс серверу аналізу транзакцій за посиланням: http://<YOUR-EK-SERVER-IP>:5601/.

2. Перейти в розділ «Visualize», де буде відображено імпортовані приклади візуалізації статистики.

3. Для того, щоб відобразити статистику за сервісами, необхідно натиснути на кнопку «Requests Good by Service».

Якщо дані статистики не відображаються, необхідно налаштувати інтервал для відображення. Для цього необхідно виконати наступні дії в вебінтерфейсі серверу аналізу

транзакцій:

- вказати потрібний Time Range, натиснувши на кнопку в правому верхньому кутку сторінки; обрати опцію «Today». Повинна відобразитися статистика за запитами.

11.3 ?????????? ?? ?????????? ??????? ?????????? ?? ??????????

Основною частиною сервера моніторингу за працездатністю є програмне забезпечення Zabbix, яке може накопичувати та візуалізувати інформацію про використання апаратних ресурсів серверів, у тому числі, середнє навантаження на процесор, об’єм використаної оперативної пам’яті, об’єм вільного дискового простору тощо.

Схема мережевої взаємодії сервера моніторингу за працездатністю наведена на рисунку 11.2.

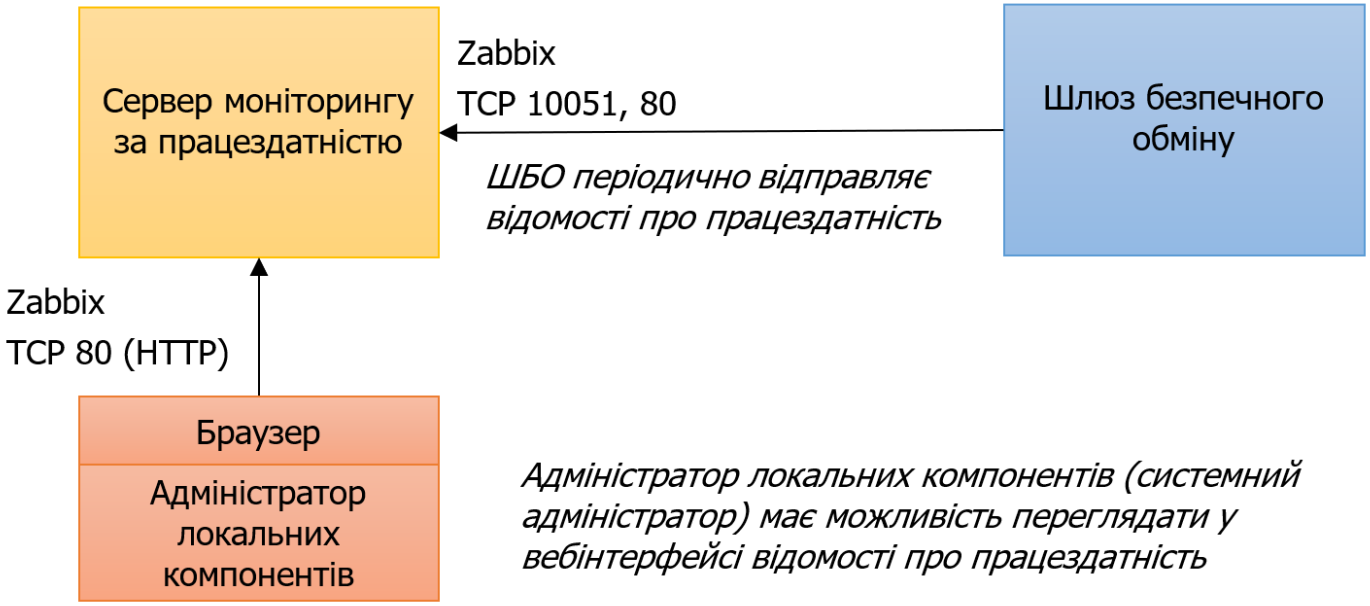


Рисунок 11.2 – Схема мережевої взаємодії сервера моніторингу за працездатністю

З метою організації мережевої взаємодії Оператор (або Суб’єкт електронної взаємодії, якщо він самостійно адмініструє власні локальні компоненти системи «Трембіта») має забезпечити можливість мережевого з’єднання із ШБО до сервера моніторингу за працездатністю на порти TCP 10051 та TCP 80.

Встановлення та всі відповідні налаштування виконуються Адміністратором локальних компонентів.

Адміністратор локальних компонентів (системний адміністратор) повинен мати можливість підключатися до Сервера моніторингу за працездатністю на порт TCP 80, на якому розміщена служба вебінтерфейсу сервера.

Під час інсталяції Адміністратор локальних компонентів (системний адміністратор) має забезпечити Сервер моніторингу за працездатністю виходом до мережі Інтернет з метою встановлення програмних пакетів з програмного репозиторію системи «Трембіта».

11.3.1. ???????????? ??????? ??????????? ?? ?????????????

Для встановлення необхідних пакетів для сервера моніторингу за працездатністю необхідно виконати наступні дії:

1. Закрити доступ до сторонніх репозиторіїв за допомогою виконання наступної команди:

```
sudo sed -i 's/^[A-Za-z0-9]/#&/' /etc/apt/sources.list
```

2. Додати у операційну систему репозиторій з пакетами системи «Трембіта» за допомогою виконання наступної команди:

```
echo 'deb https://project-repo.trembita.gov.ua:8081/repository/trembita-monitoring_archive/
graylog main' | sudo tee -a /etc/apt/sources.list
```

Перевірити результат виконання команд можна за допомогою текстового редактора nano, відкривши файл на редагування за допомогою виконання наступної команди:

```
sudo nano /etc/apt/sources.list
```

3. Додати GPG ключ репозиторію за допомогою виконання наступної команди:

```
sudo wget -O - https://project-repo.trembita.gov.ua:8081//public-keys/public.key.txt | sudo
apt-key add -
```

Якщо команду виконано успішно, буде виведено повідомлення «OK».

4. В операційній системі має бути встановлена локаль UTF-8.

> **Примітка.** Встановлення локалі описано в розділі 7.1.4.

5. Провести системне очищення та оновити списки доступних пакетів за допомогою послідовного виконання наступних команд:

```
sudo apt autoremove && sudo apt clean && sudo apt autoclean
sudo apt update
```

6. Встановити необхідні засоби за допомогою виконання наступної команди:

```
sudo apt install zabbix-server-pgsql zabbix-agent postgresql -y
```

7. Створити користувача бази даних та базу даних за допомогою послідовного виконання наступних команд:

```
sudo -u postgres createuser --pwprompt zabbix
sudo -u postgres createdb -O zabbix zabbix
```

8. Імпортувати схему бази даних за допомогою виконання наступної команди:

```
zcat /usr/share/doc/zabbix-server-pgsql/create.sql.gz | sudo -u zabbix psql zabbix
```

9. Відкрити на редагування файл конфігурації zabbix_server.conf за допомогою виконання наступної команди:

```
sudo nano /etc/zabbix/zabbix_server.conf
```

10. Ввести пароль до файлу конфігурації як значення параметру «DBPassword», а значення параметру «DBHost» – залишити порожнім:

```
DBHost=
DBPassword=
```

11. Увімкнути Zabbix сервер за допомогою послідовного виконання наступних команд:

```
sudo systemctl enable zabbix-server
sudo systemctl start zabbix-server
```

12. Встановити web частину серверу Zabbix за допомогою виконання наступної команди:

```
sudo apt install zabbix-frontend-php php-pgsql -y
```

13. Вимкнути Apache2 за допомогою послідовного виконання наступних команд:

```
sudo systemctl stop apache2
sudo systemctl disable apache2
```

14. Встановити Nginx за допомогою послідовного виконання наступних команд:

```
sudo apt install nginx-light php-fpm -y
sudo ln -s /usr/share/zabbix /var/www/html/zabbix
sudo rm /etc/nginx/sites-enabled/default
```

15. Відкрити на редагування файл конфігурації php.ini за допомогою виконання наступної команди:

```
sudo nano /etc/php/7.2/fpm/php.ini
```

16. Перевірити наявність перелічених нижче параметрів у файлі конфігурації. Якщо дані параметри відсутні – встановити їх наступним чином:

```
date.timezone = Europe/Kiev
post_max_size = 16M
max_execution_time = 300
max_input_time = 300
```

17. Створити та відкрити на редагування файл конфігурації Nginx за допомогою послідовного виконання наступних команд:

```
sudo touch /etc/nginx/sites-available/zabbix
sudo ln -s /etc/nginx/sites-available/zabbix /etc/nginx/sites-enabled/zabbix
sudo nano /etc/nginx/sites-enabled/zabbix
```

18. Внести наступні конфігураційні параметри у даний файл:

```
server {
    listen 80 default_server;
    root /var/www/html;
    index index.php index.html index.htm;
    server_name zabbix_server;
    location / {
        try_files $uri $uri/ =404;
    }
    location /(conf|app|include|local) {
        deny all;
    }
    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.2-fpm.sock;
    }
    location ~ /\.ht {
```

```
        deny all;
    }
}
```

19. Перезавантажити сервіси за допомогою виконання наступної команди:

```
sudo systemctl restart php7.2-fpm nginx
```

11.3.2. ???????????? ??????? ???????????? ?? ??????????????

Вебінтерфейс серверу моніторингу за працездатністю доступний за посиланням: http://<YOUR-ZABBIX-SERVER-IP>/zabbix/,

де **<YOUR-ZABBIX-SERVER-IP>** – адреса відповідного серверу, на якому встановлено програмне забезпечення для моніторингу за працездатністю.

Для налаштування серверу моніторингу за працездатністю Адміністратору локальних компонентів (системному адміністратору) необхідно виконати наступні дії в його вебінтерфейсі:

1. Заповнити дані, що будуть запитані в процесі налаштування у відповідності до попередніх пунктів інсталяції:

- на кроці «Configure DB connection необхідно вказати пароль, що був створений у п. 10 розділу 11.3.1 даної інструкції;

- на всіх інших кроках натиснути на кнопку «Next/Finish».

Примітка. За замовчуванням логін для входу – «Admin» ([ZABBIX-ADMIN-USER]), пароль – «zabbix» ([ZABBIX-ADMIN-PASSWORD]).

2. Запустити агент моніторингу та додати його до автозапуску за допомогою послідовного виконання наступних команд:

```
sudo systemctl start zabbix-agent
sudo systemctl enable zabbix-agent
```

11.3.3. *???????????? ???????????? ????? ?????????? ?????? ?? ??????? ???????????? ?? ??????????????*

Конфігурація підключення ШБО до серверу моніторингу за працездатністю налаштовується на ШБО у файлі /etc/uxp/monitor-agent.ini.

Для налаштування підключення ШБО до сервера моніторингу за працездатністю Адміністраторові локальних компонентів (системному адміністратору) необхідно виконати наступні дії на ШБО:

1. Відкрити на редагування файл monitor-agent.ini за допомогою виконання наступної команди:

```
sudo nano /etc/uxp/monitor-agent.ini
```

2. Розкоментувати наступні рядки (видаливши символ «#» на початку рядку):

```
[zabbix-1]
address = <YOUR-ZABBIX-SERVER-IP>
port = 10051
enable_configurator = true
username = <ZABBIX-ADMIN-USER>
password = <ZABBIX-ADMIN-PASSWORD>
host_group = uxp-pma
```

де **<YOUR-ZABBIX-SERVER-IP>** – адреса відповідного серверу, на якому встановлено програмне забезпечення для моніторингу за працездатністю,

<ZABBIX-ADMIN-USER> – логін для входу на сервер моніторингу за працездатністю,

<ZABBIX-ADMIN-PASSWORD> – пароль для входу на сервер моніторингу за працездатністю;

> **Примітка.** За замовчуванням логін для входу – «Admin» (<ZABBIX-ADMIN-USER>), пароль – «zabbix» (<ZABBIX-ADMIN-PASSWORD>).

3. Закрити редактор, натиснувши комбінацію клавіш «Ctrl+X», буде відображено повідомлення про підтвердження на збереження змін – необхідно натиснути «Y», а потім «Enter» для збереження.

4. Застосувати нову конфігурацію Zabbix за допомогою виконання наступної команди:

```
sudo reload-monitor-agent
```

5. Підключитися до вебінтерфейсу Zabbix http://<YOUR-ZABBIX-SERVER-IP>/zabbix/,

де **<YOUR-ZABBIX-SERVER-IP>** – адреса відповідного серверу, на якому встановлено ПЗ для моніторингу за працездатністю.

6. Перевірити, що в конфігурації з'явилися хости шлюзу безпечного обміну.

Для цього необхідно виконати наступні дії:

1. Перейти на вкладку «Latest data».

2. Обрати «uxp-pma» у полі «Host groups».

3. Натиснути на кнопку «Apply».

Спочатку з’являться найменування статистичних полів, через деякий час вони заповняться даними зі шлюзу безпечного обміну.

> **Примітка.** Деталі використання інструменту Zabbix наведено на офіційному вебсайті Zabbix.