9. ?????????? ?? ?????????? ?????? ?????????? ??????????

Засіб перевірки повідомлень призначений для перевірки тих повідомлень, які зберігаються у журналі повідомлень шлюзу безпечного обміну. Встановлення цього компоненту не є обов’язковим.

Засіб перевірки повідомлень надає вебінтерфейс Відповідальному за аналіз транзакцій, який дозволяє переглядати наявні збережені та підписані повідомлення (запити до сервісів та відповіді), фільтрувати їх за параметрами (у тому числі за датою отримання, ID повідомлення, кодом сервісу, кодом підсистеми-клієнта тощо). Вебінтерфейс засобу перевірки повідомлень доступний через порт TCP 5000.

- 9.1 Встановлення засобу перевірки повідомлень
- 9.2 Налаштування засобу перевірки повідомлень

9.1 ?????????? ?????? ????????? ??????????

Засіб перевірки повідомлень встановлюється на відповідному сервері баз даних та архівування, який попередньо має бути встановлений та налаштований згідно розділу 8 даної інструкції. Встановлення та налаштування засобу перевірки повідомлень виконується Адміністратором локальних компонентів (системним адміністратором).

> **Примітка.** У випадку нестачі апаратних ресурсів засіб перевірки повідомлень можна встановити на окремій віртуальній машині (фізичному сервері). В такому випадку необхідно налаштувати віддалене підключення згідно розділу 9.2.1 даної інструкції

Для інсталяції засобу перевірки повідомлень необхідно виконати наступні дії:

1. **Якщо засіб перевірки повідомлень буде встановлено на окремій віртуальній машині** – необхідно закрити доступ до сторонніх репозиторіїв за допомогою виконання наступної команди:

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

2. **Якщо засіб перевірки повідомлень буде встановлено на окремій віртуальній машині** – додати репозиторій з пакетами системи «Трембіта»:

```
echo 'deb https://project-repo.trembita.gov.ua:8081/repository/ss-1.12.6/ bionic 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. **Якщо засіб перевірки повідомлень буде встановлено на окремій віртуальній машині** – необхідно 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, то буде виведено повідомлення «OK».

4. Створити новий обліковий запис Відповідального за аналіз транзакцій, який буде використовуватись для входу в вебінтерфейс засобу перевірки повідомлень шляхом послідовного виконання наступних команд:

```
sudo useradd -M -N <username>
sudo chsh -s /bin/false <username>
sudo passwd <username>
```

де **<username>** – логін створюваного користувача латиницею.

Після виконання цих команд необхідно ввести пароль нового користувача двічі.

5. Встановити програмне забезпечення UXP Verifier для засобу перевірки повідомлень шляхом послідовного виконання наступних команд:

```
sudo apt update
sudo apt install -y uxp-transaction-analysis-ua
```

6. Під час встановлення ввести ім’я облікового запису (логін) Відповідального за аналіз транзакцій, що буде мати доступ до інтерфейсу перегляду повідомлень та пароль для даного користувача:

Для перевірки стану виконання встановлених компонентів ПЗ UXP Verifier необхідно виконати наступну команду:

```
sudo systemctl list-units | grep "uxp"
```

Список сервісів, які мають бути активними (active/running):

```
uxp-confclient.service
uxp-verifier.service
```

9.2 ?????????? ?????? ????????? ???????????

Для налаштування засобу перевірки повідомлень необхідно знати наступну інформацію:

- місцезнаходження журналу повідомлень шлюзу безпечного обміну;

- ім’я хоста сервера PostgreSQL, що містить базу даних журналу повідомлень ШБО (зазвичай для промислового середовища це IP-адреса сервера баз даних та архівування);

- ім’я користувача облікового запису бази даних, що має дозвіл на віддалений доступ на сервер PostgreSQL;

- пароль до цього облікового запису;

- якір глобальної конфігурації ШБО, якому належить база даних журналу повідомлень.

> **Примітка.** Атрибути доступу до бази даних можна подивитися в файлі /etc/uxp/db.properties на відповідному ШБО у блоці uac-messagelog.hibernate.connection.

9.2.1 ???????????? ??????? ?? ????????? ??????????? ?? ??????? ???????????

> **Важливо!** Налаштування дозволу на віддалене підключення до журналу повідомлень необхідно здійснювати лише в тому випадку, якщо засіб перевірки повідомлень встановлений на окремому сервері, а не на тому, де розміщується база даних журналу повідомлень.

Для налаштування дозволу на віддалене підключення до журналу повідомлень потрібно виконати наступні кроки на сервері, де розміщується база даних журналів повідомлень:

1. Відкрити на редагування файл /etc/postgresql/10/main/postgresql.conf за допомогою наступної команди:

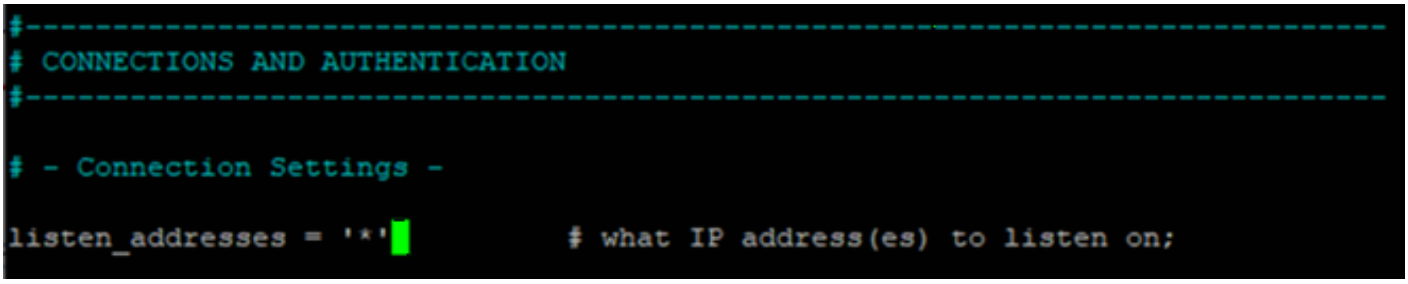
```
sudo nano /etc/postgresql/10/main/postgresql.conf
```

2. Знайти у файлі рядок з параметром «listen_addresses», розкоментувати його (видалити символ «#» на початку рядка) та замінити значення:

```
#listen_addresses = 'localhost'      # what IP address(es) to listen on;
```

на:

```
listen_addresses = '*'          # what IP address(es) to listen on;
```



3. Відкрити на редагування файл /etc/postgresql/10/main/pg_hba.conf, який містить налаштування прав доступу, за допомогою команди:

```
sudo nano /etc/postgresql/10/main/pg_hba.conf
```

4. Додати у кінець відкритого файлу наступний рядок

```
host <messagelog_dbname> <messagelog_dbuser> <verifier_ip>/32 md5
```

де **<messagelog_dbname>** – ім’я бази даних журналу повідомлень;

<messagelog_dbuser> – ім’я користувача облікового запису бази даних, що має дозвіл на віддалений доступ на сервер;

<verifier_ip> – IP-адреса сервера засобу перевірки повідомлень.

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

6. Перезавантажити PostgreSQL, щоб застосувати зміни за допомогою наступної команди:

```
systemctl restart postgresql
```

9.2.2 ???????????? ?????????? ???? ?????

База даних журналу повідомлень може знаходитись поза межами серверу, де встановлено засіб перевірки повідомлень чи шлюзу безпечного обміну, наприклад, у випадку, якщо засіб перевірки повідомлень встановлюється окремо, а не на сервері баз даних та архівування.

> **Примітка.** Передумова для налаштувань - передбачається, що база даних була створена, заповнена схемою журналу повідомлень, а доступ до бази даних із засобу перевірки повідомлень був налаштований.

Перед проведенням налаштувань потрібно перевірити підключення від засобу перевірки повідомлень до віддаленої бази даних за допомогою наступної команди:

```
psql -h <db_host> -U <messagelog_user> <messagelog_dbname>
```

де **<db_host>** – ім’я хоста серверу PostgreSQL, що розміщує базу даних журналу повідомлень;

<messagelog_dbname> – ім’я бази даних журналу повідомлень;

<messagelog_user> – логін користувача облікового запису бази даних, що має дозвіл на віддалений доступ на сервер.

В разі успішної перевірки буде відображено наступний результат:

```
serverconf.hibernate.jdbc.use_streams_for_binary = true
serverconf.hibernate.dialect = ee.ria.xroad.common.db.CustomPostgreSQLDialect
serverconf.hibernate.connection.driver_class = org.postgresql.Driver
serverconf.hibernate.connection.url = jdbc:postgresql://127.0.0.1:5432/servercon
f
serverconf.hibernate.connection.username = serverconf
serverconf.hibernate.connection.password = serverconf
uac-messagelog.hibernate.jdbc.use_streams_for_binary = true
uac-messagelog.hibernate.dialect = ee.ria.xroad.common.db.CustomPostgreSQLDialec
t
uac-messagelog.hibernate.connection.driver_class = org.postgresql.Driver
uac-messagelog.hibernate.connection.url = jdbc:postgresql://192.168.1.113:5432/m
sglog_db?ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory&
uac-messagelog.hibernate.connection.username = msglog_user
uac-messagelog.hibernate.connection.password = msglog_userp
```

Для налаштування необхідно:

1. Зупинити службу "uxp-verifier" за допомогою виконання наступної команди:

```
sudo systemctl stop uxp-verifier
```

```
secadmin@den-uxp-ta-182:~$  systemctl stop uxp-verifier
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to stop 'uxp-verifier.service'.
Authenticating as: secadmin
Password:
==== AUTHENTICATION COMPLETE ===
```

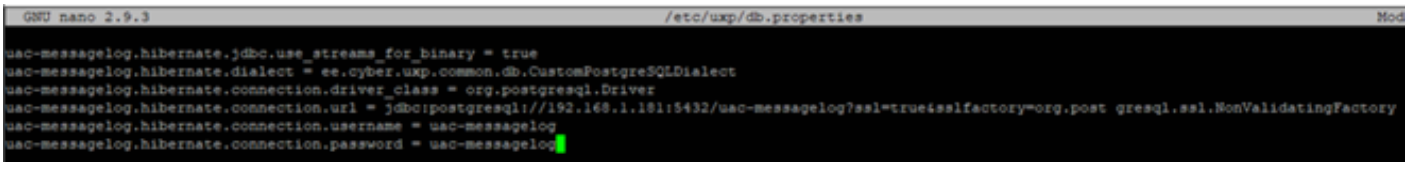
2. Відкрити на редагування файл /etc/uxp/db.properties за допомогою наступної команди:

```
sudo nano /etc/uxp/db.properties
```

- **Якщо засіб перевірки повідомлень та база даних журналу повідомлень знаходяться на різних хостах**, налаштування параметрів бази даних виглядатиме наступним чином:

```
uac-messagelog.hibernate.jdbc.use_streams_for_binary = true
uac-messagelog.hibernate.dialect = ee.cyber.uxp.common.db.CustomPostgreSQLDialect
uac-messagelog.hibernate.connection.driver_class = org.postgresql.Driver
uac-messagelog.hibernate.connection.url =
jdbc:postgresql://<db_host>:5432/<messagelog_dbname>?ssl=true&sslfactory=org.postgresql.ssl.No
nValidatingFactory
uac-messagelog.hibernate.connection.username = <messagelog_user>
uac-messagelog.hibernate.connection.password = <messagelog_password>
```

де **<db_host>** – ім’я хоста серверу PostgreSQL, де розміщено базу даних журналу повідомлень;
<messagelog_dbname> – ім’я бази даних журналу повідомлень;
<messagelog_user> – логін облікового запису бази даних, що має дозвіл на віддалений доступ на сервер;
<messagelog_password> – пароль до облікового запису бази даних, що має дозвіл на віддалений доступ на сервер.

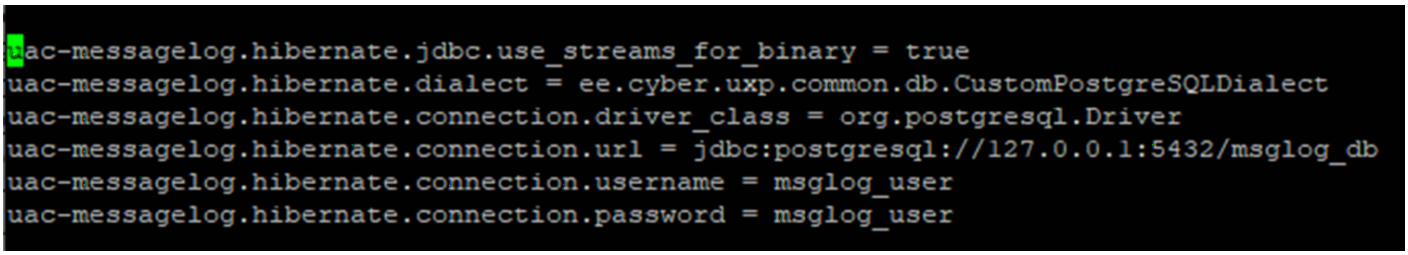


- **Якщо засіб перевірки повідомлень та база даних журналу повідомлень знаходяться на одному хості**, налаштування параметрів бази даних виглядатиме наступним чином:

```
uac-messagelog.hibernate.jdbc.use_streams_for_binary = true
uac-messagelog.hibernate.dialect = ee.cyber.uxp.common.db.CustomPostgreSQLDialect
uac-messagelog.hibernate.connection.driver_class = org.postgresql.Driver
```

```
uac-messagelog.hibernate.connection.url = jdbc:postgresql://127.0.0.1:5432/<messagelog_dbname>
uac-messagelog.hibernate.connection.username = <messagelog_user>
uac-messagelog.hibernate.connection.password = <messagelog_password>
```

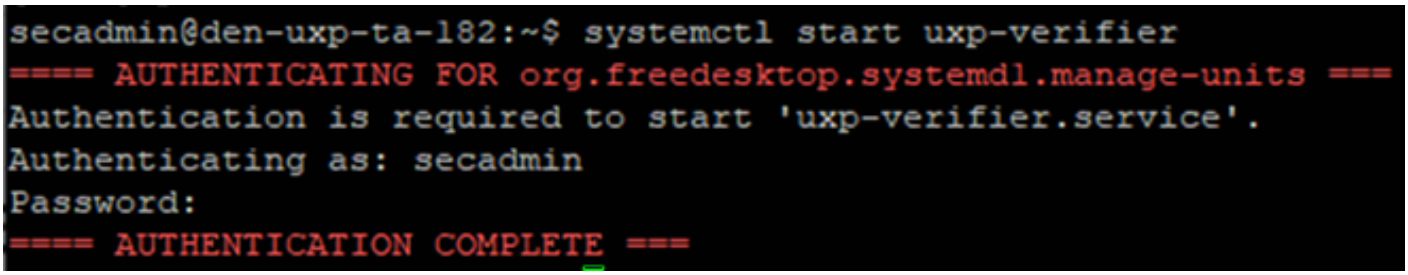
де <**messagelog_dbname**> – ім’я бази даних журналу повідомлень;
<messagelog_user> – логін облікового запису бази даних, що має дозвіл на віддалений доступ на сервер;
<messagelog_password> – пароль до облікового запису бази даних, що має дозвіл на віддалений доступ на сервер.



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

5. Запустити службу uxp-verifier за допомогою наступної команди:

```
sudo systemctl start uxp-verifier
```



9.2.3 ???????????? ????? ?????????? ????????????

Для завантаження якоря глобальної конфігурації необхідно:

1. Завантажити файл якоря конфігурації промислового середовища (файл configuration anchor) з Особистого кабінету Каталогу системи «Трембіта» (сторінка «Матеріали») на робочу станцію Адміністратора локальних компонентів (системного адміністратора).

2. Скопіювати файл якоря конфігурації на сервер засобу перевірки повідомлень використовуючи WinSCP або іншу програму.

3. Перемістити файл якоря конфігурації до директорії /etc/uxp/ серверу засобу перевірки за допомогою наступної команди:

```
sudo cp configuration_anchor_name.xml /etc/uxp/configuration-anchor.xml
```