

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](#)



```
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 «ОК».

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
```



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

на:

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

```
#-----  
# CONNECTIONS AND AUTHENTICATION  
#-----  
  
# - Connection Settings -  
  
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.

```
GNU nano 2.9.3 /etc/postgresql/10/main/pg_hba.conf Modified  
# IPv4 local connections:  
host all all 127.0.0.1/32 md5  
# IPv6 local connections:  
host all all ::1/128 md5  
# Allow replication connections from localhost, by a user with the  
# replication privilege.  
local replication all peer  
host replication all 127.0.0.1/32 md5  
host replication all ::1/128 md5  
host uac-messagelog uac-messagelog 192.168.1.182/32 md5
```

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/serverconf
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.CustomPostgreSQLDialect
uac-messagelog.hibernate.connection.driver_class = org.postgresql.Driver
uac-messagelog.hibernate.connection.url = jdbc:postgresql://192.168.1.113:5432/messagelog_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.

```
GNU nano 2.9.3 /etc/uxp/db.properties Mod
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://192.168.1.181:5432/uac-messagelog?ssl=true&sslfactory=org.postgresql.ssl.NonValidatingFactory
uac-messagelog.hibernate.connection.username = uac-messagelog
uac-messagelog.hibernate.connection.password = uac-messagelo
```

- **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.

```
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/msglog_db
uac-messagelog.hibernate.connection.username = msglog_user
uac-messagelog.hibernate.connection.password = msglog_user
```

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
```

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

### 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
```