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:

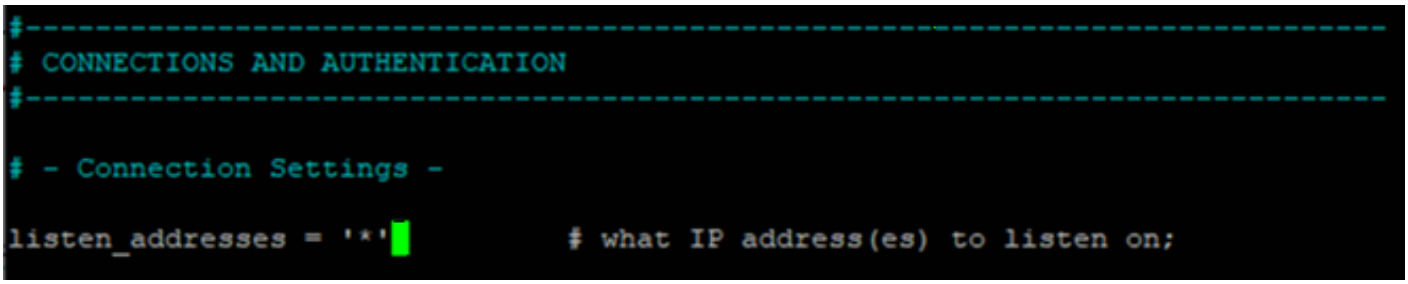
```
sudo nano /etc/postgresql/10/main/postgresql.conf
```

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 ===
```

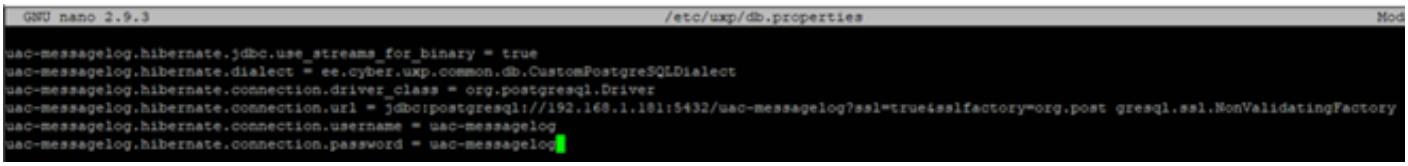
2. Відкрити на редагування файл /etc/uxp/db.properties за допомогою наступної команди:

```
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>
```

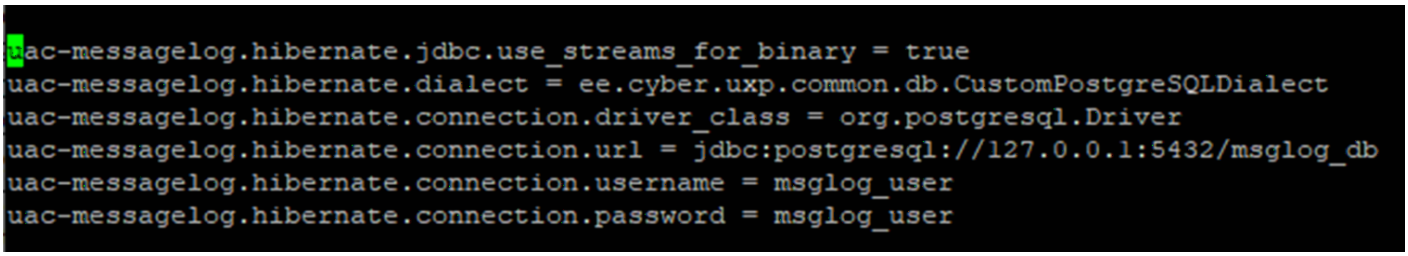
де **<db_host>** – ім’я хоста серверу PostgreSQL, де розміщено базу даних журналу повідомлень;
<messagelog_dbname> – ім’я бази даних журналу повідомлень;
<messagelog_user> – логін облікового запису бази даних, що має дозвіл на віддалений доступ на сервер;
<messagelog_password> – пароль до облікового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

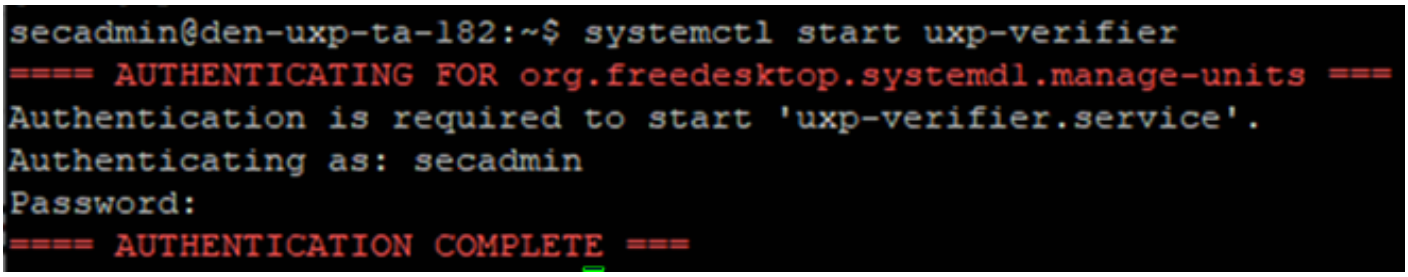
де <**messagelog_dbname>** – ім’я бази даних журналу повідомлень;
<messagelog_user> – логін облікового запису бази даних, що має дозвіл на віддалений доступ на сервер;
<messagelog_password> – пароль до облікового запису бази даних, що має дозвіл на віддалений доступ на сервер.



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
```

Версія #13
Admin створив 2024-05-29 13:17:47 UTC
Admin оновив 2024-09-25 11:36:34 UTC