10. ?????????? ?? ?????????? ??????? ??????? ????????

Для централізованого сховища журналів подій можна встановити новий або використати вже існуючий сервер аналізу журналів подій (з увімкненою службою Rsyslog Server). Встановлення та налаштування серверу аналізу журналів подій виконується Адміністратором локальних компонентів (системним адміністратором).

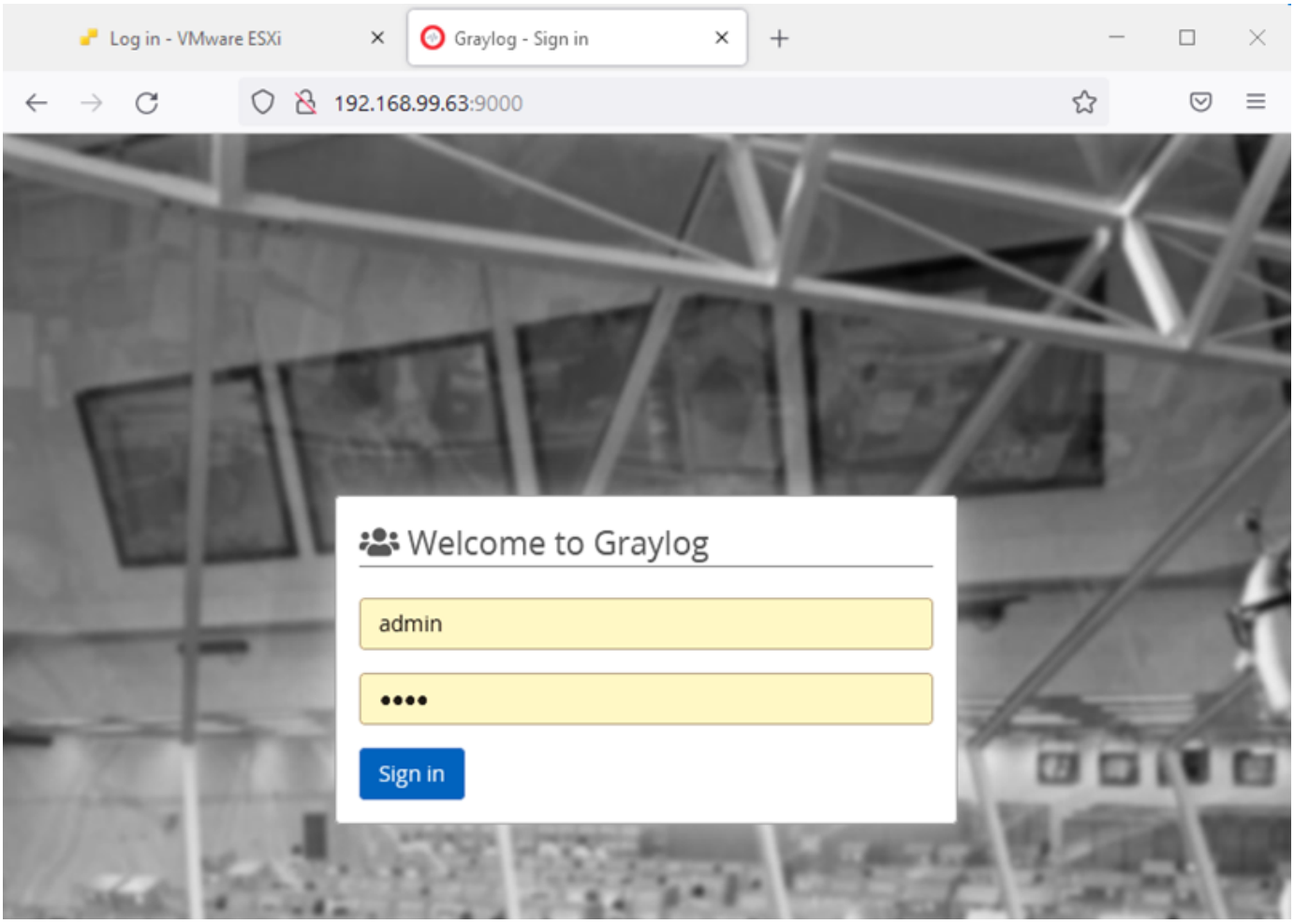
10.1 ????????? ????????????? ??????? ??????? ???????? ?????

Початкова конфігурація сервера аналізу журналів подій виконується Адміністратором локальних компонентів (системним адміністратором).

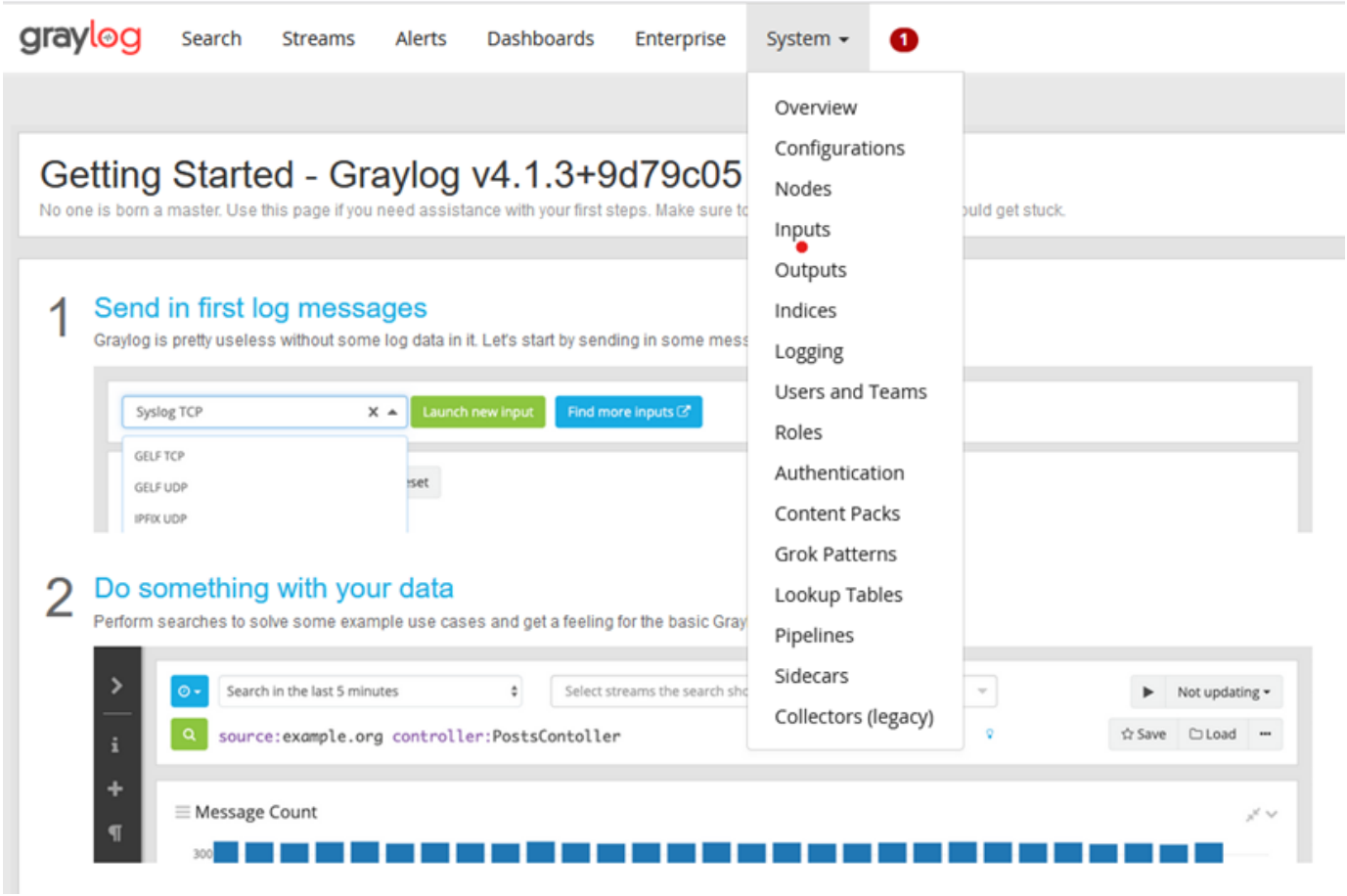
Для початкової конфігурації необхідно перейти до вебінтерфейсу серверу аналізу журналів за посиланням: http://<IP-GRAYLOG-Server>:9000,

де **<IP-GRAYLOG-Server>** - це IP – адреса серверу аналізу журналів подій,

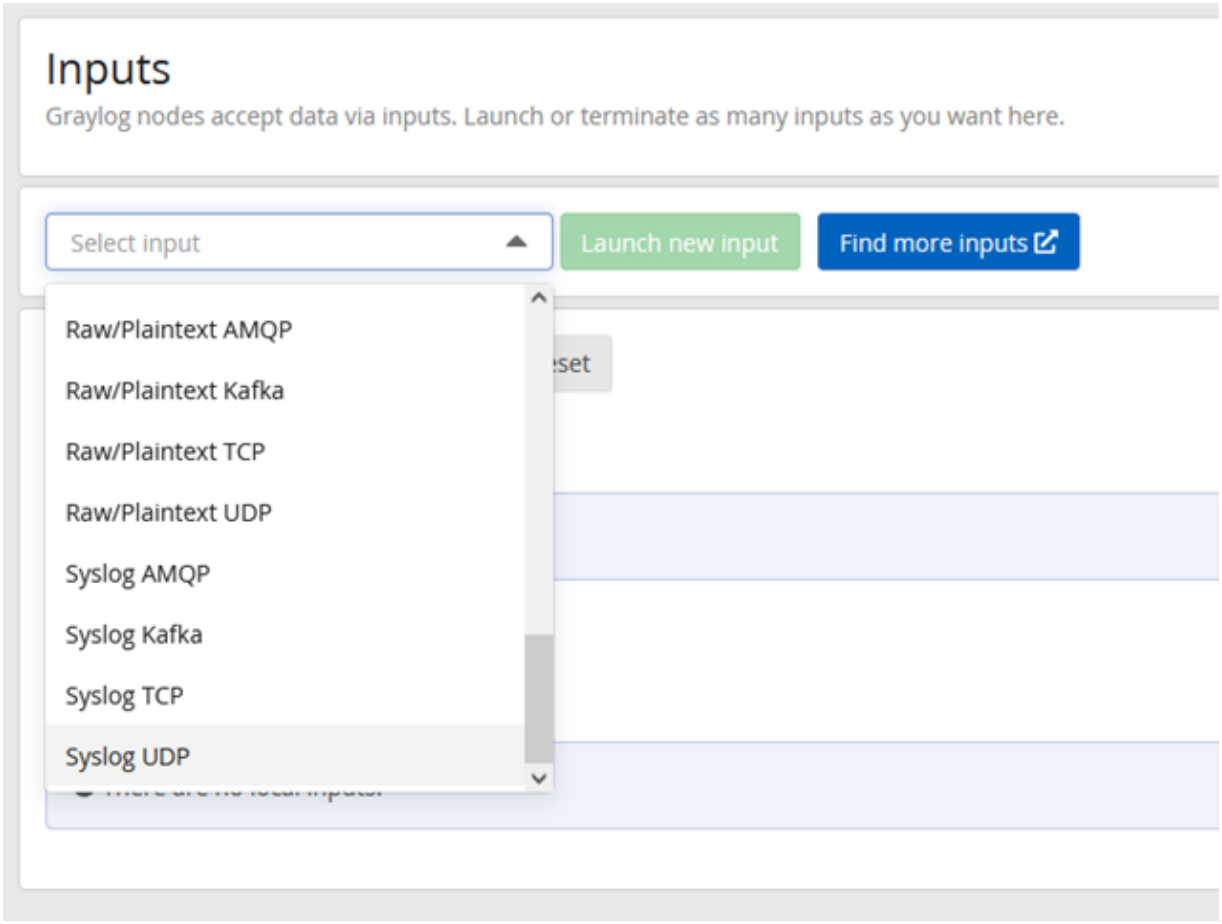
використовуючи логін «admin» та пароль, який було створено в пункті 10.2



Після успішної авторизації, необхідно перейти до вкладки System -> Inputs:

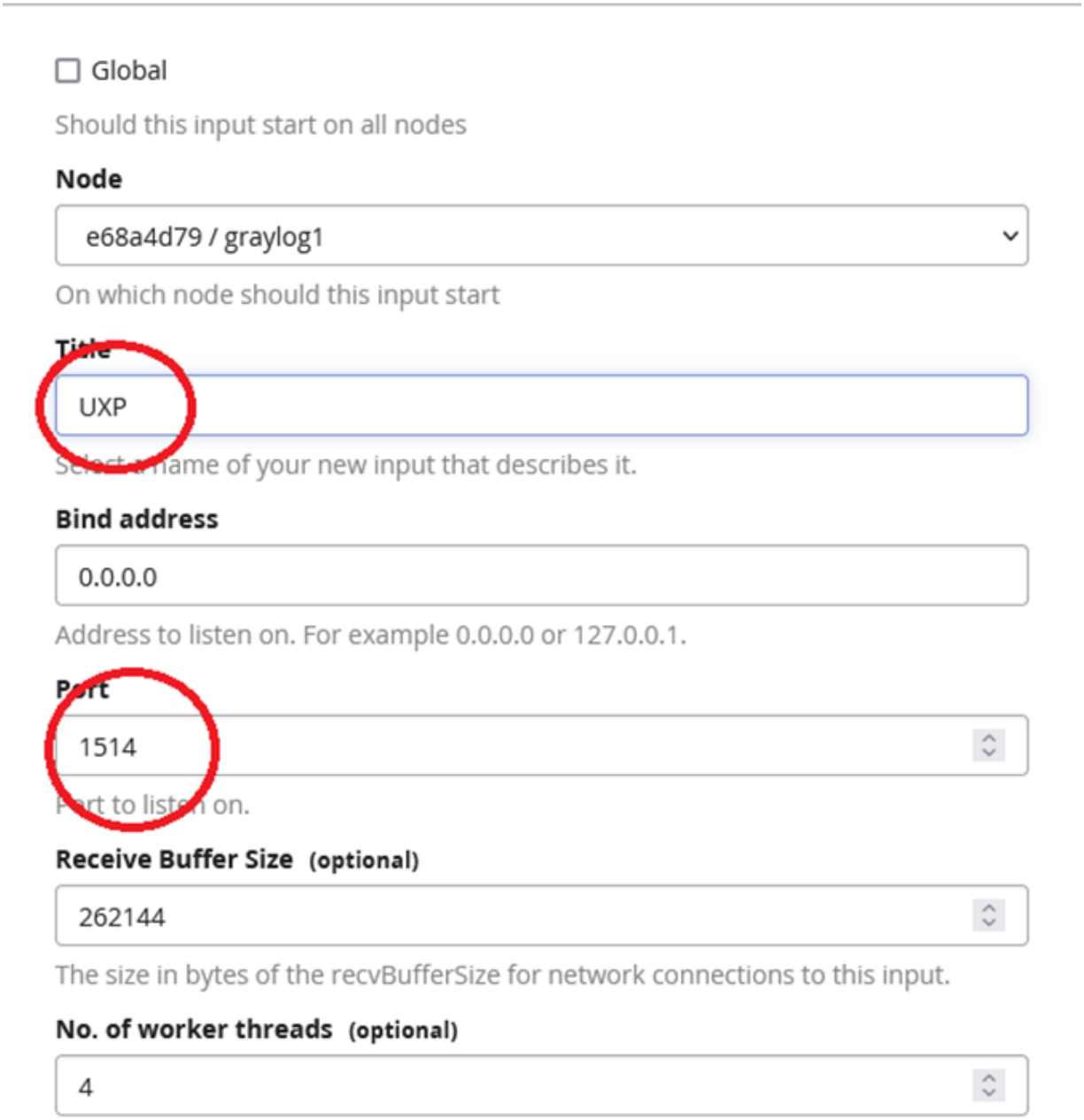


Та створити новий Input, задавши його тип як «Syslog UDP» та натиснути на кнопку «Launch new input»:

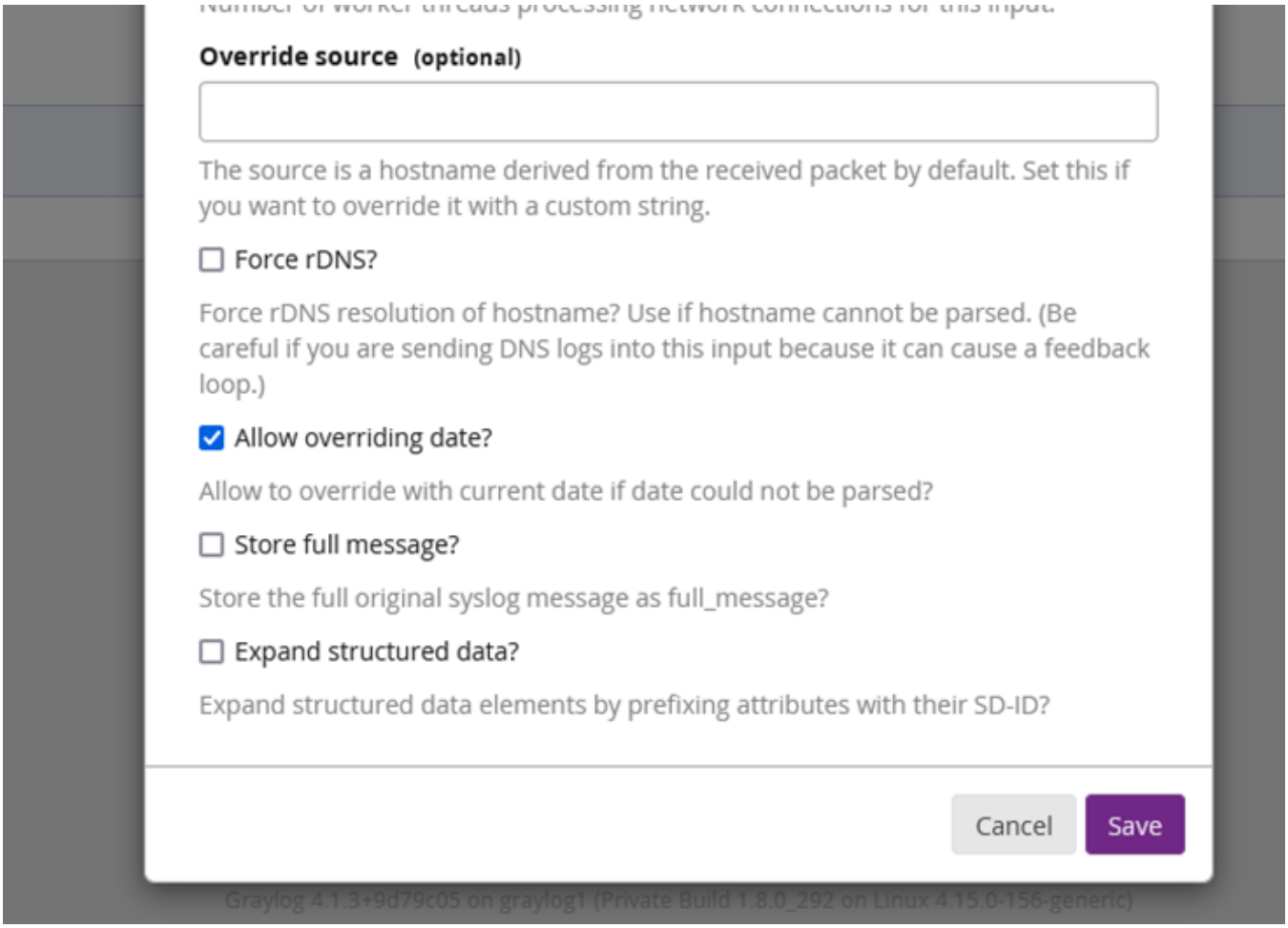


Після цього

необхідно відредагувати поля «Title» та «Port» наступним чином:



Та натиснути на кнопку «Save».


Number of worker threads processing network connections for this input.
Override source (optional)
The source is a hostname derived from the received packet by default. Set this if you want to override it with a custom string.
Force rDNS?
Force rDNS resolution of hostname? Use if hostname cannot be parsed. (Be careful if you are sending DNS logs into this input because it can cause a feedback loop.)
Allow overriding date?
Allow to override with current date if date could not be parsed?
Store full message?
Store the full original syslog message as full_message?
Expand structured data?
Expand structured data elements by prefixing attributes with their SD-ID?
Cancel
Save
Graylog 4.1.3+9d79c05 on graylog1 (Private Build 1.8.0_292 on Linux 4.15.0-156-generic)

10.2 ?????????? ?????????? ?? ????? ?????????? ??????

Параметри підключення до серверу аналізу журналів подій налаштовуються на шлюзі безпечного обміну. Для налаштування необхідно:

1. Увійти до командної консолі ШБО.

2. Відкрити на редагування файл /etc/rsyslog.d/40-uxp.conf за допомогою наступної команди:

```
sudo nano /etc/rsyslog.d/40-uxp.conf
```

3. Вказати IP-адресу сервера аналізу журналів подій у відповідній строчці даного файлу:

```
local0.info /var/log/uxp/audit.log;RSYSLOG_FileFormat
local0.info <@IP_GRAYLOG_Server>:1514
# discard further processing of local0.* to avoid doubling
& ~
```

де **<@IP_GRAYLOG_Server>** - це IP-адреса сервера аналізу журналів подій, яка призначена йому статично,

1514 – це порт, який використовується для прийому журналів, вказується через двокрапку після IP-адреси.

4. Замінити файл 45-uxpservices.conf на новий (порожній) за допомогою послідовного виконання наступних команд:

```
sudo rm /etc/rsyslog.d/45-uxpservices.conf
sudo nano /etc/rsyslog.d/45-uxpservices.conf
```

5. Додати наступні рядки до новоствореного файлу:

```
if ($programname == 'uxp-jetty' or $syslogtag == 'uxp-jetty' ) then {
   action(type="omfile" file="/var/log/uxp/jetty/jetty.log" flushOnTXEnd="off")
   action(type="omfwd" Target="<IP_SRAYLOG_Server>" Port="1514" Protocol="udp")
   stop
```

```
}

if ( $programname == 'uxp-signerconsole' or $syslogtag == 'uxp-signerconsole' ) then {
   /var/log/uxp/signer-console.log;RSYSLOG_FileFormat
   action(type="omfwd" Target="<IP_GRAYLOG_Server>" Port="1514" Protocol="udp")
   & stop
}

if ( $programname == 'uxp-signer' or $syslogtag == 'uxp-signer' ) then {
   action(type="omfwd" Target="<IP_GRAYLOG_Server>" Port="1514" Protocol="udp")
   /var/log/uxp/signer.log;RSYSLOG_FileFormat
   & stop
}

if ( $programname == 'uxp-confclient' or $syslogtag == 'uxp-confclient' ) then {
   action(type="omfwd" Target="<IP_GRAYLOG_Server>" Port="1514" Protocol="udp")
   /var/log/uxp/configuration_client.log;RSYSLOG_FileFormat
   & stop
}

if ( $programname == 'uxp-proxy' or $syslogtag == 'uxp-proxy' ) then {
   action(type="omfwd" Target="<IP_GRAYLOG_Server>" Port="1514" Protocol="udp")
   /var/log/uxp/proxy.log;RSYSLOG_FileFormat
   & stop
}

if ( $programname == 'uxp-proxymonitor' or $syslogtag == 'uxp-proxymonitor' ) then {
   action(type="omfwd" Target="<IP_GRAYLOG_Server>" Port="1514" Protocol="udp")
   /var/log/uxp/proxymonitoragent.log;RSYSLOG_FileFormat
   & stop
}

if ( $programname == 'uxp-audit' or $syslogtag == 'uxp-audit' ) then {
   action(type="omfwd" Target="<IP_GRAYLOG_Server>" Port="1514")
   /var/log/uxp/audit.log;RSYSLOG_FileFormat
   & stop
}


if ( $programname == 'ua-integrity' or $syslogtag == 'ua-integrity' ) then {
```

```
    action(type="omfwd" Target="<IP_GRAYLOG_Server>" Port="1514" Protocol="udp")
    /var/log/uaic/KZZ_integrity.log;RSYSLOG_FileFormat
    & stop
}
```

де <IP_GRAYLOG_Server> - локальна IP-адресу серверу аналізу журналів подій:

> **Примітка:**

Швидко замінити <IP_GRAYLOG_Server> на локальну IP-адресу серверу аналізу журналів подій можна виконавши наступні дії:

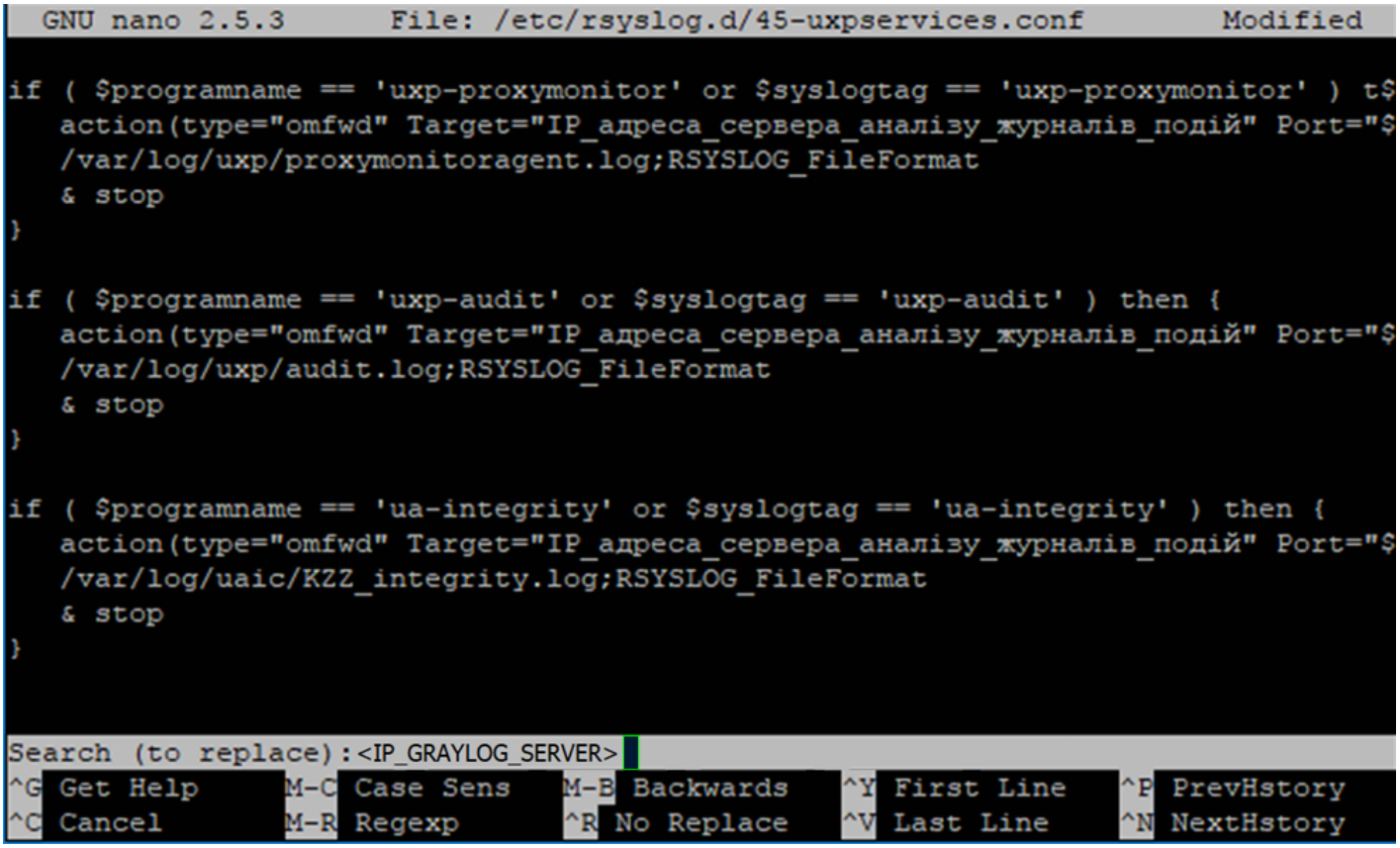
- Відкрити на редагування файл 45-uxpservices.conf за допомогою наступної команди.

```
sudo nano /etc/rsyslog.d/45-uxpservices.conf
```

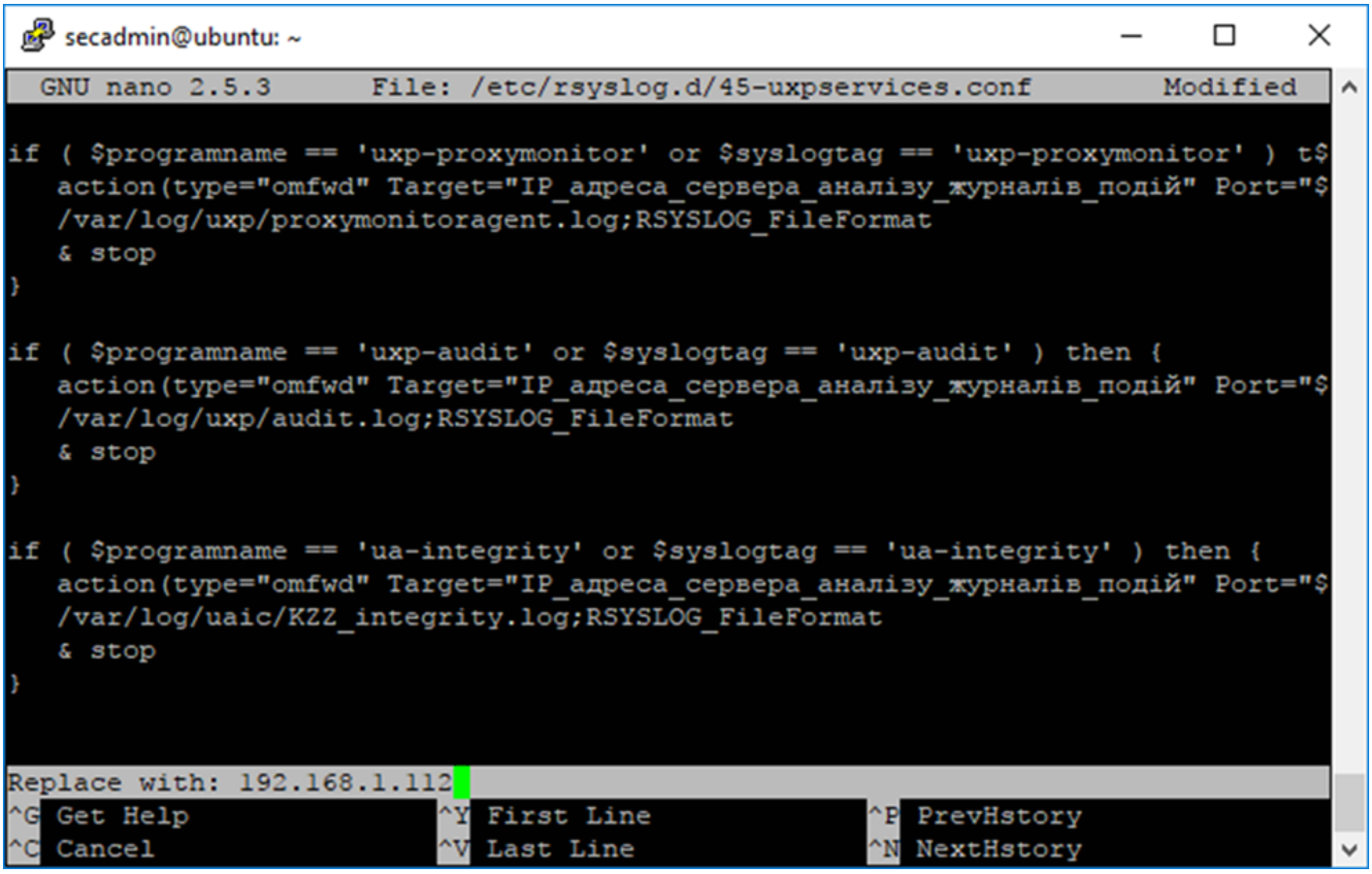
- Натиснути комбінацію клавіш «Ctrl+\» - це забезпечить пошук та подальшу заміну тексту.

- Скопіювати (або ввести) наступний текст у поле пошуку редактора nano:

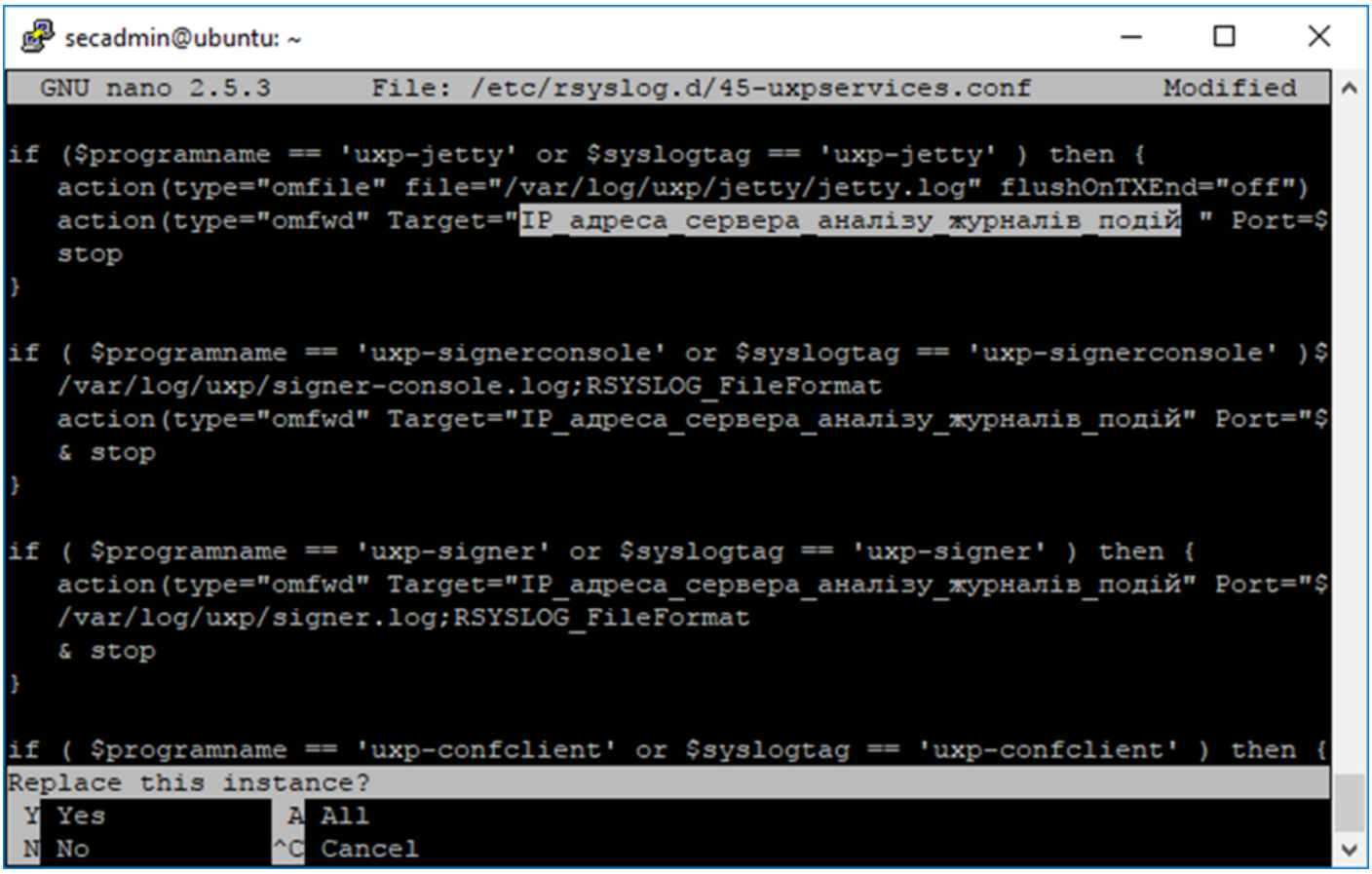
```
< IP_GRAYLOG_Server >
```

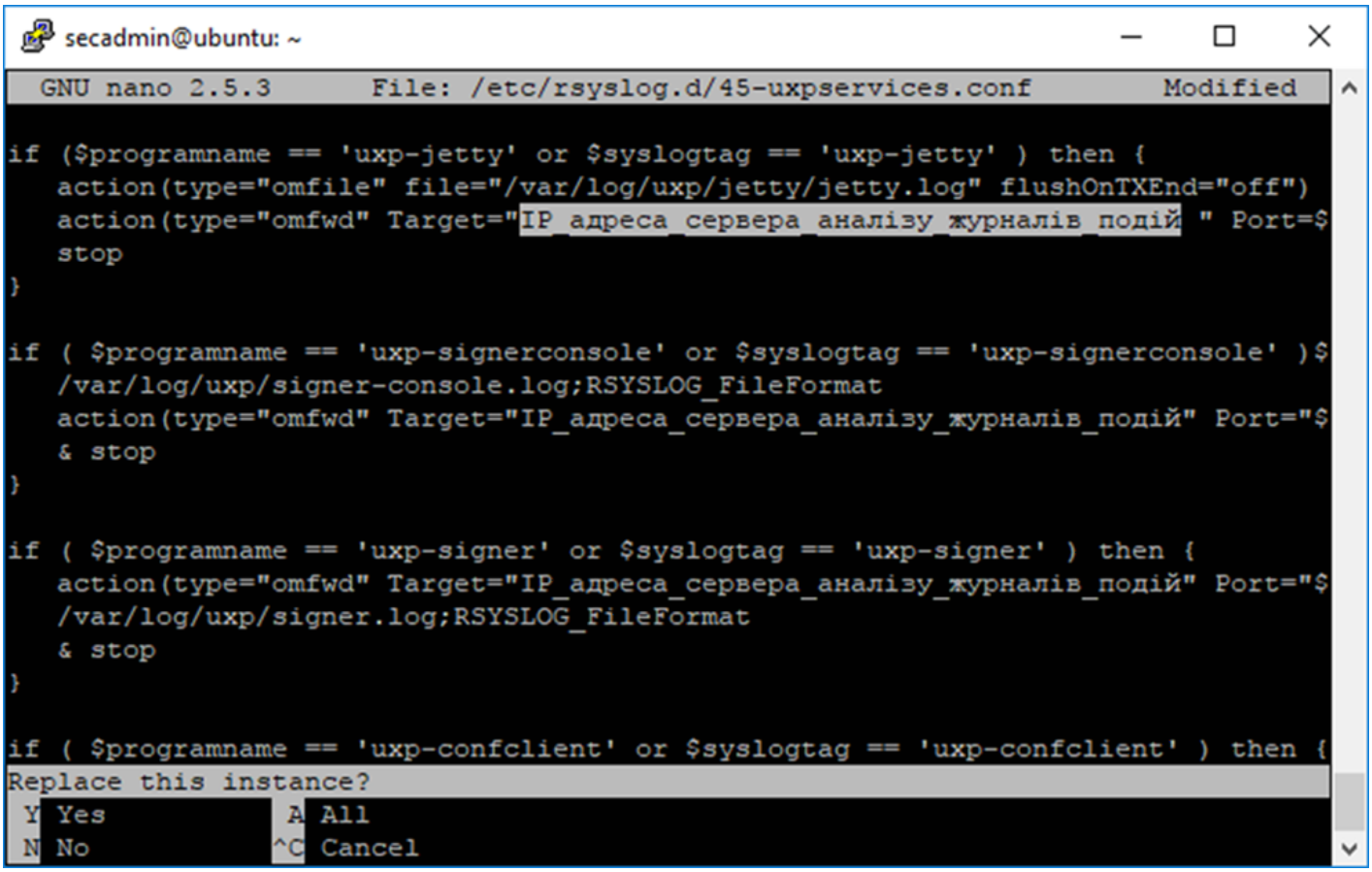


- Натиснути клавішу "Enter" та ввести локальну IP-адресу сервера аналізу журналів подій у поле «Replace with:»:



- Натиснути клавішу "Enter" та клавішу "A" (латинська розкладка) - це дозволить замінити всі знайдені рядки.





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

збереження.

7. Перезавантажити службу rsyslog на шлюзі безпечного обміну шляхом виконання наступної команди:

```
sudo service rsyslog restart
```

8. Перевірити стан Rsyslog шляхом виконання наступної команди:

```
sudo rsyslogd -N 1
```

Сервер аналізу журналів подій централізовано протоколює події, які реєструються на шлюзі безпечного обміну та передаються за протоколом SYSLOG. Для перегляду логів необхідно перейти за посиланням http://<IP_GRAYLOG_Server>:9000/search.