

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. Встановлення серверу аналізу журналів подій](#)
- [10.2. Налаштування серверу аналізу журналів подій](#)
- [10.3 Початкова конфігурація сервера аналізу журналів подій](#)
- [10.4 Налаштування підключення до шлюзу безпечного обміну](#)


```
sudo systemctl daemon-reload
sudo systemctl enable mongod.service
sudo systemctl restart mongod.service
```

6. Перевірити, що база даних коректно почала роботу за допомогою наступної команди:

```
sudo systemctl --type=service --state=active | grep mongod
```

7. Встановити пакет elasticsearch за допомогою наступної команди:

```
sudo apt-get install elasticsearch
```

8. Змінити конфігурацію сервісу elasticsearch за допомогою наступної команди:

```
sudo tee -a /etc/elasticsearch/elasticsearch.yml > /dev/null <<EOT
cluster.name: graylog
action.auto_create_index: false
EOT
```

9. Запустити сервіс elasticsearch та налаштувати його автоматичний запуск під час завантаження ОС за допомогою послідовного виконання наступних команд:

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl restart elasticsearch.service
```

10. Перевірити, що запуск сервісу відбувся успішно за допомогою наступної команди:

```
sudo systemctl --type=service --state=active | grep elasticsearch
```

11. Встановити сервер Graylog за допомогою наступної команди:

```
sudo apt-get install graylog-server
```


2. Параметр **password_secret**. Для задачі цього параметру необхідно виконати наступні дії:

- Виконати команду

```
pwgen -N 1 -s 96
```

- Буде відображено відображено строку, що міститиме буквенно-циферну комбінацію, наприклад:

```
root@graylog1:~# pwgen -N 1 -s 96
2urQVGoLUFQwefxh1Y6IkpRq0ZPbvH0Ika87sJN0BQ7VIvfngQPWtytgrrrWRmOoPMN9IyPuAoleE9BM3Pu4EWF5FM4Br3If
```

- Відкрити на редагування файл конфігурації /etc/graylog/server/server.conf за допомогою наступної команди:

```
sudo nano /etc/graylog/server/server.conf
```

- Розкоментувати (видалити символ «#») рядок з параметром password_secret та скопіювати отриману комбінацію як значення цього параметру:

```
# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 64 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted values in the database invalid. (es
password_secret = 2urQVGoLUFQwefxh1Y6IkpRq0ZPbvH0Ika87sJN0BQ7VIvfngQPWtytgrrrWRmOoPMN9IyPuAoleE9BM3Pu4EWF5FM4Br3If
# The default root user is named 'admin'
#root_username = admin
# You MUST specify a hash password for the root user (which you only need to initially set up the
# system and in case you lose connectivity to your authentication backend)
```

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

3. Параметр **http_bind_address**. Для задачі цього параметру необхідно виконати наступні дії:

- Відкрити на редагування файл конфігурації /etc/graylog/server/server.conf за допомогою наступної команди:

```
sudo nano /etc/graylog/server/server.conf
```

- Розкоментувати (видалити символ «#») рядок з параметром http_bind_address та задати значення цього параметру наступним чином:

```
http_bind_address = 0.0.0.0:9000
```

```
#
# Default: 127.0.0.1:9000
http_bind_address = 0.0.0.0:9000
#http_bind_address = [2001:db8::1]:9000

#### HTTP publish URI
#
# The HTTP URI of this Graylog node which is used to communicate with
# clients using the Graylog web interface.
#
```

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

4. Параметр **root_timezone**. Для задачі цього параметру необхідно виконати наступні дії:

- Відкрити на редагування файл конфігурації `/etc/graylog/server/server.conf` за допомогою наступної команди:

```
sudo nano /etc/graylog/server/server.conf
```

- Розкоментувати (видалити символ «#») рядок з параметром `root_timezone` та задати значення цього параметру наступним чином:

```
root_timezone = Europe/Kiev
```

```
#
# Default: 127.0.0.1:9000
http_bind_address = 0.0.0.0:9000
#http_bind_address = [2001:db8::1]:9000

#### HTTP publish URI
#
# The HTTP URI of this Graylog node which is used to communicate with
# clients using the Graylog web interface.
#
```

13. Перезапустити сервіс та перевірити, чи коректно він функціонує за допомогою послідовного виконання наступних команд:

```
sudo systemctl daemon-reload
sudo systemctl enable graylog-server.service
sudo systemctl restart graylog-server.service
sudo systemctl --type=service --state=active | grep graylog
```

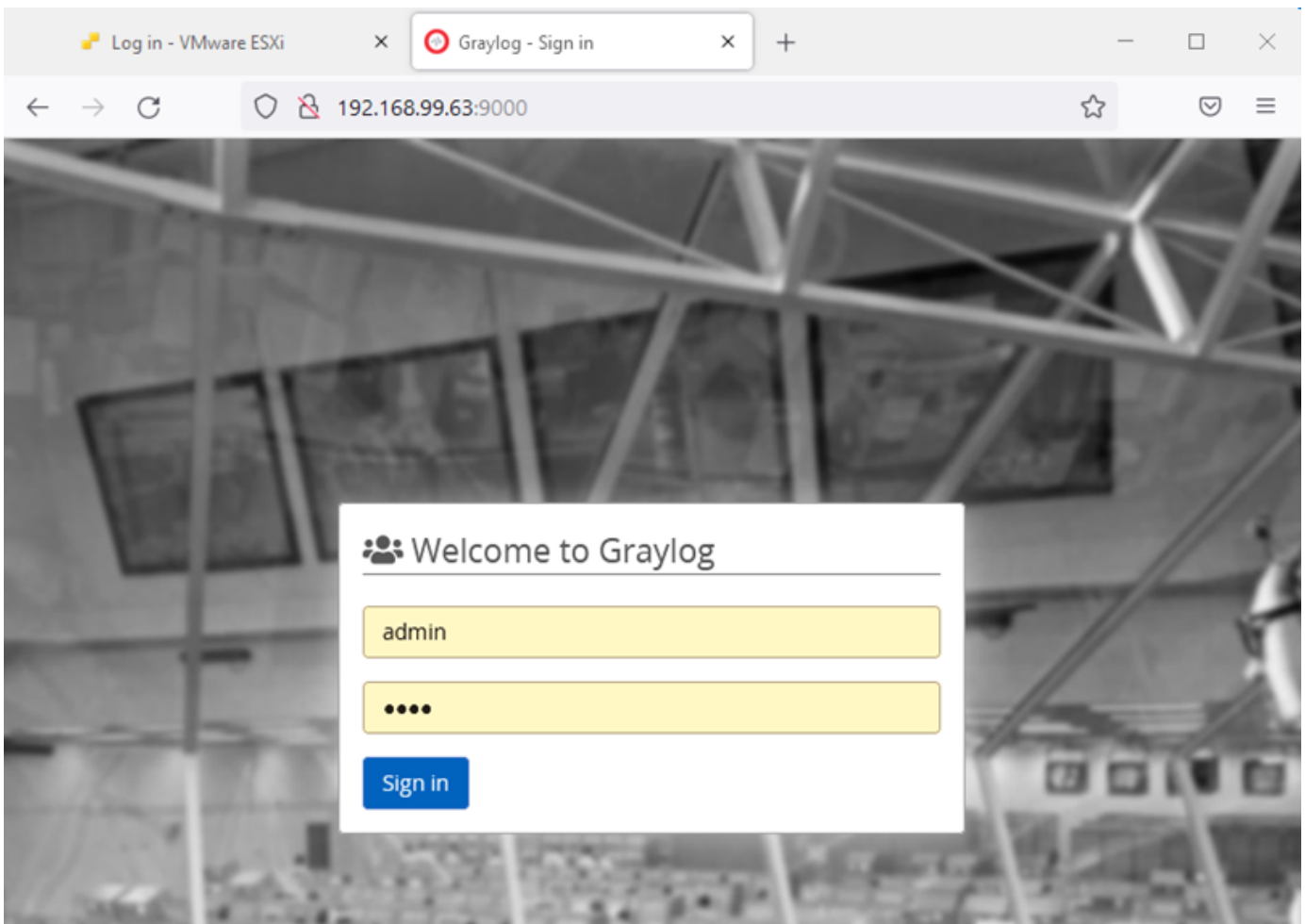

10.3 ?????????? ?????????????? ????????? ?????????? ?????????? ???????

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

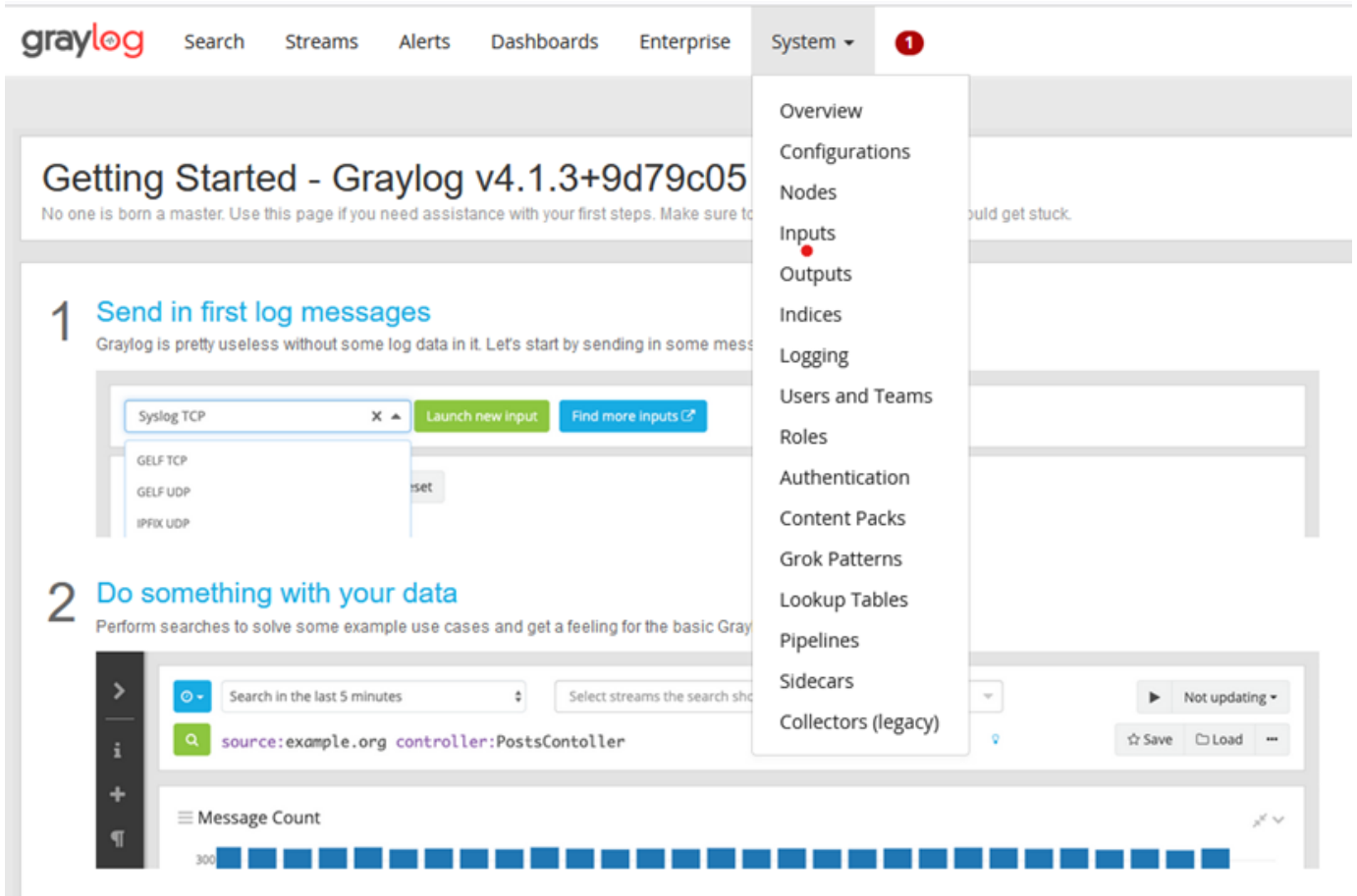
Для початкової конфігурації необхідно перейти до вебінтерфейсу серверу аналізу журналів за посиланням: <http://<IP-GRAYLOG-Server>:9000>,

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»:

Inputs

Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.

Select input

Launch new input

Find more inputs [↗](#)

Raw/Plaintext AMQP

Raw/Plaintext Kafka

Raw/Plaintext TCP

Raw/Plaintext UDP

Syslog AMQP

Syslog Kafka

Syslog TCP

Syslog UDP

set

Після цього

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

Global

Should this input start on all nodes

Node

e68a4d79 / graylog1

On which node should this input start

Title

UXP

Select a name of your new input that describes it.

Bind address

0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port

1514

Port to listen on.

Receive Buffer Size (optional)

262144

The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)

4

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

10.4 ??????????????

?????????????? ?? ??????

?????????????? ????????

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_GRAYLOG_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:

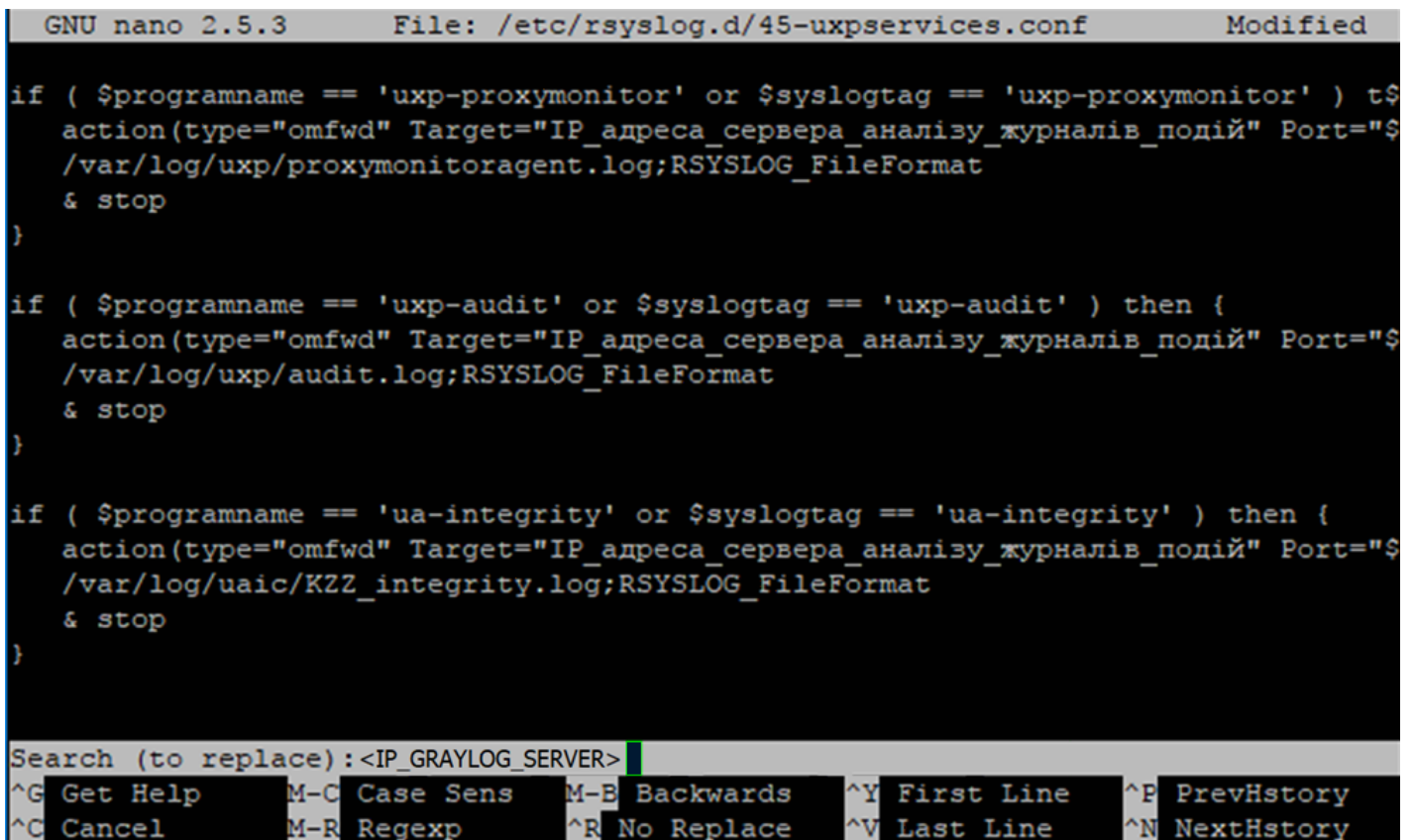
- Відкрити на редагування файл 45-uxpservices.conf за допомогою наступної команди.

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

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

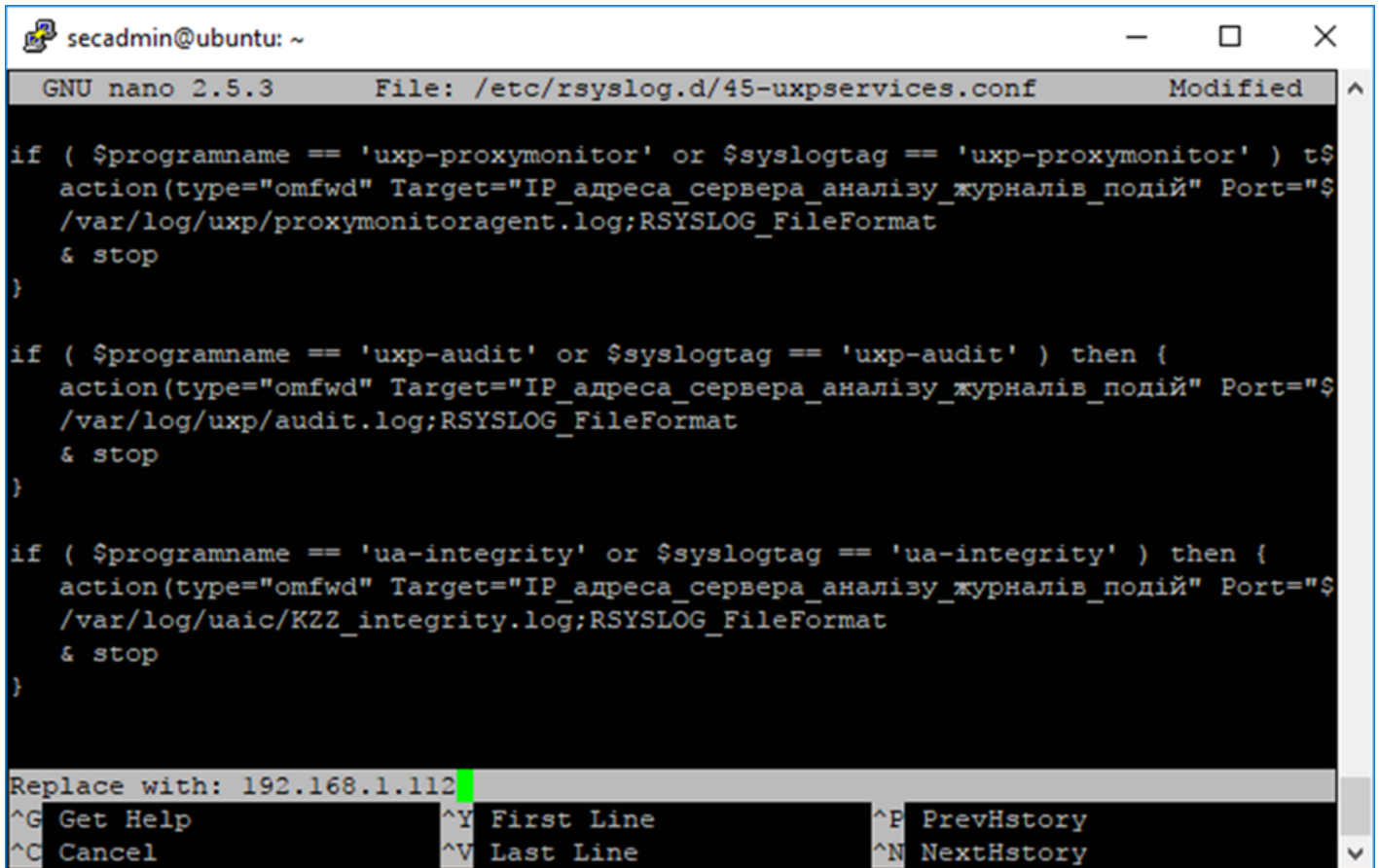
- Скопіювати (або ввести) наступний текст у поле пошуку редактора nano:

```
< IP_GRAYLOG_Server >
```



```
GNU nano 2.5.3      File: /etc/rsyslog.d/45-uxpservices.conf      Modified
if ( $programname == 'uxp-proxymonitor' or $syslogtag == 'uxp-proxymonitor' ) t$
  action(type="omfwd" Target="IP_адреса_сервера_аналізу_журналів_подій" Port="$
  /var/log/uxp/proxymonitoragent.log;RSYSLOG_FileFormat
  & stop
}
if ( $programname == 'uxp-audit' or $syslogtag == 'uxp-audit' ) then {
  action(type="omfwd" Target="IP_адреса_сервера_аналізу_журналів_подій" Port="$
  /var/log/uxp/audit.log;RSYSLOG_FileFormat
  & stop
}
if ( $programname == 'ua-integrity' or $syslogtag == 'ua-integrity' ) then {
  action(type="omfwd" Target="IP_адреса_сервера_аналізу_журналів_подій" Port="$
  /var/log/uaic/KZZ_integrity.log;RSYSLOG_FileFormat
  & stop
}
Search (to replace):<IP_GRAYLOG_SERVER>
^G Get Help      M-C Case Sens  M-B Backwards  ^Y First Line   ^P PrevHstry
^C Cancel        M-R Regexp     ^R No Replace   ^V Last Line    ^N NextHstry
```

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



```
secadmin@ubuntu: ~
GNU nano 2.5.3 File: /etc/rsyslog.d/45-uxpservices.conf Modified
if ( $programname == 'uxp-proxymonitor' or $syslogtag == 'uxp-proxymonitor' ) t$
  action(type="omfwd" Target="IP_адреса_сервера_аналізу_журналів_подій" Port="$
    /var/log/uxp/proxymonitoragent.log;RSYSLOG_FileFormat
  & stop
}

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

if ( $programname == 'ua-integrity' or $syslogtag == 'ua-integrity' ) then {
  action(type="omfwd" Target="IP_адреса_сервера_аналізу_журналів_подій" Port="$
    /var/log/uaic/KZZ_integrity.log;RSYSLOG_FileFormat
  & stop
}

Replace with: 192.168.1.112
^G Get Help      ^Y First Line   ^P PrevHistory
^C Cancel        ^V Last Line    ^N NextHistory
```

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

```
secadmin@ubuntu: ~
GNU nano 2.5.3 File: /etc/rsyslog.d/45-uxpservices.conf Modified
if ($programname == 'uxp-jetty' or $syslogtag == 'uxp-jetty' ) then {
  action(type="omfile" file="/var/log/uxp/jetty/jetty.log" flushOnTXEnd="off")
  action(type="omfwd" Target="IP адреса сервера аналізу журналів подій" Port=$
  stop
}

if ( $programname == 'uxp-signerconsole' or $syslogtag == 'uxp-signerconsole' )$
/var/log/uxp/signer-console.log;RSYSLOG_FileFormat
action(type="omfwd" Target="IP_адреса_сервера_аналізу_журналів_подій" Port="$
& stop
}

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

if ( $programname == 'uxp-confclient' or $syslogtag == 'uxp-confclient' ) then {
Replace this instance?
Y Yes A All
N No ^C Cancel
```

```
secadmin@ubuntu: ~
GNU nano 2.5.3 File: /etc/rsyslog.d/45-uxpservices.conf Modified
if ($programname == 'uxp-jetty' or $syslogtag == 'uxp-jetty' ) then {
  action(type="omfile" file="/var/log/uxp/jetty/jetty.log" flushOnTXEnd="off")
  action(type="omfwd" Target="IP адреса сервера аналізу журналів подій" Port=$
  stop
}

if ( $programname == 'uxp-signerconsole' or $syslogtag == 'uxp-signerconsole' )$
/var/log/uxp/signer-console.log;RSYSLOG_FileFormat
action(type="omfwd" Target="IP_адреса_сервера_аналізу_журналів_подій" Port="$
& stop
}

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

if ( $programname == 'uxp-confclient' or $syslogtag == 'uxp-confclient' ) then {
Replace this instance?
Y Yes A All
N No ^C Cancel
```

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.