

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:

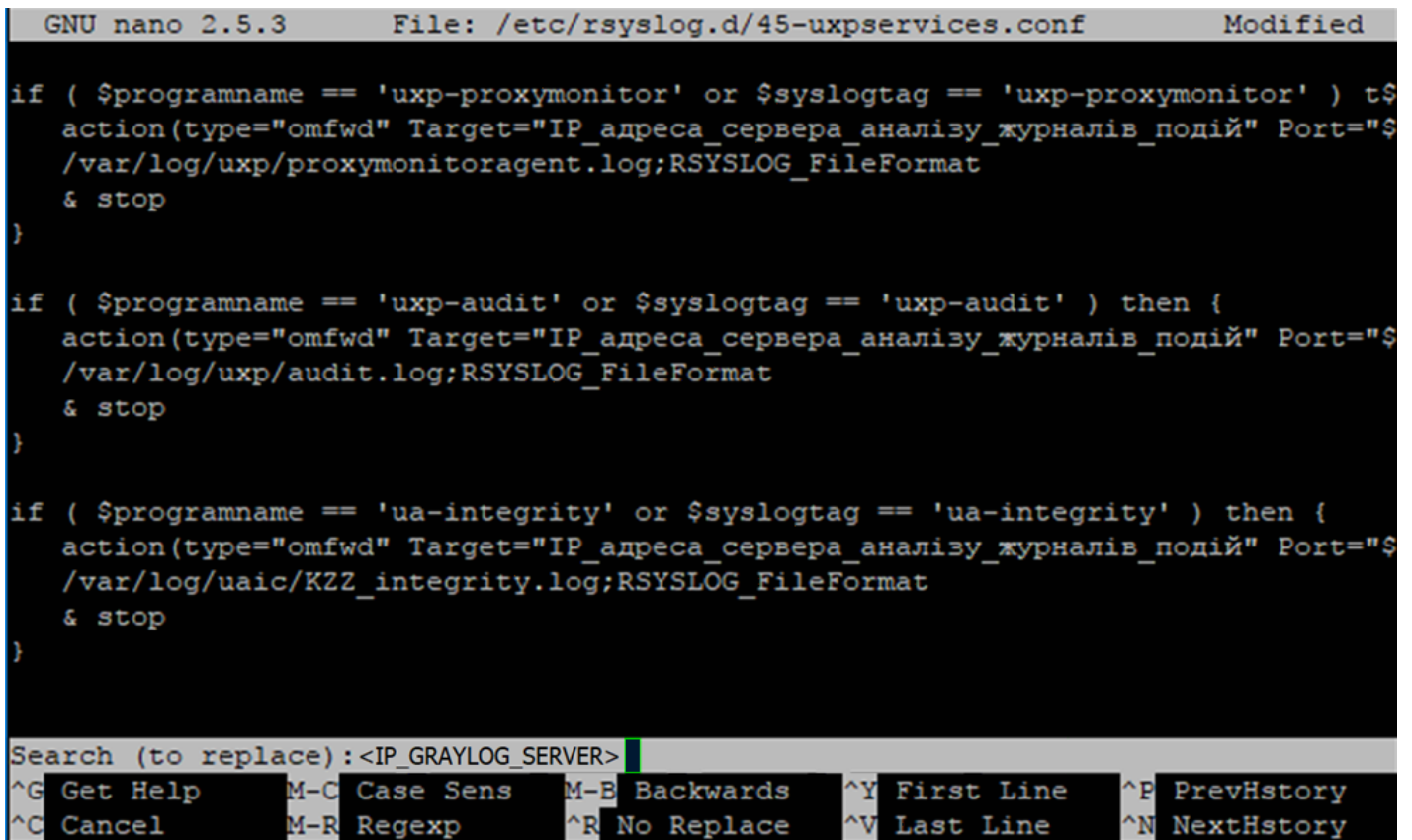
- Відкрити на редагування файл 45-uxpservices.conf за допомогою наступної команди.

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

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

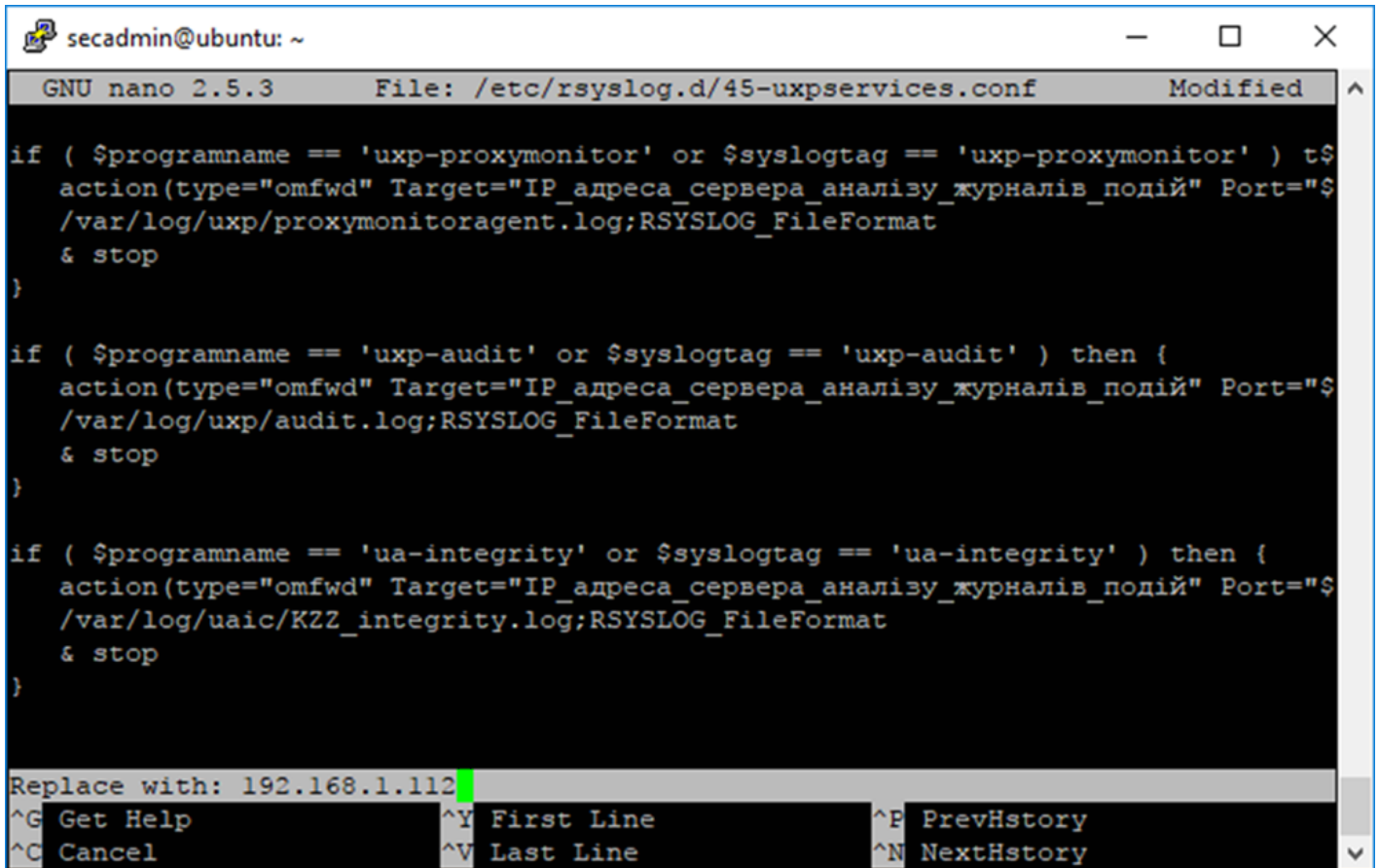
- Скопіювати (або ввести) наступний текст у поле пошуку редактора nano:

```
< 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 PrevHstory
^C Cancel        M-R Regexp      ^R No Replace    ^V Last Line    ^N NextHstory
```

- 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.

Версія #4

Admin створив 2024-05-29 16:02:05 UTC

Administrator оновив 2025-11-27 12:48:15 UTC