Настройка реакции на событие через именованный канал

1. Создайте скрипт для запуска службы:

```
# cat /usr/local/sbin/pipeparser
#!/bin/bash

PATH='/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin'

rm -f /var/run/pipelog1
mkfifo /var/run/pipelog1

while true
do
 MSG=$(head -1 /var/run/pipelog1)
 echo -n $(date +%Y-%m-%dT%H:%M:%S) >> /tmp/myaction
 echo -n " My action for message: $MSG" >> /tmp/myaction
 remIP=$(echo $MSG | sed -r 's/.*from ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+).*/\1/')
 echo " IS iptables -I INPUT -s $remIP -p tcp --dport 22 -j DROP" >>
/tmp/myaction
done
```

2. Создайте юнит systemd для запуска службы и активируйте его:

```
# systemctl cat pipeparser.service
# /etc/systemd/system/pipeparser.service
[Unit]
Description = Service for start simple pipe parser
Before=rsyslog.service

[Service]
Type=simple
ExecStart=/usr/local/sbin/pipeparser

[Install]
WantedBy=multi-user.target

# systemctl daemon-reload
# systemctl enable --now pipeparser.service
```

3. Настройте и перезапустите rsyslog:

```
# cat /etc/rsyslog.d/myparser.conf
if $programname contains 'sshd' and $msg contains 'Failed password for root
from' then |/var/run/pipelog1
# systemctl restart rsyslog.service
```

4. Проверьте работу парсера:

```
# ssh root@127.0.0.1
root@127.0.0.1's password:
Permission denied, please try again.
root@127.0.0.1's password:

# tail -1 /tmp/myaction
2025-11-10T21:58:00 My action for message: 2025-11-10T21:58:00.835726+05:00
debian sshd-session[3850]: Failed password for root from 127.0.0.1 port 41234
ssh2 IS iptables -I INPUT -s 127.0.0.1 -p tcp --dport 22 -j DROP

# date
Пн 10 ноя 2025 21:58:16 +05
```