Эшелон
учебный центр

Мониторинг событий ИБ в среде Linux: события, фильтры и директивы корреляции для выявления инцидентов

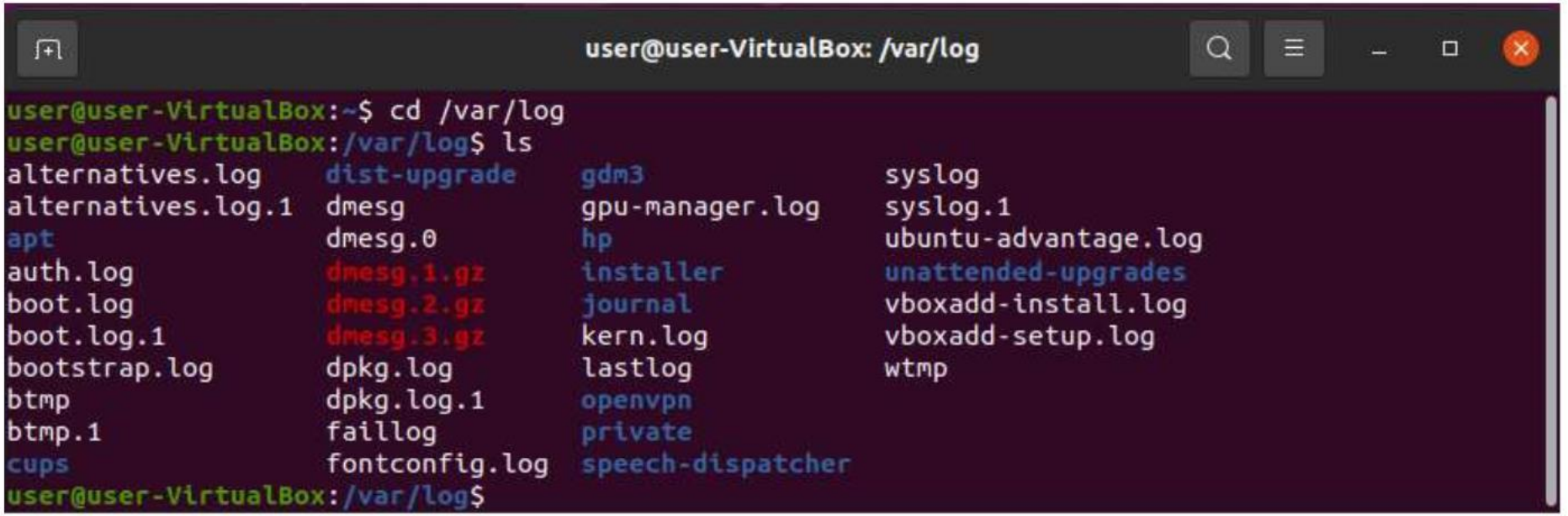
Каменский Станислав, Специалист группы внедрения СЗИ

KOMRAD troubleshooting

1. Проверка доступности по сети: ping
2. Проверка работы всех сервисов: systemctl list-units --type=service
3. Просмотр журнала сервиса: journalctl -u service-name.service

Стандартное журналирование в Linux

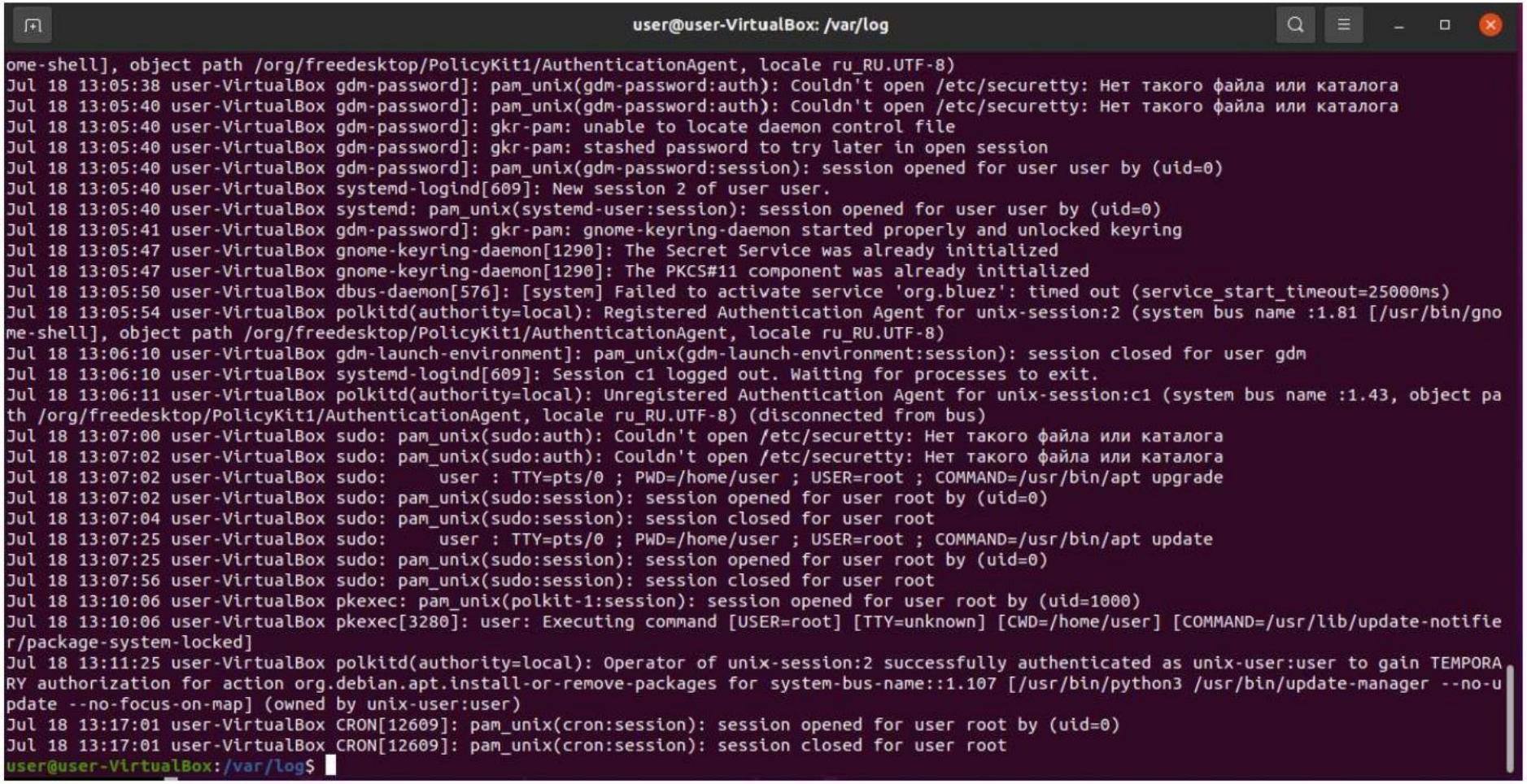
- Файлы журналов сохраняются в директорию /var/log



Важные системные журналы

- В /var/log/syslog и /var/log/messages записываются системные события. Debian-based системы как Ubuntu сохраняют данные в /var/log/syslog, в то время как Red Hat-based системы как RHEL or CentOS используют /var/log/messages.
- В /var/log/auth.log и /var/log/secure записываются события, связанные с безопасностью (вход в систему, действия root, вывод из модулей PAM и др.). Ubuntu и Debian используют /var/log/auth.log, в то время как Red
  Hat and CentOS используют /var/log/secure.
- В /var/log/kern.log записываются события ядра, ошибки и предупреждения.
- В /var/log/cron сохраняются события о запланированных задачах.

Содержимое auth.log



Что такое syslog?

Syslog это стандарт регистрации событий и их передачи

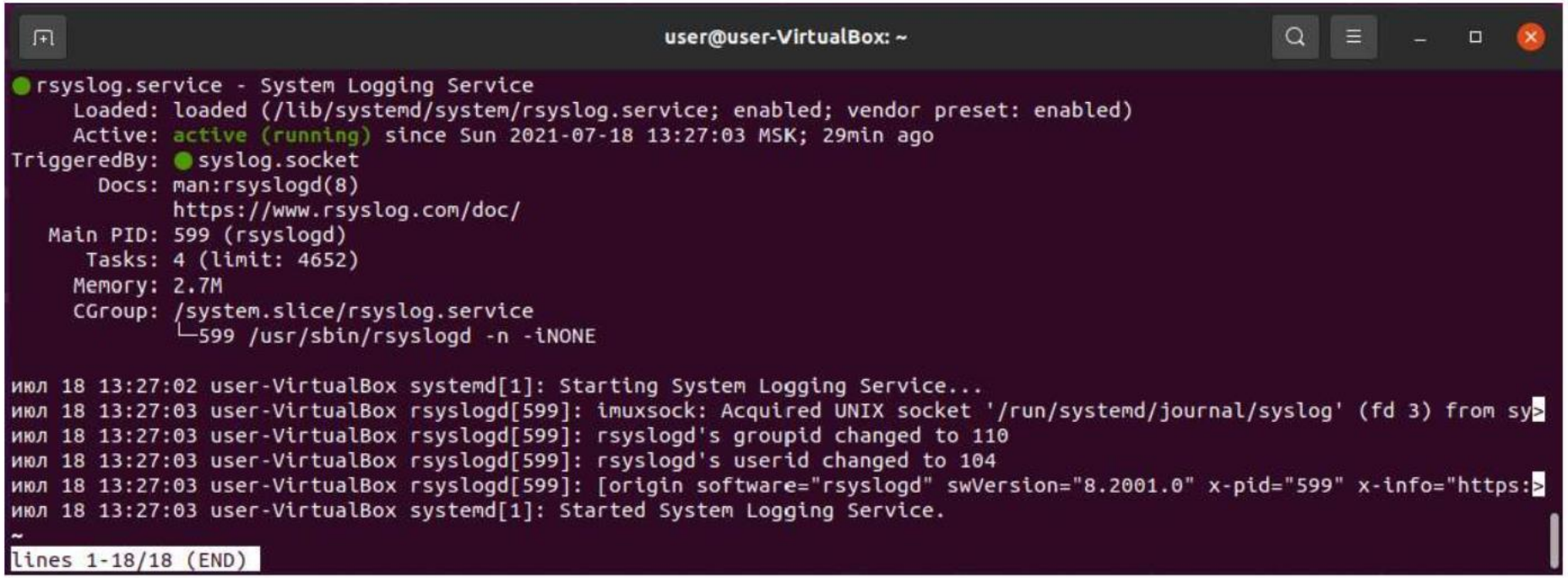
Слово “syslog” в зависимости от контекста может означать следующее:

- Сервис syslog, который получает и обрабатывает syslog-сообщения. Он ожидает события, создав socket /dev/log, в который пишут приложения. Он может писать события в локальный файл или направлять события на удаленный сервер. Есть несколько реализаций сервиса, самые популярные rsyslogd и syslog-ng.
- Протокол syslog (RFC 5424), который определяет, как передавать события по сети.
- Формат события syslog, включающего заголовок и содержимое события.

Отправка событий из журнала /var/log/auth.log в SIEM-систему КОМРАД

- Проверяем, что rsyslog запущен:

sudo systemctl status rsyslog



Настройка rsyslog

- Все настройки rsyslog находятся в файле /etc/rsyslog.conf и других конфигурационных файлах из /etc/rsyslog.d/ (можно посмотреть наличие файлов с помощью команды:

  ls /etc/rsys*

- Основной конфигурационный файл - /etc/rsyslog.conf, в нем подключены все файлы из папки /etc/rsyslog.d/ с помощью директивы IncludeConfig в самом начале файла:

  IncludeConfig /etc/rsyslog.d/*.conf

Источники событий Linux

auth;
authpriv;
cron;
daemon;
kern;
lpr;
mail;
mark;
news;
security (эквивалентно auth);
syslog;
user;
uucp;
local0 … local7;

Настройка отправки всех событий по TCP

. action(type="omfwd" target="192.168.88.250" port="49000" protocol="tcp" action.resumeRetryCount="100" queue.type="linkedList" queue.size="10000")

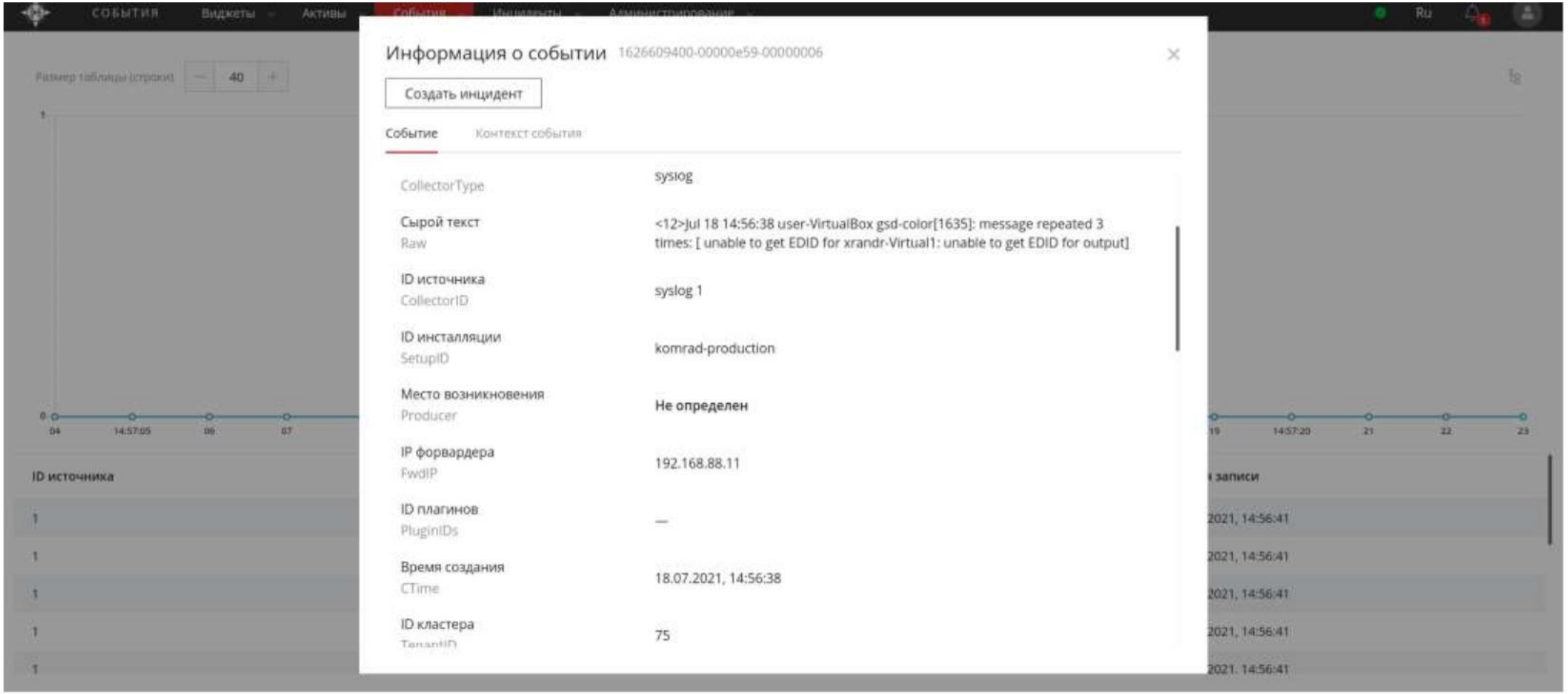
Перезапуск сервиса:

sudo systemctl restart rsyslog

Проверка статуса сервиса и отсутствия ошибок парсинга конфигурационного файла:

sudo systemctl status rsyslog

Результат: события в КОМРАД



Отправка только auth событий по TCP

auth,authpriv.* action(type="omfwd" target="192.168.88.250" port= "49000" protocol="tcp" action.resumeRetryCount="100" queue.type="linkedList" queue.size="10000")

Перезапуск сервиса:

sudo systemctl restart rsyslog

Проверка статуса сервиса и отсутствия ошибок парсинга конфигурационного файла:

sudo systemctl status rsyslog

СПАСИБО ЗА ВНИМАНИЕ!

Каменский Станислав
s.kamenskij@npo-echelon.ru


Эшелон
учебный центр