

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

Каменский Станислав, Специалист группы внедрения СЗИ

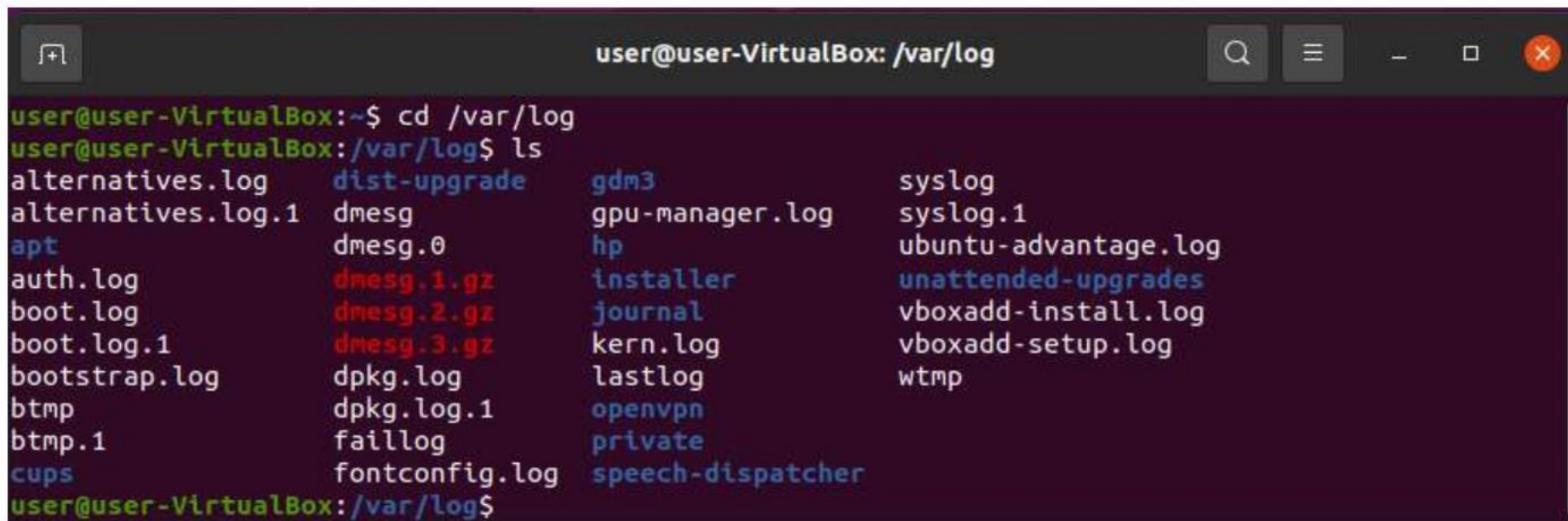


# KOMRAD troubleshooting

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`



```
user@user-VirtualBox: /var/log
user@user-VirtualBox:~$ cd /var/log
user@user-VirtualBox:/var/log$ ls
alternatives.log      dist-upgrade          gdm3                  syslog
alternatives.log.1   dmesg                 gpu-manager.log       syslog.1
apt                   dmesg.0              hp                    ubuntu-advantage.log
auth.log              dmesg.1.gz           installer             unattended-upgrades
boot.log             dmesg.2.gz           journal               vboxadd-install.log
boot.log.1           dmesg.3.gz           kern.log              vboxadd-setup.log
bootstrap.log        dpkg.log              lastlog               wtmp
btm                   dpkg.log.1           openvpn
btm.1                faillog               private
cups                  fontconfig.log       speech-dispatcher
```

# 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

```
user@user-VirtualBox: /var/log
ome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Jul 18 13:05:38 user-VirtualBox gdm-password]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: Нет такого файла или каталога
Jul 18 13:05:40 user-VirtualBox gdm-password]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: Нет такого файла или каталога
Jul 18 13:05:40 user-VirtualBox gdm-password]: gkr-pam: unable to locate daemon control file
Jul 18 13:05:40 user-VirtualBox gdm-password]: gkr-pam: stashed password to try later in open session
Jul 18 13:05:40 user-VirtualBox gdm-password]: pam_unix(gdm-password:session): session opened for user user by (uid=0)
Jul 18 13:05:40 user-VirtualBox systemd-logind[609]: New session 2 of user user.
Jul 18 13:05:40 user-VirtualBox systemd: pam_unix(systemd-user:session): session opened for user user by (uid=0)
Jul 18 13:05:41 user-VirtualBox gdm-password]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Jul 18 13:05:47 user-VirtualBox gnome-keyring-daemon[1290]: The Secret Service was already initialized
Jul 18 13:05:47 user-VirtualBox gnome-keyring-daemon[1290]: The PKCS#11 component was already initialized
Jul 18 13:05:50 user-VirtualBox dbus-daemon[576]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
Jul 18 13:05:54 user-VirtualBox polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.81 [/usr/bin/gno
me-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8)
Jul 18 13:06:10 user-VirtualBox gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Jul 18 13:06:10 user-VirtualBox systemd-logind[609]: Session c1 logged out. Waiting for processes to exit.
Jul 18 13:06:11 user-VirtualBox polkitd(authority=local): Unregistered Authentication Agent for unix-session:c1 (system bus name :1.43, object pa
th /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ru_RU.UTF-8) (disconnected from bus)
Jul 18 13:07:00 user-VirtualBox sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: Нет такого файла или каталога
Jul 18 13:07:02 user-VirtualBox sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: Нет такого файла или каталога
Jul 18 13:07:02 user-VirtualBox sudo: user : TTY=pts/0 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/apt upgrade
Jul 18 13:07:02 user-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jul 18 13:07:04 user-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Jul 18 13:07:25 user-VirtualBox sudo: user : TTY=pts/0 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/apt update
Jul 18 13:07:25 user-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jul 18 13:07:56 user-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Jul 18 13:10:06 user-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Jul 18 13:10:06 user-VirtualBox pkexec[3280]: user: Executing command [USER=root] [TTY=unknown] [CWD=/home/user] [COMMAND=/usr/lib/update-notifie
r/package-system-locked]
Jul 18 13:11:25 user-VirtualBox polkitd(authority=local): Operator of unix-session:2 successfully authenticated as unix-user:user to gain TEMPORA
RY authorization for action org.debian.apt.install-or-remove-packages for system-bus-name::1.107 [/usr/bin/python3 /usr/bin/update-manager --no-u
pdate --no-focus-on-map] (owned by unix-user:user)
Jul 18 13:17:01 user-VirtualBox CRON[12609]: pam_unix(cron:session): session opened for user root by (uid=0)
Jul 18 13:17:01 user-VirtualBox CRON[12609]: pam_unix(cron:session): session closed for user root
user@user-VirtualBox: /var/log$
```

# Что такое syslog?

Syslog это стандарт регистрации событий и их передачи

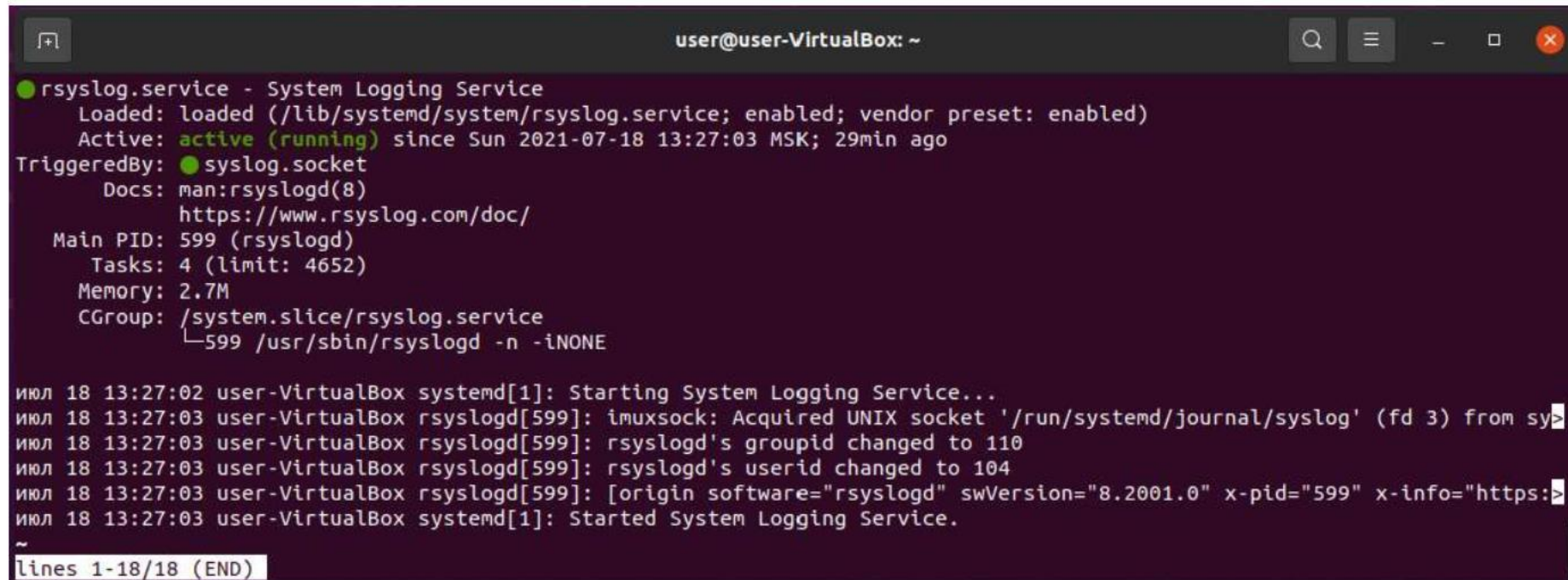
Слово “syslog” в зависимости от контекста может означать следующее:

- 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
```



```
user@user-VirtualBox: ~  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)  
   Active: active (running) since Sun 2021-07-18 13:27:03 MSK; 29min ago  
 TriggeredBy: ● syslog.socket  
   Docs: man:rsyslogd(8)  
         https://www.rsyslog.com/doc/  
 Main PID: 599 (rsyslogd)  
   Tasks: 4 (limit: 4652)  
  Memory: 2.7M  
   CGroup: /system.slice/rsyslog.service  
           └─599 /usr/sbin/rsyslogd -n -iNONE  
  
июл 18 13:27:02 user-VirtualBox systemd[1]: Starting System Logging Service...  
июл 18 13:27:03 user-VirtualBox rsyslogd[599]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from sy  
июл 18 13:27:03 user-VirtualBox rsyslogd[599]: rsyslogd's groupid changed to 110  
июл 18 13:27:03 user-VirtualBox rsyslogd[599]: rsyslogd's userid changed to 104  
июл 18 13:27:03 user-VirtualBox rsyslogd[599]: [origin software="rsyslogd" swVersion="8.2001.0" x-pid="599" x-info="https:~  
июл 18 13:27:03 user-VirtualBox systemd[1]: Started System Logging Service.  
~  
lines 1-18/18 (END)
```

# 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

The screenshot displays a monitoring dashboard with a modal window titled "Информация о событии" (Event Information) for ID 1626609400-00000e59-00000006. The modal includes a "Создать инцидент" (Create Incident) button and two tabs: "Событие" (Event) and "Контекст события" (Event Context). The "Событие" tab shows the following details:

CollectorType	syslog
Сырой текст Raw	<12>jul 18 14:56:38 user-VirtualBox gsd-color[1635]: message repeated 3 times: [ unable to get EDID for xrandr-Virtual1; unable to get EDID for output]
ID источника CollectorID	syslog 1
ID инсталляции SetupID	komrad-production
Место возникновения Producer	Не определен
IP форвардера FwdIP	192.168.88.11
ID плагинов PluginIDs	—
Время создания CTime	18.07.2021, 14:56:38
ID кластера TenantID	75

The background interface shows a timeline with a "Размер таблицы (строк)" (Table size (rows)) control set to 40. Below the timeline, there is a table for "ID источника" (Source ID) with five entries, each with a value of 1. On the right side, a "Записи" (Records) section shows a list of timestamps: 2021, 14:56:41.

# 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](mailto:s.kamenskij@npo-echelon.ru)



**Эшелон**  
учебный центр