# Proxmox Virtual Environment

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **HE** является официальной рекомендацией вендора.

## Типы собираемых событий

- Аутентификация
- Создание / Удаление LXC-контейнеров и VM (`vzcreate`, `qmcreate`, `vzdestroy`, `qmdestroy`)
- Запуск / Остановка LXC-контейнеров и VM (`qmshutdown`, `qmstop`, `vzshutdown`, `vzstop`)
- Запуск / завершение задач

## Настройка сбора событий с помощью Rsyslog

**RSyslog** — системный демон для журналирования в Linux. Он собирает события от различных источников (файлы логов, системные службы, journald) и отправляет их дальше по стандартному протоколу Syslog (UDP/TCP, а также с поддержкой TLS)

1. Проверьте статус сервиса RSyslog. Если сервис отсутствует - выполните установку пакета:

```
### Debian, Ubuntu (apt-get)
apt-get install rsyslog

### RHEL (yum)
yum install rsyslog
```

или для поддержи TLS-шифрования при отправке логов установите библиотеку **gtls** для RSyslog:

```
### Debian, Ubuntu (apt-get)
apt install rsyslog-gnutls

### RHEL (yum)
yum install rsyslog-gnutls
```

2. Запустите сервис:

```
systemctl enable rsyslog.service
systemctl start rsyslog.service
```

3.Проверьте статус:

```
systemctl status rsyslog.service
```

4. Создайте файл конфигурации для загрузки необходимых модулей `/etc/rsyslog.d/00-modules.conf`

Раскомментируйте секцию “**For journald**”. Для работы TLS: раскомментируйте секцию “**For tls**”

```
module(load="imfile")

### For tls
#module(load="gtls")
#global(DefaultNetstreamDriver="gtls")

### For journald
module(load="imjournal" StateFile="imjournal.state")
```

5. Добавьте файл конфигурации для логов `/etc/rsyslog.d/pve.conf`

```
if ($inputname == "imuxsock" and
    ($programname == "pvedaemon"
    )) then {
            action(
                name="fwd_pve_journal_tcp"
                type="omfwd"
                target="IP or FQDN" # IP or FQDN of Sysylog server (FQDN only for TLS)
                port="port" # port of Sysylog server
                protocol="tcp" # tcp or udp
                # StreamDriver="gtls" # For TLS
                # StreamDriverMode="1"  # For TLS
                # StreamDriverAuthMode="anon" # For TLS without Verification
                # StreamDriverAuthMode="x509/name" # For TLS with Verification
                # StreamDriverPermittedPeer="FQDN" # For TLS with Verification
                # tls.cacert="/etc/rsyslog/ca.crt" # For TLS with Verification
```

```
                queue.type="LinkedList"
                queue.size="10000"
                action.resumeRetryCount="-1"
        )
        stop
}
```

6. примените конфигурационные файлы RSyslog, перезапустите сервис, убедитесь в отсутствии ошибок

```
systemctl restart rsyslog.service
systemctl status rsyslog.service
```

---

Revision #5
Created 2025-11-19 12:31:33 UTC by lerat
Updated 2025-11-24 08:44:28 UTC by Boris Rzr