# PostgreSQL

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

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/help/KUMA/2.1/ru-RU/251880.htm

# Установка плагина pgAudit

Чтобы установить плагин pgAudit:

1. В командном интерпретаторе выполните команды под учетной записью с правами администратора:

```
sudo apt update
sudo apt -y install postgresql-<версия базы данных PostgreSQL>-pgaudit
```

Версию плагина необходимо выбрать в зависимости от версии СУБД PostgresSQL. Информацию о версиях СУБД PostgreSQL и необходимых версиях плагина см.по ссылке: https://github.com/pgaudit/pgaudit#postgresql-version-compatibility.

> Пример:
> `sudo apt -y install postgresql-12-pgaudit`

2. Найдите конфигурационный файл `postgres.conf`. Для этого **в командной строке СУБД PostgresSQL** выполните команду:

```
SHOW config_file;
```

В ответе будет указано расположение конфигурационного файла.

3. Создайте резервную копию конфигурационного файла `postgres.conf`.

Откройте файл `postgres.conf` и скопируйте или замените имеющиеся значения на указанные ниже.

```
## pgAudit settings
shared_preload_libraries = 'pgaudit'
## database logging settings
log_destination = 'syslog'
## syslog facility
syslog_facility = 'LOCAL0'
## event ident
syslog_ident = 'Postgres'
## sequence numbers in syslog
syslog_sequence_numbers = on
## split messages in syslog
syslog_split_messages = off
## message encoding
lc_messages = 'en_US.UTF-8'
## min message level for logging
client_min_messages = log
## min error message level for logging
log_min_error_statement = info
## log checkpoints (buffers, restarts)
log_checkpoints = off
## log query duration
log_duration = off
## error description level
log_error_verbosity = default
## user connections logging
log_connections = on
## user disconnections logging
log_disconnections = on
## log prefix format
log_line_prefix = '%m|%a|%d|%p|%r|%i|%u| %e '
## log_statement
log_statement = 'none'
## hostname logging status. dns bane resolving affect
#performance!
log_hostname = off
## logging collector buffer status
#logging_collector = off
## pg audit settings
pgaudit.log_parameter = on
pgaudit.log='ROLE, DDL, MISC, FUNCTION'
```

4. Перезапустите службу СУБД PostgreSQL при помощи команды:

```
sudo systemctl restart postgresql
```

5. Чтобы загрузить плагин pgAudit в СУБД PostgreSQL, в командной строке СУБД PostgreSQL выполните команду:

```
CREATE EXTENSION pgaudit;
```

---

# Настройка Syslog для отправки событий

Чтобы настроить передачу событий от сервера, на котором установлена PostgreSQL, в коллектор:

1. Проверьте, что на сервере источника событий установлен сервис rsyslog. Для этого выполните следующую команду:

```
sudo systemctl status rsyslog.service
```

Если сервис rsyslog не установлен на сервере, установите его, выполнив следующие команды:

```
yum install rsyslog
sudo systemctl enable rsyslog.service
sudo systemctl start rsyslog.service
```

В каталоге `/etc/rsyslog.d/` создайте файл `pgsql-to-siem.conf` со следующим содержанием:

```
If $programname contains 'Postgres' then @<IP-адрес коллектора>:<порт коллектора>
```

Если вы хотите отправлять события по протоколу TCP, содержимое файла должно быть таким:

```
If $programname contains 'Postgres' then @@<IP-адрес коллектора>:<порт коллектора>
```

В конфигурационный файл `/etc/rsyslog.conf` добавьте следующие строки:

```
$IncludeConfig /etc/pgsql-to-siem.conf
$RepeatedMsgReduction off
```

Перезапустите сервис rsyslog, выполнив следующую команду:

```
sudo systemctl restart rsyslog.service
```

# Настройка KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий pgAudit.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне pgAudit.

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] PostgreSQL pgAudit syslog.**

3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище**. Для отправки обработанных событий в хранилище.
- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

# Полезные ссылки

Настройка получения событий pgAudit (онлайн-справка KUMA):

https://support.kaspersky.com/help/KUMA/2.1/ru-RU/251880.htm

Revision #9
Created 11 August 2023 11:05:07 by Koala
Updated 7 July 2024 08:48:36 by Koala