PostgreSQL

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

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

Установка плагина pgAudit

????? ?????????? ?????? pgAudit:

1. ? ????????? ????????????? ????????? ??????? ??? ??????? ??????? ? ??????? ????????????:

```
sudo apt update
sudo apt -y install postgresql-<?????? ???? ?????? PostgreSQL>-pgaudit
```

?????? ??????? ?????????? ??????? ? ??????????? ?? ?????? ???? PostgresSQL. ?????????? ? ??????? ???? PostgreSQL ? ??????????? ??????? ??????? ??.?? ??????: https://github.com/pgaudit/pgaudit#postgresql-version-compatibility.

??????: `sudo apt -y install postgresql-12-pgaudit`

2. ??????? ???????????????? ???? `postgres.conf`. ??? ????? **в командной строке СУБД PostgresSQL** ????????? ???????:

```
SHOW config_file;
```

? ?????? ????? ??????? ???????????? ???????????????? ?????.

3. ???????? ????????? ????? ???????????????? ????? `postgres.conf`.

???????? ???? `postgres.conf` ? ?????????? ??? ???????? ????????? ???????? ?? ????????? ????.

```
## 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. ????????????? ?????? ???? PostgreSQL ??? ?????? ???????:

```
sudo systemctl restart postgresql
```

5. ????? ????????? ?????? pgAudit ? ???? PostgreSQL, ? ????????? ?????? ???? PostgreSQL ????????? ???????:

```
CREATE EXTENSION pgaudit;
```

Настройка Syslog для отправки событий

????? ????????? ???????? ??????? ?? ???????, ?? ??????? ??????????? PostgreSQL, ? ?????????:

1. ?????????, ??? ?? ??????? ????????? ??????? ?????????? ?????? rsyslog. ??? ????? ????????? ????????? ???????:

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

???? ?????? rsyslog ?? ?????????? ?? ???????, ?????????? ???, ???????? ????????? ???????:

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

? ???????? `/etc/rsyslog.d/` ???????? ???? `pgsql-to-siem.conf` ?? ????????? ???????????:

```
If $programname contains 'Postgres' then @<IP-????? ??????????>:<???? ??????????>
```

???? ?? ?????? ?????????? ??????? ?? ????????? TCP, ?????????? ????? ?????? ???? ?????:

```
If $programname contains 'Postgres' then @@<IP-????? ??????????>:<???? ??????????>
```

? ???????????????? ???? `/etc/rsyslog.conf` ???????? ????????? ??????:

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

????????????? ?????? rsyslog, ???????? ????????? ???????:

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

Настройка KUMA

????? ???? ??? ????????? ???????? ??????? ?????????, ????????? ??????? ????????? ? ???-?????????? KUMA ??? ??????? pgAudit.

1. ?? ???? **Транспорт** ??????? ??? ? ???? ? ??????????? ? ??????????? ?? ??????? pgAudit.

2. ?? ???? **Парсинг** ??????? ???????? ???????????? **[OOTB] PostgreSQL pgAudit syslog.**

3. ?? ???? **Маршрутизация** ?????????, ??? ? ????? ???????? ?????????? ????????? ????????? ????? ???????????:

- **Хранилище**. ??? ???????? ???????????? ??????? ? ?????????.
- **Коррелятор**. ??? ???????? ???????????? ??????? ? ??????????.

???? ????? ?????????? **Хранилище** ? **Коррелятор** ?? ?????????, ???????? ??.

4. ?? ???? **Проверка параметров** ??????? **Сохранить и создать сервис**.

5. ?????????? ??????????? ??????? ??? ????????? ?????????? KUMA.

Полезные ссылки

????????? ????????? ??????? pgAudit (??????-??????? KUMA):

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

Revision #10
Created 2023-08-11 11:05:07 UTC by Koala
Updated 2026-07-21 16:16:38 UTC by Koala