



Postgres Professional: путь от SDL к сертификации РБПО

Попов Валерий Викторович

Шаплов Николай Николаевич

9 лет

на рынке с 2015 г.

>20 лет

опыта в разработке PostgreSQL

>1,7 млрд руб.

объем инвестиций в развитие СУБД Postgres Pro

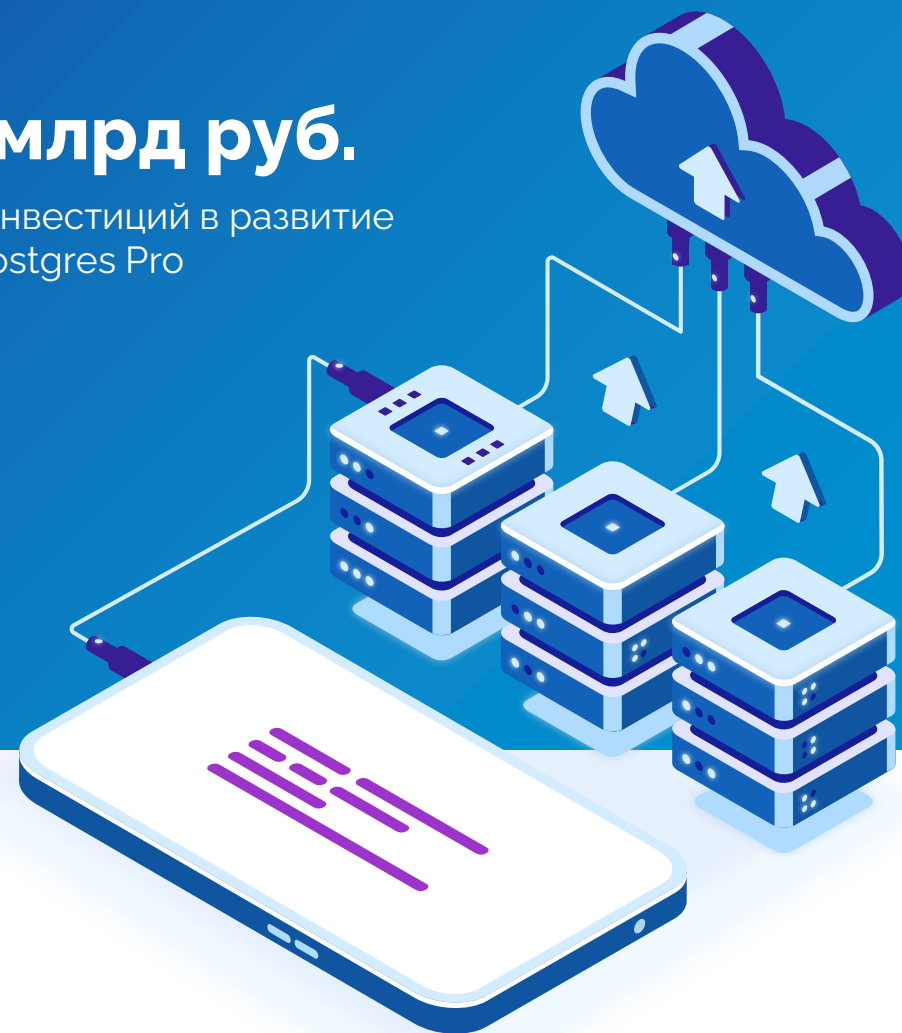
>250 чел.

штат компании

включая ведущих разработчиков и коммитеров

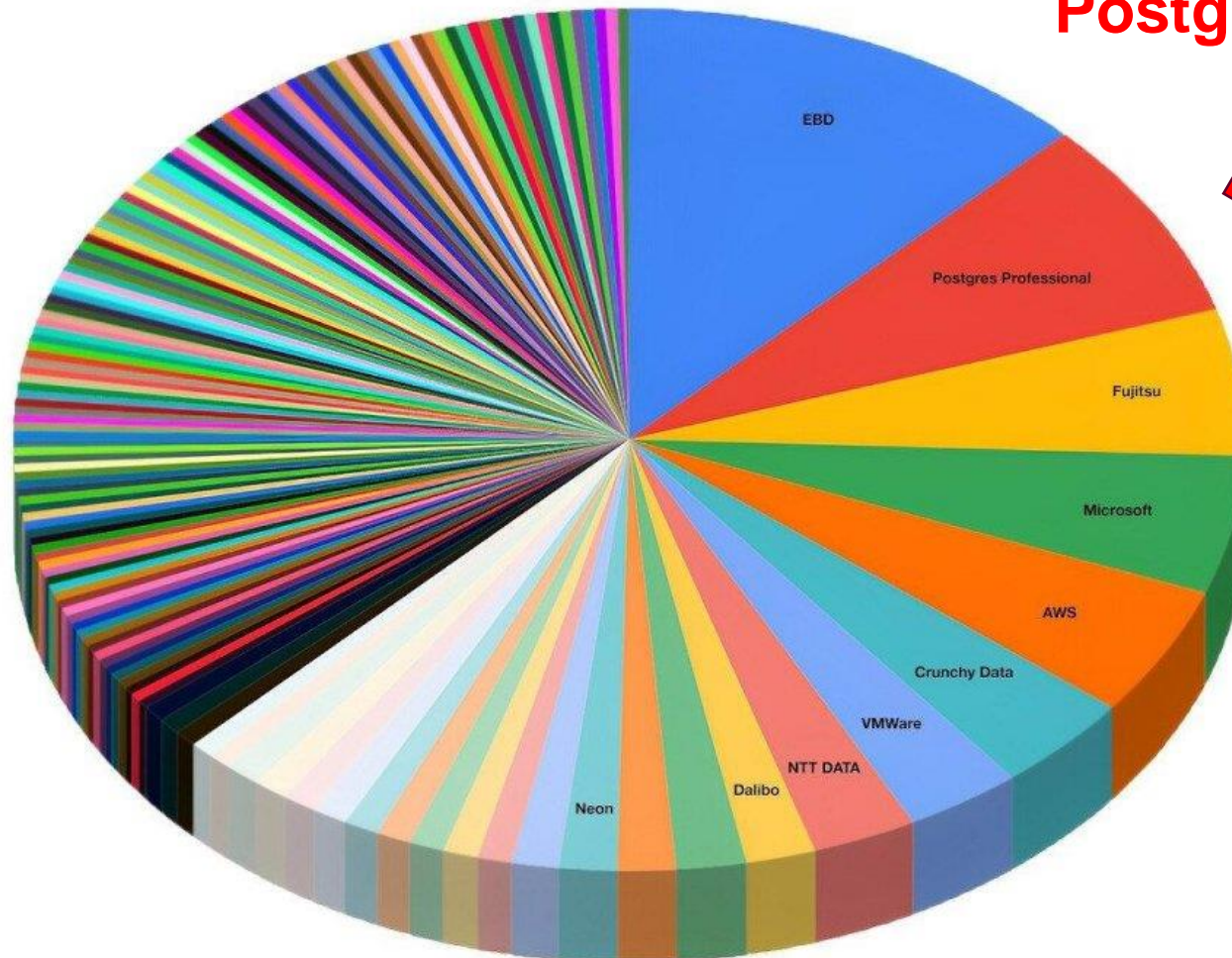
>100 патчей

направляют сотрудники компании ежегодно в международное сообщество PostgreSQL



Рейтинг контрибьютеров в PostgreSQL по данным Enterprise DB

Postgres Professional



<https://www.enterprisedb.com/blog/importance-of-giving-back-to-postgresql>

- EDB Postgres Professional Fujitsu Microsoft AWS Crunchy Data VMware NTT DATA Dalibo Timescale HighGo Neon Cybertec Adjust
- Credativ Google Kontur Materialize NTT Red Hat SRA OSS Yugabyte Aiven Instaclustr Loxodata pganalyze PostgreSQL Experts
- AD Parts Analytics Engines Anastigmatix Apple Arclion Labs Arenadata Atos Avaya Axians NL Bank of China BCL Betsys Betterment
- Bigbank Blacksmith Applications Braintree Caesars Digital Capital Rx Capsico Health CdC Citus Data Clearco Cockroach Labs Code Synthesis Tools
- Codice Lieve Cofano Software Solutions Coinbase Conova Communications GmbH CrateDB CRSCube Data Egret dbi services Deutsche Telecom Dext
- DockYard Doctolib DuckDB Labs EdgeDB End Point Corp Entelect EPAM Systems Fivetran Forest Management Institute Garner Gentoo
- GLS Bank GTT HeteroDB HP IBM ILande Illuminated Computing Index Instructure Intel Intellasoft Intezer JackDB Jampp 58 more

СУБД POSTGRES PRO

Standard

Современная СУБД, включает все новые функции PostgreSQL и полезные доработки от компании

Enterprise

Наиболее полнофункциональная СУБД с высокой производительностью и масштабируемостью

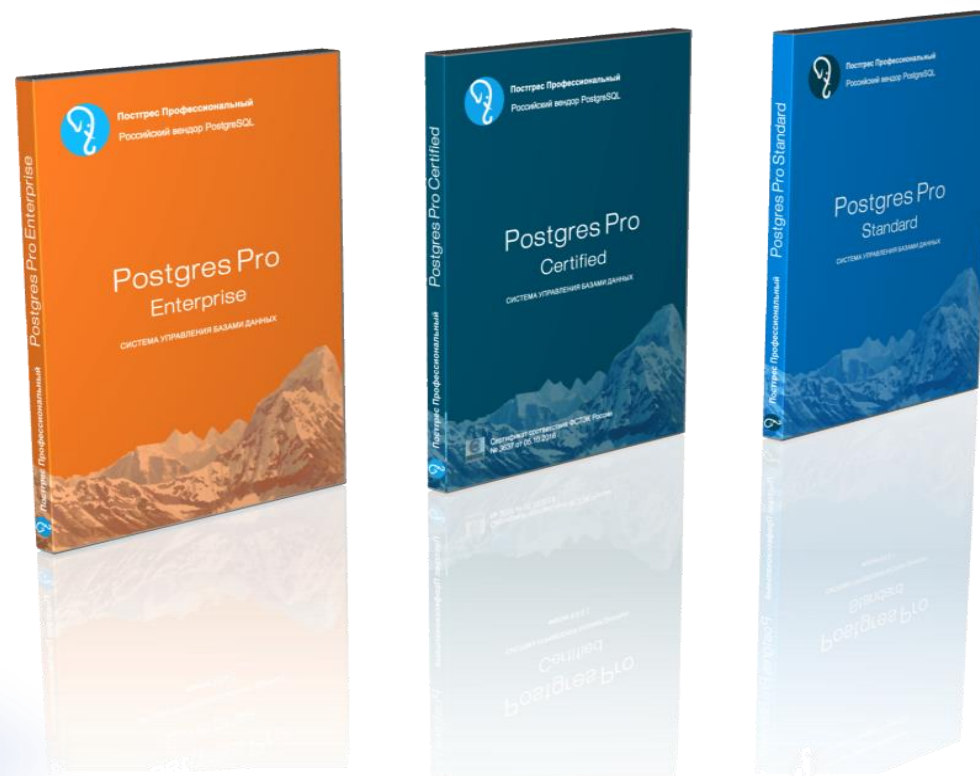
Shardman

Распределенная СУБД, предоставляющая строгие гарантии целостности данных

Certified

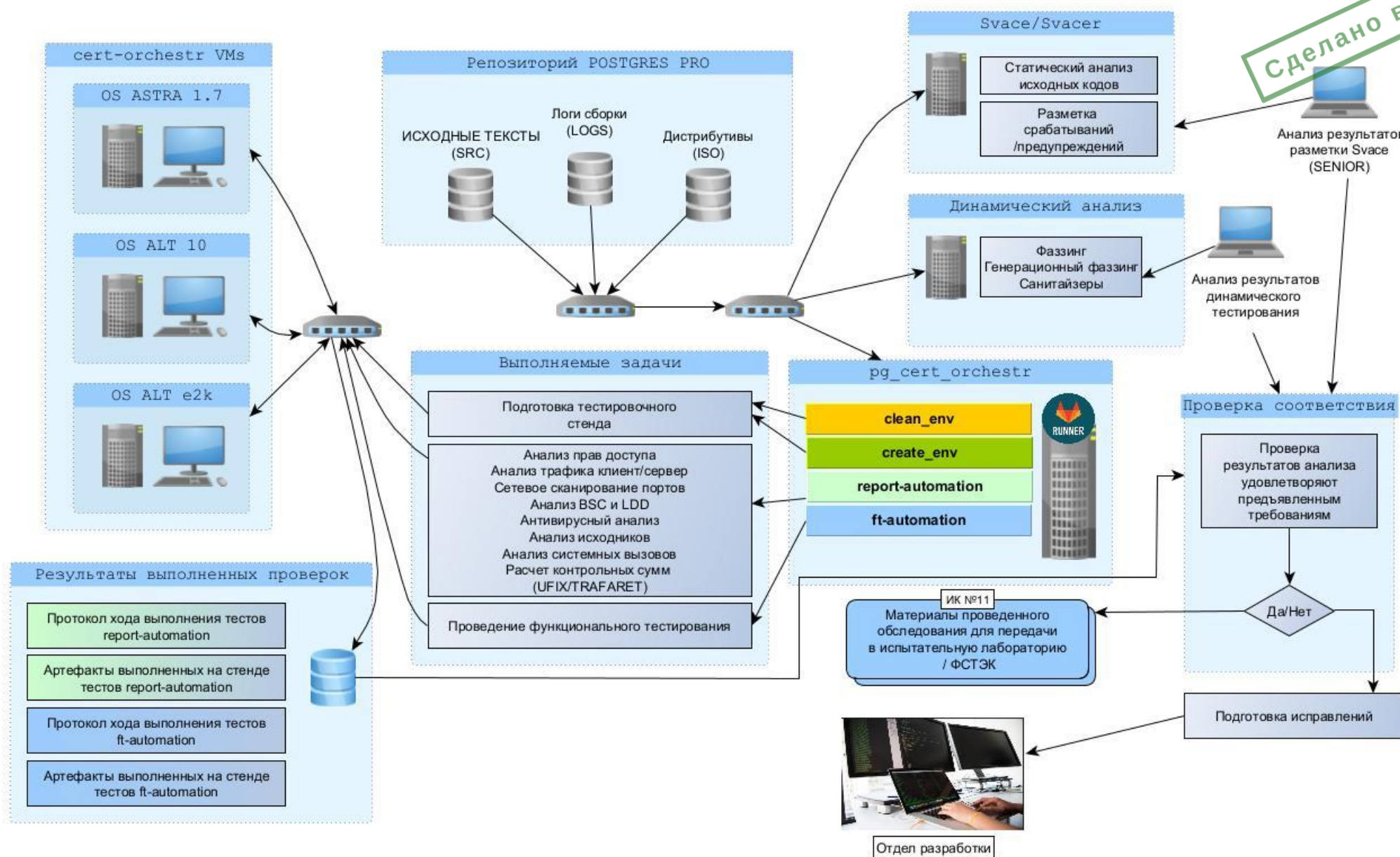
Сертифицированные ФСТЭК России версии Standard, Enterprise и Shardman. Требования к СУБД (4), УД(4)

Сделано в 2023



ПРОЦЕСС ВЫПУСКА ОБНОВЛЕНИЙ

Сделано в 2023



Элемент проверки новых релизов (ИК) Динамический анализ кода (фаззинг)

- CRUSHER, SYDR-FUZZ, AFL++
- ГЕНЕРАЦИОННЫЙ ФАЗЗИНГ Sqlancer и Squirrel
- ФАЗЗИНГ СЕТЕВОГО ПРОТОКОЛА (libpq)
- ФАЗЗИНГ input-функций типов данных (28 типов: jsonb, int, line, varchar,...)
- ФАЗЗИНГ ОПЕРАЦИЙ НАД ТИПАМИ (128 операций: Structure Aware Fuzzing)
- FUTAG: автоматическая генерация целей для libpq

LCOV - code coverage report

Current view: top level		Hit	Total	Coverage
Test: profdata.lcov	Lines:	30	88	34.1 %
Date: 2023-05-30 21:10:58	Functions:	1	7	14.3 %

Directory s	Line Coverage s		Functions s	
..futag-fuzz-drivers/PQdb/PQdb1	██████████	100.0 %	30 / 30	100.0 %
libpq/pq/src/include/libpq	██████████	0.0 %	0 / 3	0.0 %
libpq/pq/src/include/mb	██████████	0.0 %	0 / 55	0.0 %

Generated by: LCOV version 1.14

```
american fuzzy lop ++4.02c {Master} (File) [fast]
] process timing [ progress ] overall results [ progress ]
  run time : 0 days, 2 hrs, 1 min, 29 sec [x] cycles done : 591
  last new find : 0 days, 2 hrs, 1 min, 27 sec [x] corpus count : 3
  last saved crash : none seen yet [x] saved crashes : 0
  last saved hang : 0 days, 2 hrs, 1 min, 27 sec [x] saved hangs : 1
] cycle progress [ progress ] map coverage [ progress ]
  now processing : 1.591 (33.3%) [x] map density : 43.75% / 53.12%
  runs timed out : 0 (0.00%) [x] count coverage : 16.06 bits/tuple
] stage progress [ progress ] findings in depth [ progress ]
  now trying : splice 3 [x] favored items : 3 (100.00%)
  stage execs : 68/82 (82.93%) [x] new edges on : 3 (100.00%)
  total execs : 3.85M [x] total crashes : 0 (0 saved)
  exec speed : 840.0/sec [x] total tmouts : 2304 (0 saved)
] fuzzing strategy yields [ progress ] item geometry [ progress ]
  bit flips : disabled (default, enable with -D) [x] levels : 2
  byte flips : disabled (default, enable with -D) [x] pending : 0
  arithmetics : disabled (default, enable with -D) [x] pend fav : 0
  known ints : disabled (default, enable with -D) [x] own finds : 2
  dictionary : n/a [x] imported : 0
  havoc/splice : 1/1.34M, 1/2.51M [x] stability : 100.00%
  py/custom/rq : unused, unused, unused, unused [ progress ]
  trim/eff : disabled, disabled [x] [cpu000:100%]
#####
```

ФАЗЗИНГ СЕТЕВОГО ПРОТОКОЛА

Эмулирование сетевого взаимодействия

Переопределение системных функций сетевого стека. Postgres работает в однопроцессном режиме, но вместо сети общается с фаззером.

Фаззим стартовый пакет 1 (handshake) и стартовый пакет 2 – с паролем

FUTAG

Автоматически выделены и были протестированы все функции libpq

Сделано в 2023

Элемент проверки новых релизов (ИК)

Подготовка отчётных материалов (Протоколы)

The screenshot displays a LaTeX editor interface with a file explorer on the left and a document preview on the right. The file explorer shows a project structure with folders like 'REPORT-LATEX' and 'STATIC_PAGE', and files such as '00_all_in_one.tex' and '00_all_in_one.pdf'. The main editor area shows the LaTeX source code for 'report-latex > 00_all_in_one.tex', including package declarations, settings, and document structure commands. The preview window shows a document titled 'ПРОТОКОЛ № ППГ/3637/ИИ09/ПР2 испытаний' (Protocol No. PPG/3637/II09/PR2 tests) for 'Системы управления базами данных Postgres Pro' (Postgres Pro database management systems). The document content includes the title, authors, and a table of contents.

ПРОТОКОЛ № ППГ/3637/ИИ09/ПР2
испытаний
Системы управления базами данных Postgres Pro
на соответствие требованиям методического документа
«Методика выявления уязвимостей и недеklarированных возможностей в
программном обеспечении» (ФСТЭК России, 2020) –
по 4 уровню контроля

Москва
2023

Протокол № ППГ/3637/ИИ09/ПР2

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ	4
2 ОБЪЕКТ ИСПЫТАНИЙ	5
3 ЦЕЛИ ИСПЫТАНИЙ	7
4 СРЕДСТВА И УСЛОВИЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ	8
5 РЕЗУЛЬТАТЫ ИСПЫТАНИЙ	14
6 ВЫВОДЫ	270

Фаззинг: Системный подход (или куда подевалось время)

Фаззить надо так, чтобы это было легко и привычно, как «почистить зубы»



• Система автоматизации

Фаззинг — большое количество очень похожих действий, отличающихся большим количеством мелких нюансов.

- Обычные `сі`-скрипты не очень удобно;
- Избегаем дублирования кода;
- Грубая нюансировка — конфиги;
- Кастомное поведение удобно реализовывать через систему наследования ООП.

Проверено
временем

- **Поверхность патча**
- **Простота портирования**

Новые версии исследуемой программы выходят регулярно. Важно не тратить много времени на портирование фаззинг-врезок и фаззинг-модулей.

**Проверено
временем**

- **Единый каталог целей**
- **Простота добавления цели**

- Если у вас нет единой точки хранения информации о запускаемых целях, списки неизбежно разъедутся и наступит хаос;
- Добавление новой цели должно быть рутинной процедурой, потребляющей минимум ресурсов.

In Progress...

Сделано в 2023

- Сводные таблицы результатов
- Простота воспроизведения

- Что там нафаззилось - интересно смотреть в первый раз. На десятый не интересно совсем. Чтобы не пропустить важные результаты, отчет для инженера должен быть простым, содержательным и наглядным.
- Для срабатываний:
 - Собрать максимум отладочной информации автоматически
 - Сделать напоминалку как запускать руками
 - Как добиться аналогичного эффекта на большом postgres'e (SQL, netcat)

Сделано в 2023

Сделано в 2023


• Процедура передачи бага


Найденный баг должен быть праздником для фаззингиста. Если приходится биться за то, чтобы найденный баг взяли в работу, если багу никто не рад, фаззингист не захочет ничего находить.

In Progress...

Протестировать
СУБД Postgres Pro:



 117036, Москва, ул. Дмитрия Ульянова, 7А

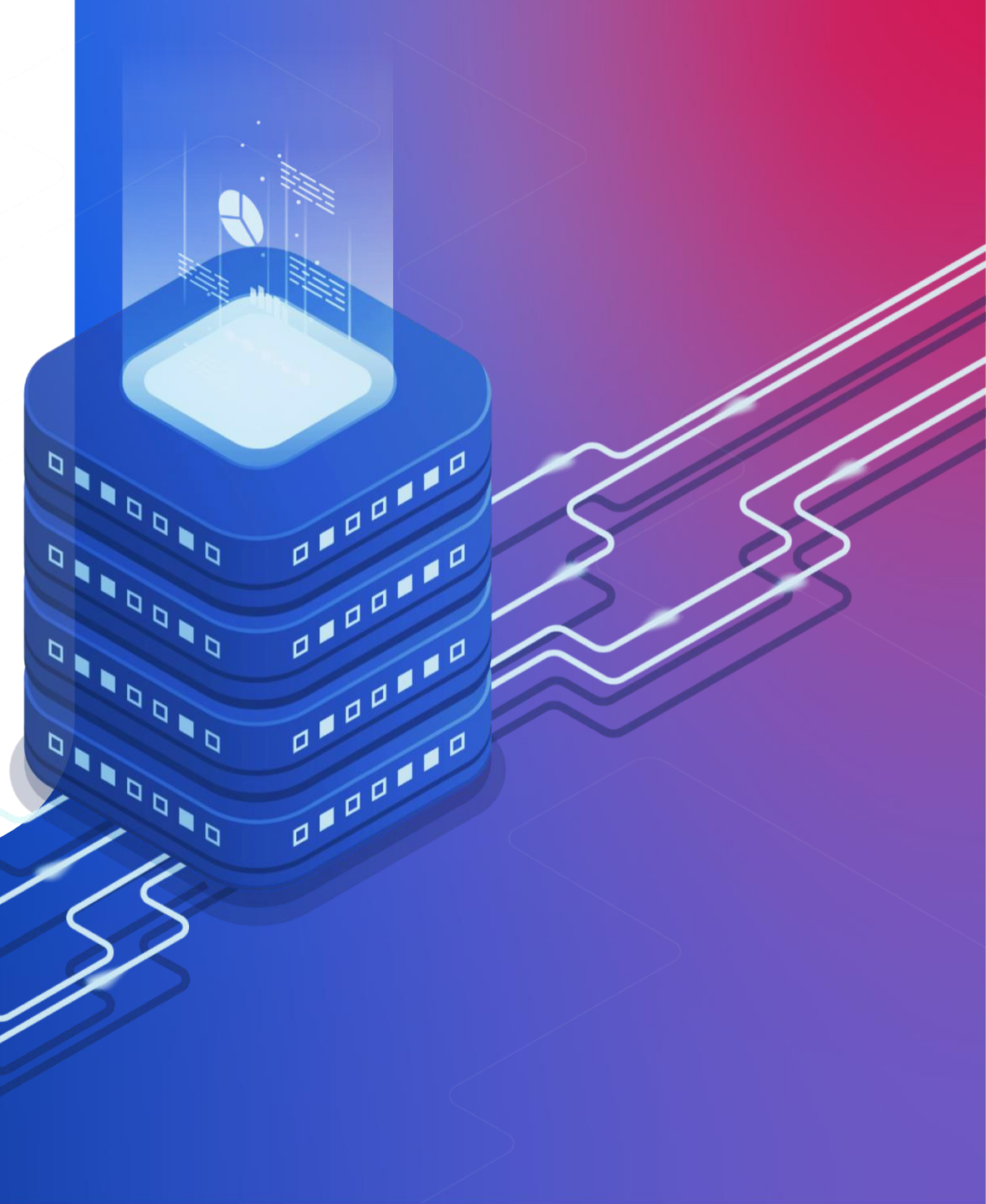
 8 (495) 150-06-91

 sales@postgrespro.ru

postgrespro.ru

PosgresPro

Спасибо
за внимание!



PostgresPro

Q & A

