PostgresPro

Как мы научились сертифицировать по 40 релизов постгреса в год

Валерий Попов,

Руководитель отдела ИБ Postgres Professional

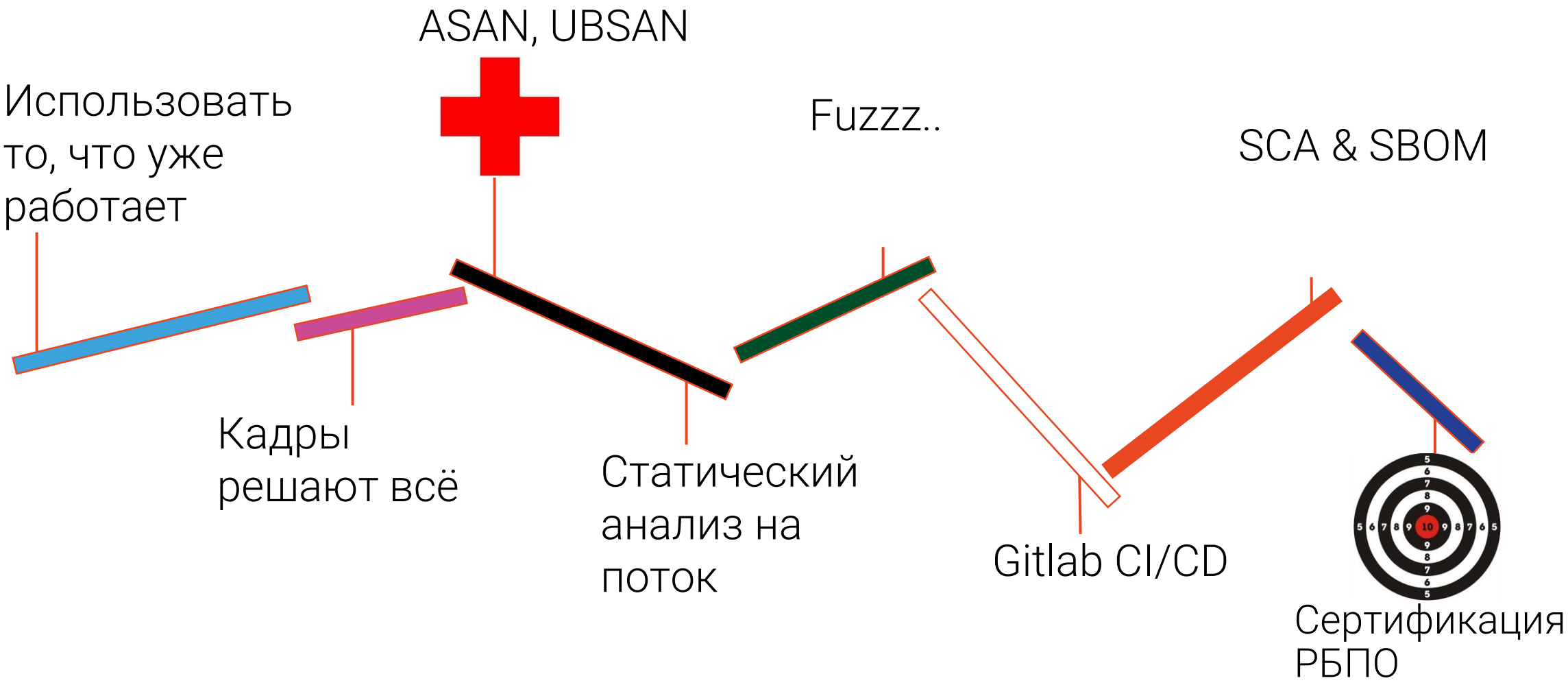
PostgresPro

Попов Валерий

Руководитель отдела ИБ компании Postgres Professional

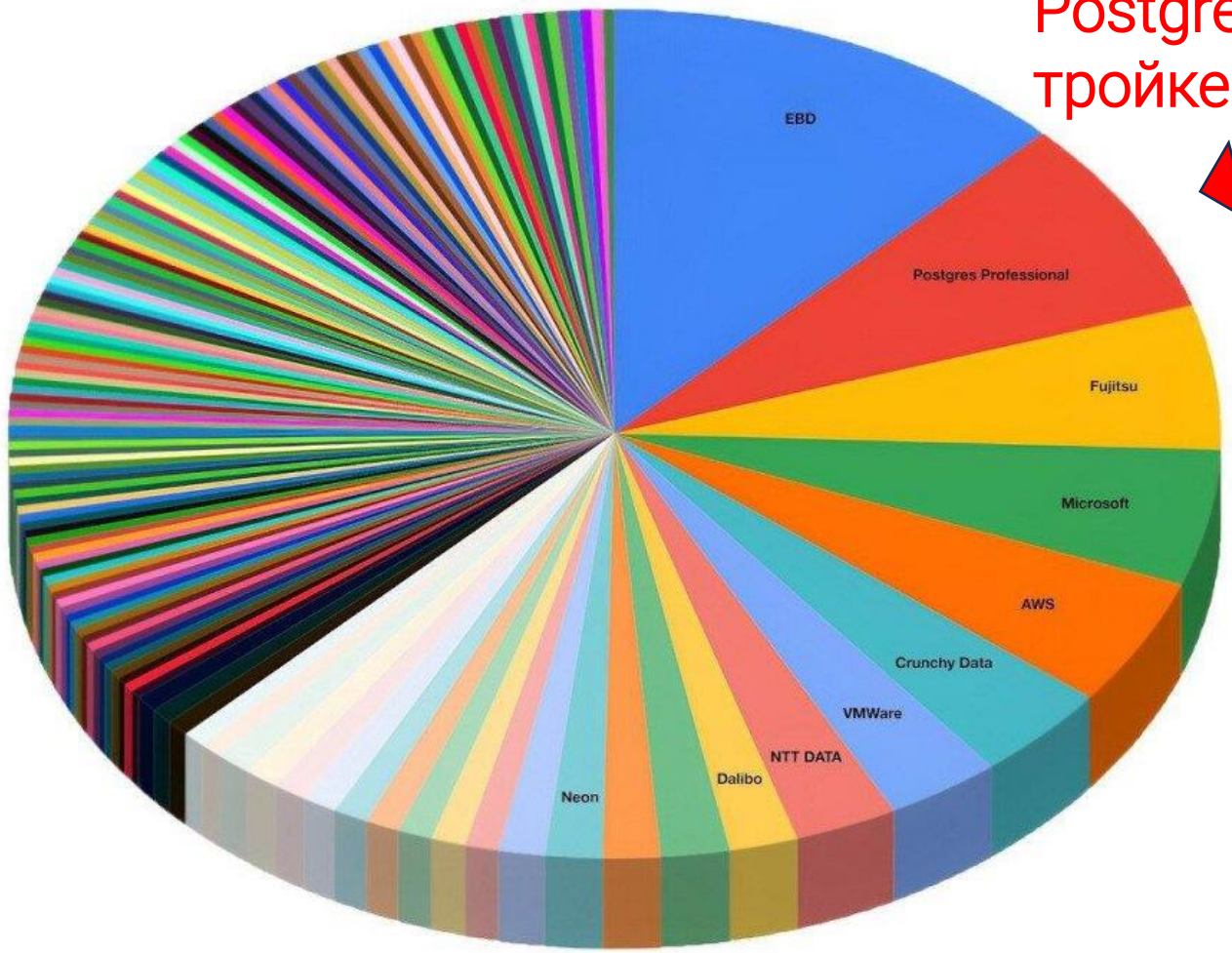
PostgresPro

О чем будем говорить (этапы внедрения РБПО)



Рейтинг контрибьютеров в PostgreSQL-15 по данным Enterprise DB

Postgres Professional в тройке лидеров!



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 Arcion 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

PostgresPro

Исследования «ванильного» PostgreSQL

SYNOPSYS® My Dashboard FAQ OSS Success Stories Projects Using Scan About Community v.popov@postgrespro.ru

Projects on Coverity Scan

Did you know Coverity Scan found XSS security vulnerability in

PostgreSQL_REL_16_STABLE	1,825,268	C/C++
Postgres	1,203,170	C/C++
Postgres Pro	1,323,387	C/C++

https://coverage.postgresql.org

Импорт закладок... Начальная страница Часто посещаемые PostgreSQL: Security I... Most Visited Getting Started RSS-лента новостей ... RSS-лента новостей ... Comments on Бизнес... Портал закупок Другие закладк

LCOV - code coverage report

Current view: top level
Test: PostgreSQL 18devel
Date: 2024-09-22 09:11:47
Legend: Rating: low: < 75 % medium: >= 75 % high: >= 90 %

	Hit	Total	Coverage
Lines:	408928	515934	79.3 %
Functions:	24669	27616	89.3 %

Directory	Line Coverage		Functions	
contrib/amcheck	73.8 %	1087 / 1473	96.2 %	51 / 53
contrib/auth_delay	0.0 %	0 / 13	0.0 %	0 / 3
contrib/auto_explain	89.3 %	92 / 103	100.0 %	6 / 6
contrib/basebackup_to_shell	86.5 %	90 / 104	100.0 %	14 / 14

PostgresPro

Исследования «ванильного» PostgreSQL

oss-fuzz / projects / postgresql / **fuzzer** /

DavidKorczynski postgresql: fix build (#8963) e04e7b4 · 2 years ago History

Name	Last commit message	Last commit date
..		
Makefile	postgresql: fix build (#8963)	2 years ago
dbfuzz.c	[Postgresql] Added initialization parts to fuzzers (#4357)	4 years ago
fuzzer_initialize.c	postgresql: fix build (#8963)	2 years ago
json_parser_fuzzer.c	[PostgreSQL] Fix startup crashes (#4430)	4 years ago
protocol_fuzzer.c	postgresql: fix build (#6570)	3 years ago
simple_query_fuzzer.c	postgresql: fix build (#8963)	2 years ago

PostgresPro

О кадрах

- Нужных специалистов нужно выращивать самим
- Глубокое понимание кода и принципов работы необходимы для проведения статического анализа и фаззинга

PostgresPro

О санитайзерах

```
$ CC=clang-11 CXX=clang++-11 CFLAGS="-fsanitize=address" CXXFLAGS="-
fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --enable-tap-tests --
enable-debug
```

```
=================================================================
==1998448==ERROR: AddressSanitizer: odr-violation (0x000002c157a0):
  [1] size=1 'trace_sort' src/tuplesort11.c:130:7
  [2] size=1 'trace_sort' tuplesort.c:131:7
```

Эффективно помогает находить проблемные места

PostgresPro

Статический анализ

Нужна квалификация senior

Разметили весь код, дальше - легче

Автоматическое создание задач в Jira на исправление

Охватываем все проекты

DEREF_OF_NULL.RET.ALLOC

Checker_severity: **Normal**
Checker_reliability: **High**
DEREF_OF_NULL.RET.ALLOC
Reviewed by: k.baranov
postmaster.c
Svacer link

```
Message:
Pointer '&port->remote_port[0]', returned from function 'strdup' at postmaster.c:4381,
may be NULL and is dereferenced at postmaster.c:4473.
```

Attachments

Drop files to attach, or browse.

Issue Links

is duplicated by

~~SDL-1137~~ Svace | postmaster.c — CLOSED

~~SDL-1141~~ Svace | postmaster.c — CLOSED

relates to

~~PGPRO-12025~~ Returned from function strdup may be NULL in postm... — DONE

PGPRO-12100 Пропихнуть в ваниллу исправление Returned from f... — BACKLOG

О фаззинге

- CRUSHER, SYDR-FUZZ, AFL++
- ГЕНЕРАЦИОННЫЙ ФАЗЗИНГ Sqlancer и Squirrel
- ФАЗЗИНГ СЕТЕВОГО ПРОТОКОЛА (libpq)
- ФАЗЗИНГ input-функций типов данных (jsonb, int, line, varchar,…)
- ФАЗЗИНГ ОПЕРАЦИЙ НАД ТИПАМИ (Structure Aware Fuzzing)

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	Line Coverage		Functions	
.futag-fuzz-drivers/PQdb/PQdb1	100.0 %	30 / 30	100.0 %	1 / 1
libpg/pg/src/include/libpg	0.0 %	0 / 3	0.0 %	0 / 1
libpg/pg/src/include/mb	0.0 %	0 / 55	0.0 %	0 / 5

Generated by: LCOV version 1.14

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

SCA & SBOM

- trivy
- cdxgen
- CodeScoring
- Проверяем все проекты >80

Total 81 items

Project	Start date	Last updated
ee-manager-gui	–	31.01.2025
plpgsql_check 2.5.3	–	31.01.2025
etcd	–	31.01.2025
plpgsql_check 2.7.12	–	31.01.2025
goppem	–	31.01.2025
pg_probackup_ee-astra1.8	–	31.01.2025
shardman-utils	–	31.01.2025
plpgsql_check 2.5.2	–	31.01.2025
etcd 3.5.18	–	31.01.2025

Thank you for reporting these issues.

We will take a look and fix it as soon as possible.

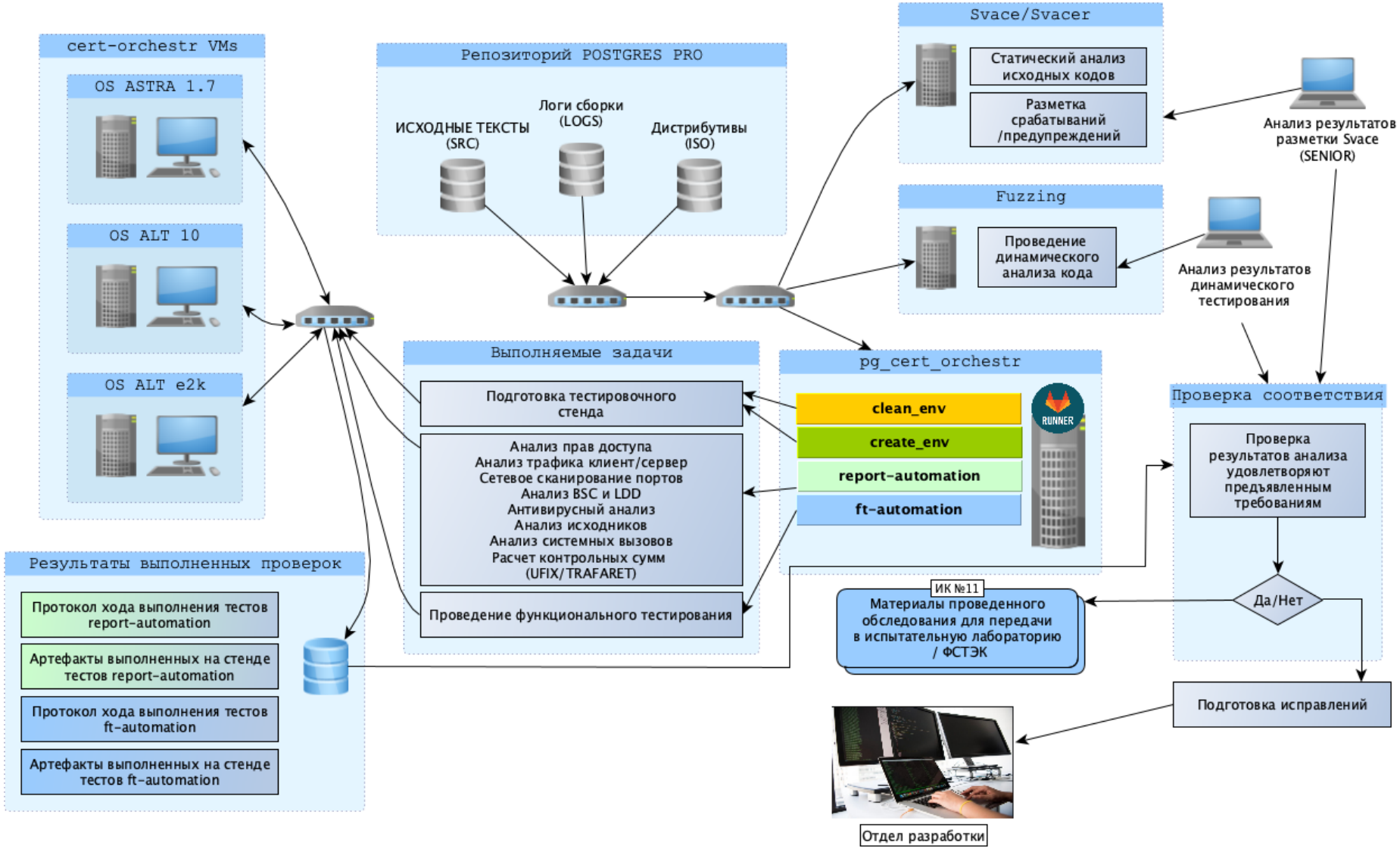
Adding @ivan@vald.es

Regards,
Benjamin

On Fri, Jan 31, 2025 at 1:34 PM 'Коротков Максим' via etcd-maintainers <etcd-maintainers@googlegroups.com> wrote:

> Hi, in version 3.5.18, the OSA vulnerability scanner found several vulnerable dependencies.
> CVE-2024-45339, GO-2025-3372 - github.com/golang/glog v0.0.0-20160126235308 - fixed 1.2.4
> CVE-2021-20329 - go.mongodb.org/mongo-driver@v1.3.0 - fixed 1.5.1
> ---
> Best regards, Maksim Korotkov
> Postgres Pro

Процессы сертификационных испытаний Postgres Pro



Спасибо за внимание!

v.popov@postgrespro.ru