PostgreSQL и информационная безопасность

Чего не будет в докладе

- Человеческий фактор (Gitlab)
- Защита от физического доступа к железу
- Аппаратные уязвимости
- Уязвимости ОС
- Сеть

О чем тогда доклад?

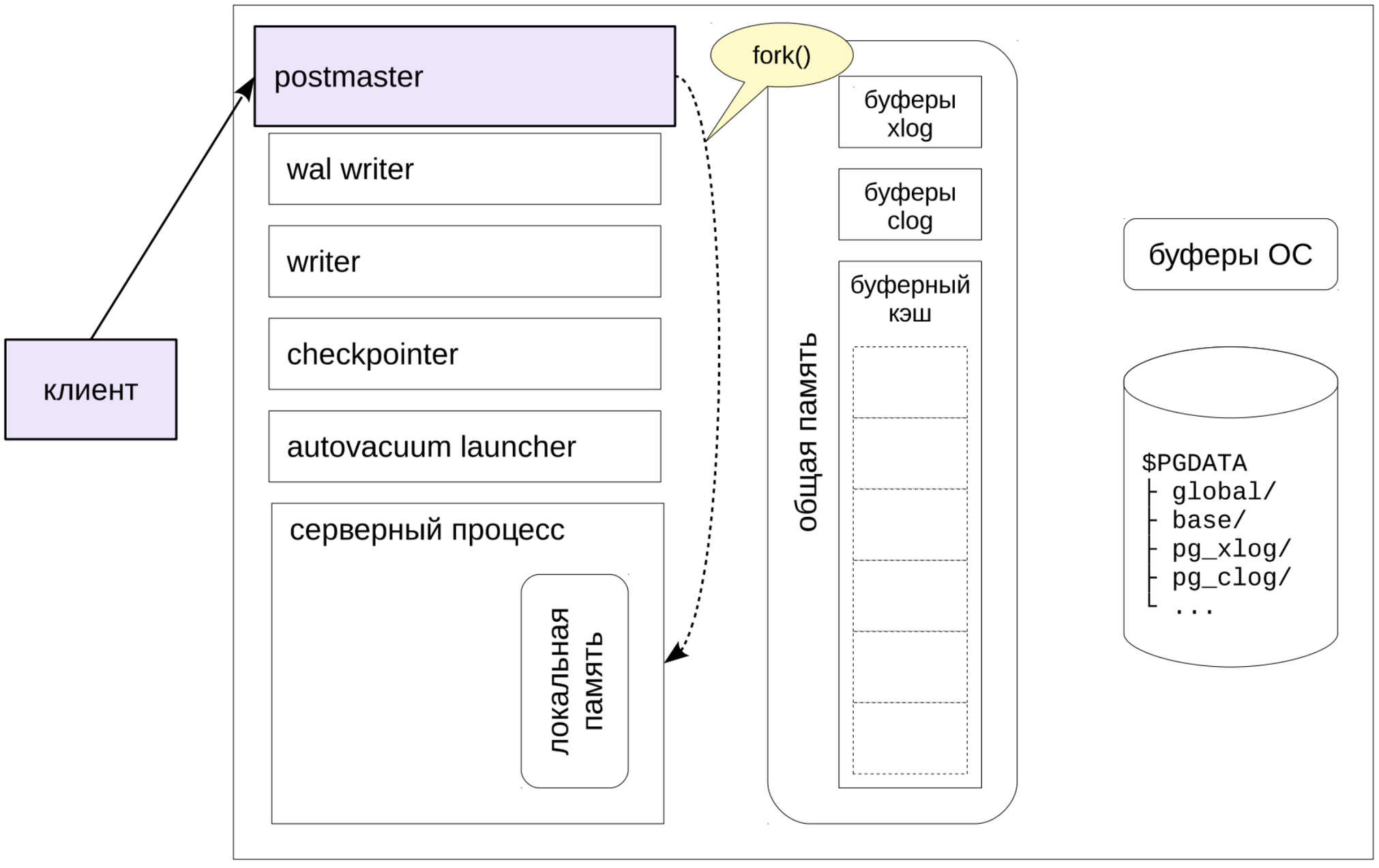
- Анализ архитектуры СУБД (модули)

- Оценка ИБ каждого модуля

СУБД под капотом

- Процессы (треды)
- Файлы
- Клиент-серверный протокол
- Внутреннее представление данных

Схема работы PostgreSQL



Безопасность процессов

- Непривилегированный пользователь ОС
- OOM killer (vm.overcommit_memory=2)
- Безопасность процессов и разделяемой памяти на ОС и коде pg

Интересные файлы и каталоги в PostgreSQL

- $PGDATA
    - global
    - base
    - pg_wal (pg_xlog)
- Настройки
    - pg_hba.conf
    - pg_ident.conf
    - postgresql.conf
- Логи
- Расширения = $(pg_config —sharedir)/extension + $(pg_config --bindir)/../lib
- Дампы
- Мгновенные снимки ФС (btrfs, overlayfs)

Безопасность файлов

- Минимальные права все на каталоги и файлы ($pgdata - 700)
- Помнить про WAL, дампы, снимки ФС (мастер, реплики, архивы PITR, компьютеры разработчиков)
- Бэкапы настроек (не только WAL)
- Не забывать про вынесенные tablespace
- Безопасность файловых кэшей делегирована ОС

Клиент-серверный протокол

- TCP/IP и доменные сокеты UNIX (порт 5432)
- Аутентификация клиента (pg_hba.conf)
- SSL
- Запросы (простые, расширенные, функции, copy)

Файрвол и настройки подключения

- Политика DROP
- Минимальный набор портов и протоколов (icmp)
- listen_addresses + pg_hba.conf (trust/gssapi/sasl…)
- VPN или SSL в PostgreSQL

Клиент-серверный протокол и SQL инъекции

- SQL инъекции возникают при конструировании запроса из блоков (шаблонизаторы SQL/параметры как текст)

- Протокол «простых запросов»
    - SQL как текстовая строка
    - разбор запроса - план - выполнение
- Протокол «расширенных запросов»
    - SQL + подготовленные типизированные параметры
    - разбор запроса - подготовка оператора - привязка параметров (создание портала) - план - выполнение

Безопасная разработка схемы БД

- Работа с отключенным автокоммитом
- Схема в системе контроля версий
- Миграции Dev - Test - Production
- Принцип минимальных прав на объекты схемы
- DB owner != cluster superuser
- pgcrypto

Безопасные паттерны схемы БД

- Работа с таблицами через функции и представления
  - security definer, stable/volatile/immutable
  - пользователь БД != пользователь приложения (пулы соединений)
- Безопасность на уровне строк
  - политики безопасности строк в таблице
  - герметичные функции

Расширения, доступ к ФС

- Загружаются в разделяемую память процессов pg
- Классическая проблема доверия пакетам
- Небезопасные языки и copy (superuser only)
    - доступ к ФС из-под postgres (rm $pgdata)
    - copy (select 123) to program 'whoami > /tmp/111’;

Благодарю за внимание

https://habrahabr.ru/users/darthunix
telegram: @darthunix