PostgresPro

1С PREMIUM

PGMeetup:
Решение вопросов ИБ в приложениях 1С, развернутых на СУБД Postgres Pro

Андрей Гусаков и Виталий Замлынский

13.05.2025

Представляем участников PGMeetup

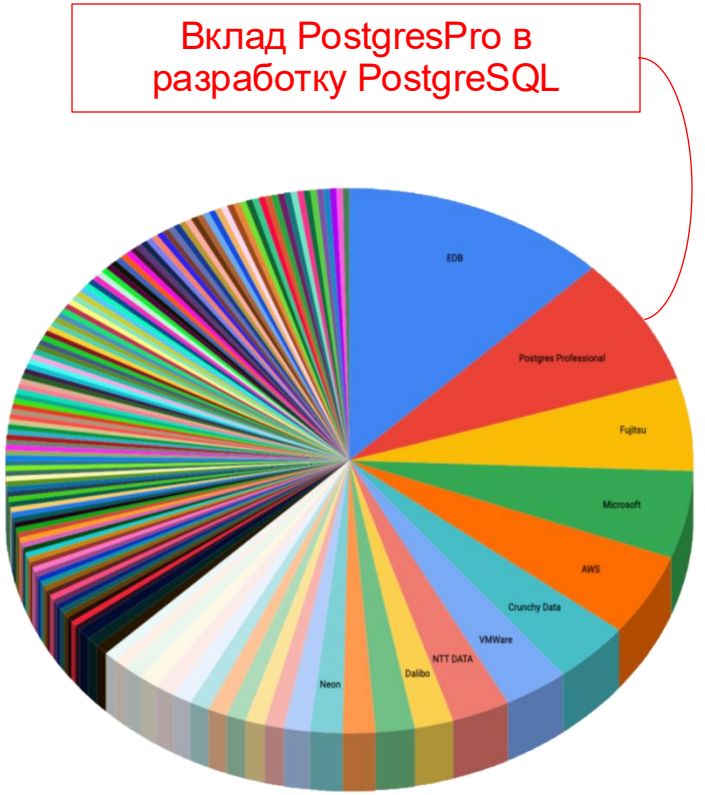
- Компания «1С-Премиум», дочерняя структура фирмы «1С»,
  - Оказывает Премиальную поддержку крупным заказчикам для обеспечения повышения качества развития и эксплуатации решений 1С на корпоративном рынке
  - Имеет широкий портфель сервисов (в том числе для поддержки работы СУБД PostgreSQL)
- Команда состоит из сертифицированных экспертов PostgreSQL и 1С

- Клиенты компании: «Газпром нефть», «Северсталь», «Таграс», «X5», «Альфа-страхование», машзавод «Красный Октябрь», ГК «Детский мир» и др.

1c-prem.ru

Представляем участников PGMeetup

- ООО "Постгрес Профессиональный" – разработчик и правообладатель ПО класса СУБД на основе PostgreSQL в соответствии с реестровой записью №104 от 18.03.2016 в reestr.digital.gov.ru
- ООО «Постгрес Профессиональный» является обладателем лицензии ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации (см. reestr.fstec.ru/reg2)
- Сертификация (подтверждение характеристик) проводится с 2016 года; сейчас – по «Требованиям по безопасности информации к системам управления базами данных», утвержденным приказом ФСТЭК России от 14 апреля 2023 г. N 64, самого высокого для защиты конфиденциальной информации четвертого класса защиты и уровня доверия (продукту и его производству)
- Postgres Pro – контрибьютер #2 в код PostgreSQL в мире (после EnterpriseDB); 17 версия вышла в ноябре 2024 г. для STD и в конце декабря 2025 г. для ENT-релизов
- Совместимость ПО – это crowdtesting + дальнейшее развитие и поддержка + заплатки для устранения уязвимостей (см. postgresql.org/support/security)



Для 1С:Предприятие разработчиками компании Postgres Professional во все сборки включены в поставку...

PostgresPro

Специальный набор патчей (1c support patches):

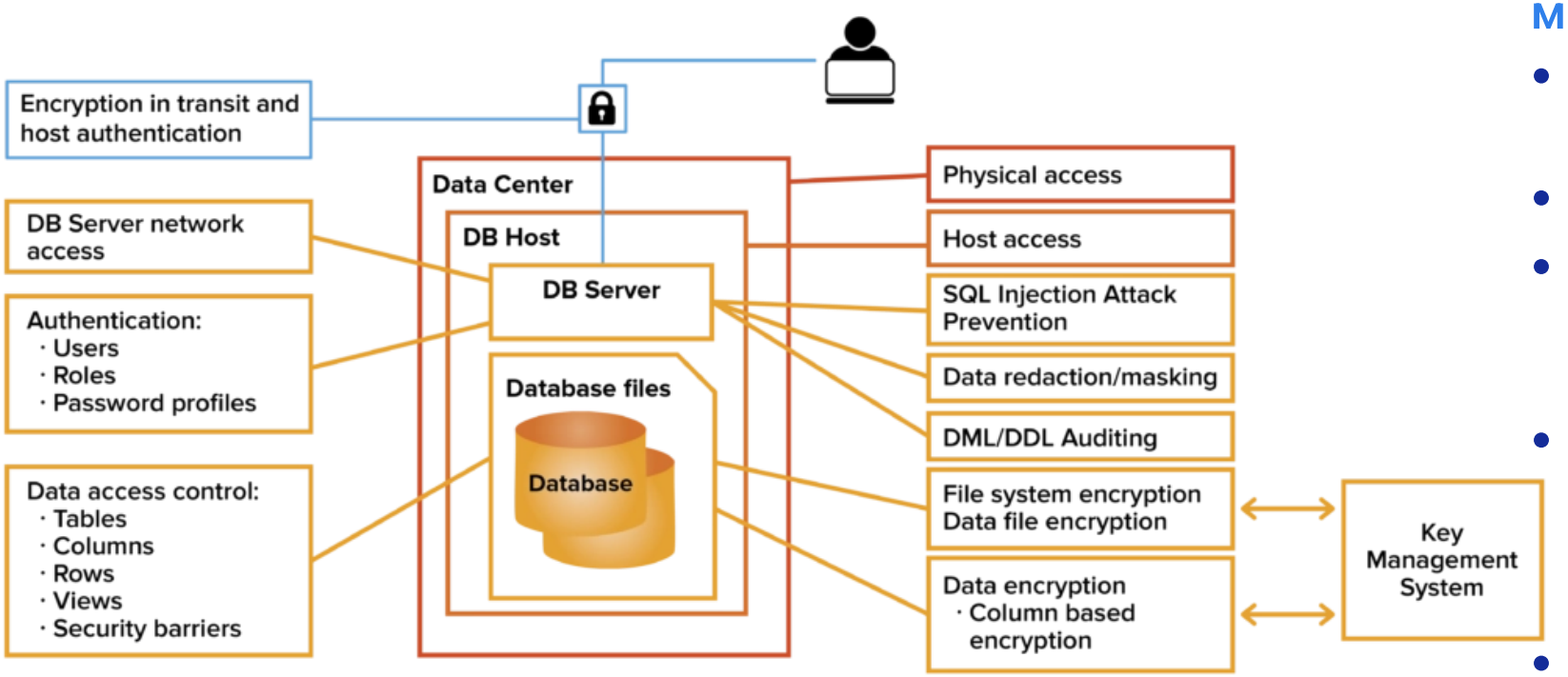
- Два необходимых режима блокировок: APPLICATION SHARE и APPLICATION EXCLUSIVE
- Оптимизация работы с оператором OR

а также специальные Расширения для работы 1С :

- модуль fasttrun, который предоставляет транзакционно-небезопасную функцию для усечения временных таблиц, что предотвращает разрастание каталога pg_class,
- модуль fulleq, предоставляющий дополнительный оператор равенства для совместимости с Microsoft SQL Server,
- модуль mchar, предоставляющий дополнительный тип данных для совместимости с Microsoft SQL Server,
- модуль plantuner, добавляющий поддержку указаний для планировщика, подключающих или отключающих определённые индексы при выполнении запроса

Все эти модули разработаны сотрудниками нашей компании

Подход к организации защиты СУБД



В PostgreSQL имеется множество решений ИБ:

- Ролевая модель управления привилегиями
- Row Level Security
- Безопасность подключений (диапазон IP, порты, таймауты, SSL)
- Идентификация и аутентификация пользователей (пароли, LDAP, cert, Kerberos)
- Встроенный аудит (журнал событий)
- Встроенная криптозащита (пароли, столбцы, на стороне клиента)

itopstimes.com/itsec/creating-a-multi-layered-security-architecture-for-your-databases

Почему этого недостаточно для защиты информации?

- Проблема суперпользователя – бесконтрольность, невозможность отследить опасные действия, риски использования superuser для работы сервисов
- Проблема доступа к чувствительным данным привилегированных пользователей
- Для маскирования данных надо применять внешние утилиты/расширения
- Недостаточная гибкость аудита и повышенная нагрузка от него на СУБД
- Риски безопасности при несанкционированном изменении файлов СУБД
- Неудобная криптография – непрозрачно для приложений, утилит, имеются уязвимости

- Растущие требования регуляторов – к распределению обязанностей, к сложности пароля и таймаутам, к перечню и содержимому регистрируемых событий безопасности, к очистке памяти

Применяем средства защиты к СУБД для 1С

(теория)

Контроль привилегированных пользователей

PostgresPro

Задача – снизить вероятность того, что суперпользователь в одиночку выполнит несанкционированные действия

Использование запретительного подхода сохраняет лазейки для обхода ограничений, т.к. не существует всеобъемлющего списка того, что у суперпользователя нужно отобрать

Минимальный набор прав обычного пользователя

Набор прав суперпользователя

Контроль привилегированных пользователей

Задача – снизить вероятность того, что суперпользователь в одиночку выполнит несанкционированные действия

Использование запретительного подхода сохраняет лазейки для обхода ограничений, т.к. не существует всеобъемлющего списка того, что у суперпользователя нужно отобрать

Минимальный набор прав обычного пользователя

Набор прав суперпользователя

Используем разрешительный подход:

- Создадим администратора БД для настройки конкретной БД
- Создадим администратора СУБД для настройки экземпляра СУБД

root: edit pg_hba.conf
auth type = reject
chown root & chmod 640

- Временно заблокируем суперпользователя с помощью администратора инфраструктуры

- Установим правила журналирования любых действий с пользователями, изменений конфигурации СУБД, изменений хранимых процедур, любых DDL
- Воспользуемся бэкпортом кода (*) из 16-й версии

	13*	14*	15*	16
Postgres Pro Standard		14.10.1+	15.5.1+	16.1.1+
Postgres Pro Enterprise	13.13.1+	14.10.1+	15.5.1+	16.1.1+

Разграничение прав администраторов – реализация

PostgresPro

- Создание роли администратора СУБД
  - Выполняется от имени суперпользователя
  - Выдача системных привилегий: CREATEDB, CREATEROLE, REPLICATION
  - Выдача функциональных привилегий на большой набор предопределённых ролей и системных функций (см. следующий слайд)
- Типовые обязанности администратора СУБД
  - Создаёт новые БД
  - Создаёт пользователей – администраторов БД
  - Создаёт tablespaces
  - Меняет настройки СУБД
  - Создаёт пользователей для репликации
  - Управляет репликацией
- Создание роли администратора БД
  - Выполняется от имени администратора СУБД
  - Выдача системных привилегий: CREATEROLE
  - Выдача функциональных привилегий: мини-набор предопределённых ролей (см. следующий слайд)
- Типовые обязанности администратора БД
  - Создаёт таблицы и хранимые функции в БД (т.к. обычным пользователям запрещены любые изменения кода информационных систем [CREATE]; они не могут создавать или изменять код хранимых процедур, функций, пакетов, триггеров)
  - Создаёт пользователей БД
  - Резервное копирование и восстановление своей БД

«Замена» суперпользователя администратором СУБД...

PostgresPro

- При создании Администратора СУБД ему выдаются права на следующие предопределенные роли:

и администратором БД

- pg_read_all_settings
- pg_read_all_stats
- pg_stat_scan_tables
- pg_monitor

чтение различных полезных параметров конфигурации, статистики и другой системной информации

- pg_signal_backend
- pg_checkpoint

выполнение экстренных действий на уровне инстанса

- *pg_create_tablespace* *(разработка PostgressPro, не*
- *pg_manage_profiles* *требует прав суперпользователя)*

создание табличных пространств и управление профилями

- ... и на системные функции:
  - pg_reload_conf()
  - pg_rotate_logfile()

управление конфигурацией и логированием

  - pg_create_restore_point()
  - pg_backup_start()
  - pg_backup_stop()

управление бэкапированием и восстановлением

  - pg_switch_wal()
  - pg_promote()
  - pg_wal_replay_pause()
  - pg_wal_replay_resume()

управление журналом предзаписи и репликацией

habr.com/ru/companies/postgrespro/articles/788268/

Как ставить недоверенные расширения без superuser?

PostgresPro

- Расширение состоит из управляющего файла и минимум одного SQL-скрипта; оно может быть доверенным или недоверенным. Установка недоверенного расширения обычно требует привлечения суперпользователя...
- Используем то, что trusted-расширение ставится от имени postgres; и при этом SQL-файлы расширения выполняются от супер-пользователя без его login к базе, внутренними механизмами
- Безопасность достигается необходимостью вовлечения нескольких человек в установку расширения: Администратора СУБД и Администратора инфраструктуры (на схеме – System Security Admin)

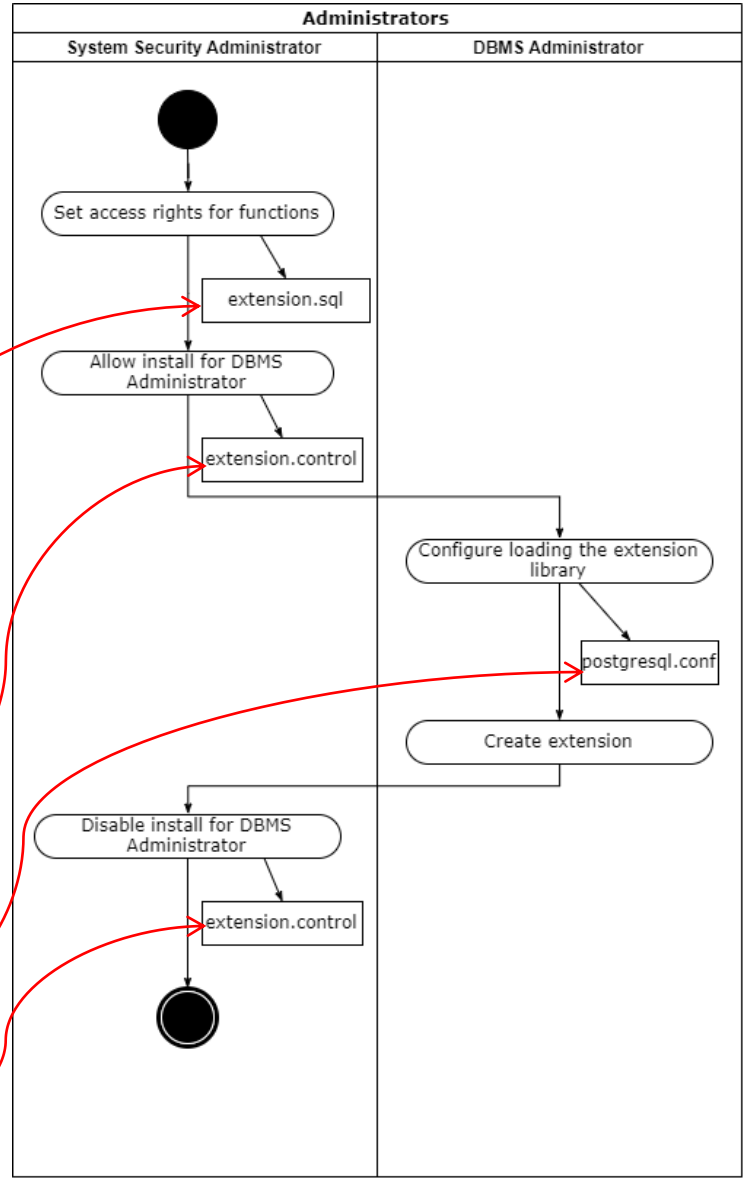
Пример выдачи разрешения Администратору СУБД для установки расширения pg_proaudit

```
-- Create new versions of objects
CREATE FUNCTION pg_proaudit_show()
RETURNS TABLE(
  db_name text,
  event_type text,
  object_type text,
  object_oid oid,
  role_name text)
AS 'MODULE_PATHNAME', 'pg_proaudit_show_conf'
LANGUAGE C VOLATILE;
REVOKE ALL ON FUNCTION pg_proaudit_show() FROM PUBLIC;
GRANT ALL ON FUNCTION pg_proaudit_show() TO PGPRO_DBMS_ADMIN;
```

trusted = true

add file to shared_preload_libraries + systemctl restart postgresql

trusted = false



Видео

Установка расширения pg_proaudit без суперпользователя

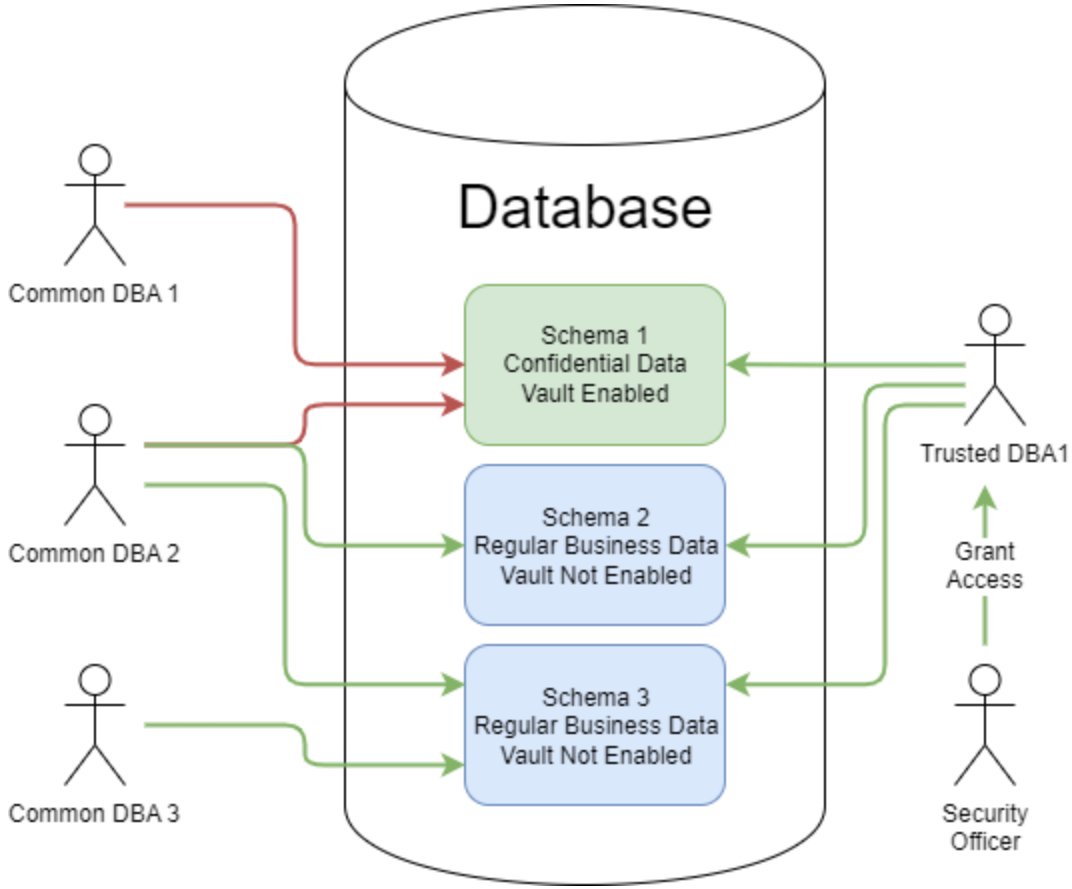
Дополнительно см. обучающее видео на тему «Как минимизировать угрозы со стороны суперпользователя» на postgrespro.ru/video/how-to

Как ограничить доступ администратора к данным?

PostgresPro

Предоставить доступ доверенным бизнес-пользователям не проблема, но к сожалению к чувствительным данным получают доступ и администраторы...

- В больших организациях слишком много администраторов имеют доступ к объектам экземпляра СУБД, так как им надо производить регулярное обслуживание своих БД, осуществлять резервное копирование и т.д.
- Надо отнять у них права доступа к чувствительным данным и коммерческой тайне, передав им «доверенным» администраторам
- В больших организациях доступ к БД раздаёт отдел безопасности, а не Админы СУБД. Нужно, чтобы доступ к чувствительным данным и коммерческой тайне давали тоже только они



Администратор без доступа к данным – реализация

PostgresPro

- Используется разграничение прав администраторов СУБД с деактивацией УЗ суперпользователя для повседневных операций
- Вводится понятие защищенной зоны на уровне схемы
- Вводятся специальные роли для использования в защищенной схеме – ее владельца (доверенного администратора) и менеджера прав доступа
- Назначение схеме менеджера прав доступа превращает ее в защищенную
- Владелец схемы имеет доступ к ее объектам по умолчанию, но теперь администраторы и бизнес-пользователи могут получить доступ к ним только после явного разрешения от менеджера прав доступа
- Для контроля доступа используется стандартный механизм ACL

- Разработка PostgressPro:
  - Код выдачи прав на доступ к объектам – pg_class, pg_proc, pg_type, pg_collation
  - В структуре каталога pg_namespace - новое поле nspsecofficer, аналогичное nspowner
  - Роль SECURITY OFFICER внесена в Schema в явном виде
  - В синтаксисе ALTER SCHEMA появилось «ALTER SCHEMA … SECURITY OFFICER TO …»
  - В pg_dump – возможность выгрузки только прав доступа для pg_restore под Security Officer

Видео

Создание защищенной схемы и ее владельца «с нуля» (в пустой БД)

Дополнительно см. обучающее видео на тему «Ограничение доступа привилегированных пользователей к данным» на postgrespro.ru/video/how-to

Регистрация событий безопасности

Задача – расширить охват аудита и снизить нагрузку на СУБД:

- pgAudit -> pg_proaudit (v1.0 быстрый, но сложные настройки) -> pg_proaudit (v2.0)
- Оптимизированный механизм поиска – правило для аудирования подбирается фильтрацией правил по комбинации
  - Имя базы данных
  - Тип события (можно указать как конкретные команды, так и классы событий)
  - Тип объекта
  - Имя объекта
  - Имя роли (можно указать как конкретного пользователя, так и групповую роль)
- Легко настраивать правила
- Может логировать любую команду SQL; в т.ч. – какой пользователь выполнил действие
- Выше быстродействие благодаря параллельной обработке
- Выполнен бэкпорт утилиты в PgPro версии 14.11+, 15.6+

Настройки записи событий безопасности

PostgresPro

Для доступа к настройкам необходимо получить разрешение от пользователя с атрибутом SUPERUSER

Для регистрации событий – функция
pg_proaudit_set_rule(db_name text, event_type text, object_type text, object_name text, role_name text, comment text)

Для удаления конкретного правила – функция
pg_proaudit_remove_rule(db_name text, event_type text, object_type text, object_name text, role_name text)

Для сохранения изменений в файле конфигурации pg_proaudit.conf – функция **pg_proaudit_save**()

- Файл pg_proaudit.conf размещается в каталоге данных кластера (PGDATA). Изменить расположение файла pg_proaudit.conf нельзя.

Для считывания конфигурации регистрации из файла pg_proaudit.conf – функция **pg_proaudit_reload**()

Для получения списка регистрируемых событий в виде таблицы – функция **pg_proaudit_show**()

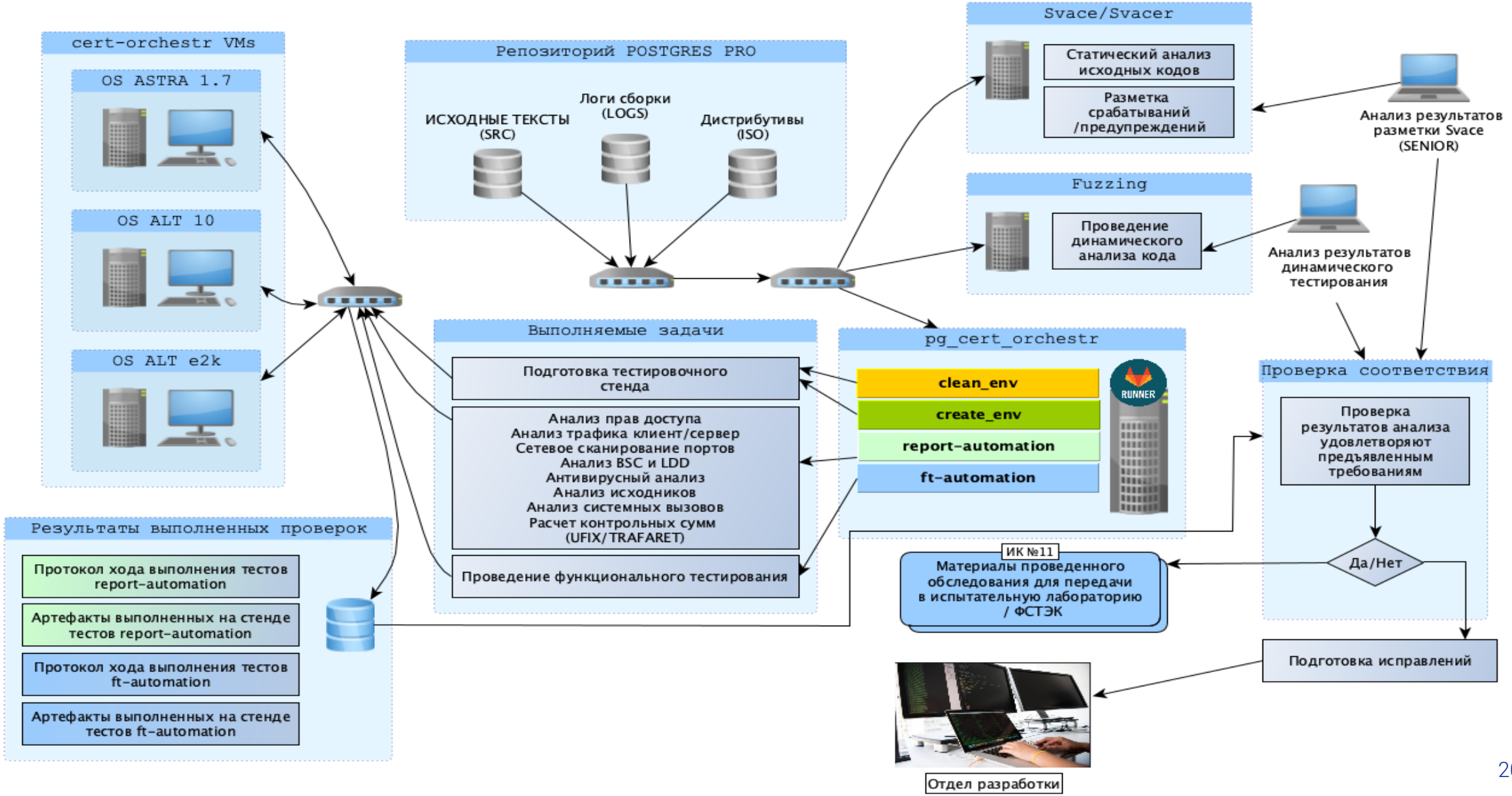
Для удаления всех правил регистрации событий – функция **pg_proaudit_reset**()

Применяем сертифицированные средства защиты к СУБД для 1С

Процесс выпуска, отличия от несертифицированных релизов, где можно применять

Процесс выпуска сертифицированных обновлений

PostgresPro



Где можно использовать наши сертифицированные версии

PostgresPro

Системы управления базами данных, соответствующие 4 классу защиты, применяются:

- в значимых объектах критической информационной инфраструктуры 1 категории значимости,
- в государственных информационных системах 1 класса защищенности,
- в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности,
- в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных,
- в информационных системах общего пользования II класса

fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-14-aprelya-2023-g-n-64

Применяем средства защиты к СУБД для 1С

(практика на площадке 1С PREMIUM)

Демонстрация сбора событий безопасности на уровне СУБД

Описание стенда – выполненные настройки

- Проведено развертывание кластера СУБД Postgres Pro Enterprise для 1С:Предприятие версии 16.8 на ОС Ubuntu 24
- Создана роль Пользователя 1С user_ones с правами суперпользователя
- Средствами 1С добавлена демо-БД ZUP на основе конфигурации «1С:Зарплата и управление персоналом», владельцем которой является роль user_ones
- Созданы роли Администратора кластера dbms_admin и Менеджера прав доступа dv_sec_officer
- С помощью Менеджера прав доступа dv_sec_officer в БД ZUP создана защищенная зона на уровне схемы PUBLIC
- Создана БД для сбора данных аудита SECURITY
- Установлено расширение pg_proaudit, создана вспомогательная групповая роль ONES_AUDIT и определены правила аудирования
- Отключена роль postgres, а у роли user_ones отняты права суперпользователя

Схема стенда

Вопросы аудита

- Кто подключается?
- Меняется ли системная конфигурация и другие настройки?
- Меняется ли структура данных?
- Как изменяются чувствительные данные?
- Меняется ли ролевая модель?
- Какие действия предпринимают привилегированные пользователи?

Установленные правила аудирования

PostgresPro
1С PREMIUM

db	event_type	object_type	object_name	role_name	comment
	AUTHORIZE				все новые авторизации (соединения)
	DISCONNECT				все окончания соединений
	ALL_ROLE				все действия над пользователями и ролями - CREATE, ALTER, DROP в отношении USER, ROLE, GROUP, PROFILE, а также выполнение команды GRANT
	ALTER SYSTEM				все изменения системной конфигурации
	ALL_DDL	EXTENSION			создание/удаление расширений
ZUP	ALL_DML	SCHEMA	PUBLIC	ONES_AUDIT (Групповая роль)	весь доступ к данным внутри безопасной схемы
ZUP	ALL_DDL	SCHEMA	PUBLIC	ONES_AUDIT (Групповая роль)	все создания и модификации базы данных, таблиц, представлений, хранимых функций и процедур
	ALL	FUNCTION		DV_SEC_OFFICER	все действия офицера безопасности с функциями
	ALL			POSTGRES	все действия суперпользователя
	ALL			PGPRO_DBMS_ADMIN	все действия Администраторов СУБД

Сценарий демонстрации

PostgresPro
1С PREMIUM

- Проверка существующих доступов к защищенной схеме
- Заведение роли инженера поддержки от имени Администратора СУБД
- Предоставление доступа инженеру поддержки к базе данных 1С от имени Офицера безопасности для создания резервных копий с помощью программы pg_dump
- Выявление несанкционированного доступа к данным 1С и нейтрализация угрозы
- Отслеживание событий и доступа к объектам БД 1С с помощью отчетов pg_proaudit

PostgresPro

1С PREMIUM

Чего ждать в новых версиях Postgres Pro?

PostgresPro

Для заказчиков 1С наиболее интересно будет расширение Transparent Data Encryption, уже доступное для иностранных пользователей Postgres Pro Ent 17

- TDE – вариант защитного преобразования данных на жёстком диске и на любом носителе резервного копирования без преобразования данных в кэше, в shared memory или во время передачи
- Процесс преобразования прозрачен на уровне SQL, выполняется в момент обращения к ПЗУ и не требует никаких изменений в приложениях. Он защищает данные перед их записью на диск и выполняет обратное преобразование при чтении с него
- Утилиты, обращающихся к файлам данных напрямую (pg_basebackup, pg_rewind, pg_waldump, pg_checksum и др.), также могут прозрачно работать с защищенными данными
- Для защиты применяются надежные стандартные алгоритмы и иерархическая система секретов. Чтобы предотвратить несанкционированное обратное преобразование, TDE хранит мастер-секрет во внешнем по отношению к базе данных модуле безопасности, называемом хранилищем секретов
- Для защиты таблиц создается новый TABLESPACE, включается режим преобразования; затем таблицы создаются или перемещаются
- При записи WAL-файлов данные таблиц из защищаемых TABLESPACE также будут преобразовываться. Данные таблиц из незащищаемых TABLESPACE не преобразовываются

Ведется работа по интеграции TDE с лицензированными поставщиками СКЗИ

Преимущества TDE перед преобразованием на уровне приложения

PostgresPro

- Не требуется хранение секретов и процедура их ротации на стороне многочисленных клиентов
- Не требуется изменять запросы приложений к БД – преобразование прозрачно для приложений
- Можно фильтровать данные (sql where, having) по значению колонки защищённой таблицы
- Можно связывать таблицы (foreign key) по значению колонки защищённой таблицы
- Можно накладывать ограничения (constraints) по значению колонки защищённой таблицы

Дополнительная информация

Вебинар «СУБД Postgres Pro для 1С: новые возможности» 13 мая 2024 г.

- Докладчики – Марк Ривкин, Андрей Забелин, Антон Дорошкевич
- Возможности и производительность, совместимые с «1С» технологии в СУБД, новый тип лицензий и сертификатов технической поддержки Postgres Pro Enterprise
- rutube.ru/video/f7364dae2045b149a5514b9e3c545b4a

Презентация «Правила лицензирования СУБД Postgres Pro» 21 июня 2024 г.

- Автор – Марк Ривкин
- Коммерческие предложения – лицензии, поддержка, консалтинг
- Примеры лицензирования для 1С
  - По ядрам
  - По серверам и пользователям
- postgrespro.ru/materials/5971003

PostgresPro

Спасибо за внимание!

sales@postgrespro.ru