Сергей Новиков
HilltopAds

PGDAY'17 RUSSIA
КОНФЕРЕНЦИЯ ПО БАЗАМ ДАННЫХ

Безопасность с нуля и каждый день

Исходные данные:

- Крупный FinTech-проект

Исходные данные:

- Крупный FinTech-проект
- Торги идут 24 / 7

Исходные данные:

- Крупный FinTech-проект
- Торги идут 24 / 7
- Downtime – это дорого

Исходные данные:

- Крупный FinTech-проект
- Торги идут 24 / 7
- Downtime – это дорого
- Стартап по духу и по содержанию

Основные симптомы:

- Приложения работают под ролью владельца БД

Основные симптомы:

- Приложения работают под ролью владельца БД
- Пароль от этой роли знают все

Основные симптомы:

- Приложения работают под ролью владельца БД
- Пароль от этой роли знают все
- Много SUPERUSER

Основные симптомы:

- Приложения работают под ролью владельца БД
- Пароль от этой роли знают все
- Много SUPERUSER
- GRANT ALL ON SCHEMA public TO PUBLIC

Основные симптомы:

- Приложения работают под ролью владельца БД
- Пароль от этой роли знают все
- Много SUPERUSER
- GRANT ALL ON SCHEMA public TO PUBLIC
- У postgres есть пароль

Основные симптомы:

- Приложения работают под ролью владельца БД
- Пароль от этой роли знают все
- Много SUPERUSER
- GRANT ALL ON SCHEMA public TO PUBLIC
- У postgres есть пароль
- postgres OFFICE-IP trust

Наводим порядок с ролями приложений:

- Каждому приложению – персональная роль
- Владелец БД только для миграций
- Роли приложений имеют минимальные права
- Дополнительные действия доступны через SECURITY DEFINER
- Все приложения ходят в БД строго через pgBouncer и только с серверов приложений

Наводим порядок с ролями сотрудников:

- Каждому сотруднику – персональная роль
- Авторизация через LDAP или peer
- Все сотрудники ходят в БД строго напрямую
- Доступ в серверную подсеть строго через VPN
- У всех log_min_duration_statement = 0

Наводим порядок с групповыми ролями:

- group_read – только чтение (без критичных данных)
- group_write – только запись и вызов хранимок
- group_admin – только права SUPERUSER

Наводим порядок с групповыми ролями:

- group_read – только чтение (без критичных данных)
- group_write – только запись и вызов хранимок
- group_admin – только права SUPERUSER

И группы для авторизации:

- group_application – для локального pgBouncer
- group_personal – для сотрудников

Итоговая таблица групп:

hba / rights	group_read	group_write	group_admin
group_application	Другие микросервисы	Основное приложение	
group_personal	Большинство разработчиков	Доверенные разработчики	DBA, сисадмины

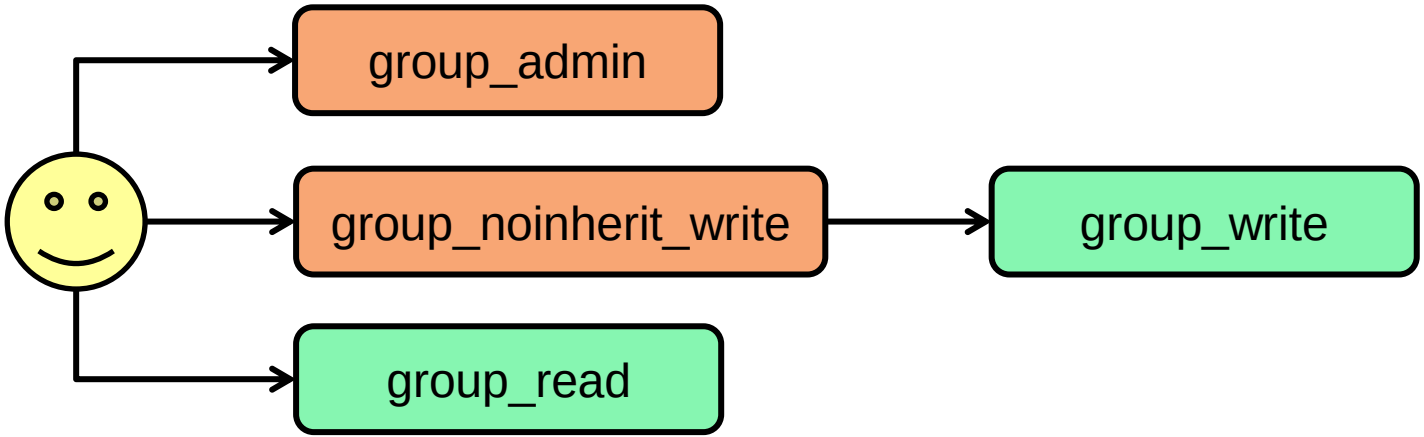
Пример pg_hba.conf:

```
# Deploy (owner)
hostssl     db      db_owner            CI/CD-IP    cert

# Application (pgBouncer)
local       db      +group_application              peer map=application

# Personal
local       all     +group_personal                 peer
host        all     +group_personal     VPN-IP      ldap
```

Проблема INHERIT:

- Доверенные разработчики имеют права на чтение и на запись
- В большинстве случаев нужно только чтение
- Права на запись хотелось бы включать по запросу
- Флаг NOINHERIT можно поставить на роль, но не на связку ролей (нет опции GRANT group TO role WITH NOINHERIT)

Решение:



Безопасность данных – о чём вообще речь?

Безопасность данных – о чём вообще речь?

- Данные клиентов критичны на чтение

Безопасность данных – о чём вообще речь?

- Данные клиентов критичны на чтение
- Финансовые данные критичны на запись

Безопасность данных – о чём вообще речь?

- Данные клиентов критичны на чтение
- Финансовые данные критичны на запись
- И то, и другое решается правами доступа на таблицы/колонки и SECURITY DEFINER

Безопасность данных – о чём вообще речь?

- Данные клиентов критичны на чтение
- Финансовые данные критичны на запись
- И то, и другое решается правами доступа на таблицы/колонки и SECURITY DEFINER
- Доступ на чтение должен быть точечным

Безопасность данных – о чём вообще речь?

- Данные клиентов критичны на чтение
- Финансовые данные критичны на запись
- И то, и другое решается правами доступа на таблицы/колонки и SECURITY DEFINER
- Доступ на чтение должен быть точечным
- Источник запроса можно определить с помощью логирования в хранимках и триггерах

Проблема тестовой среды:

- Нужен объём, приближенный к боевому
- Нужны данные, приближенные к боевым
- Нужны более широкие права на чтение и запись
- Схему нужно периодически синхронизировать

Решение:

- Раз в неделю копируется боевая БД и маскируется
- Данные клиентов генерируются по словарю
- Быстрая очистка – DROP COLUMN или TRUNCATE
- Наиболее критичные данные чистятся с последующим VACUUM FULL
- Права доступа повышаются после маскирования

Сбор и анализ логов (PostgreSQL):

- log_destination = csvlog
- log_timezone = UTC
- log_filename = postgresql-%a
- log_rotation_age = 1d
- log_truncate_on_rotation = on

Сбор и анализ логов (Fluentd / Logstash):

- Преобразовать CSV в JSON по формату
- Добавить hostname сервера
- Удостовериться, что @timestamp поддерживает миллисекунды

Сбор и анализ логов (Elasticsearch + Kibana):

- В Elasticsearch установить template mapping (https://github.com/red-defender/pg-utils/tree/master/csvlog_elasticsearch)
- В Kibana обновить структуру индекса и выбрать поле временной отметки

Логирование из хранимок и триггеров:

```
CREATE FUNCTION write_log(
    _message    TEXT,
    _severity   TEXT    DEFAULT 'INFO',
    _context    JSONB   DEFAULT '{}' -- Можно парсить в template mapping!
) RETURNS VOID LANGUAGE plpgsql VOLATILE
AS $$
BEGIN
    RAISE LOG USING
        MESSAGE = _message,
        DETAIL = _context,
        HINT = 'APP-' || UPPER(_severity);
END;
$$;
```

И наконец, пара слов о безопасности…

И наконец, пара слов о безопасности…

- Как получить shell из-под postgres, имея доступ только к config-файлам?

И наконец, пара слов о безопасности…

- Как получить shell из-под postgres, имея доступ только к config-файлам?
- Что такое postgresql.auto.conf?

И наконец, пара слов о безопасности…

- Как получить shell из-под postgres, имея доступ только к config-файлам?
- Что такое postgresql.auto.conf?
- А точно ли файлы не менялись?

И наконец, пара слов о безопасности…

- Как получить shell из-под postgres, имея доступ только к config-файлам?
- Что такое postgresql.auto.conf?
- А точно ли файлы не менялись?
- include? config_file?

И наконец, пара слов о безопасности…

- Как получить shell из-под postgres, имея доступ только к config-файлам?
- Что такое postgresql.auto.conf?
- А точно ли файлы не менялись?
- include? config_file?
- Как мониторить применённые настройки hba?

Выводы по обнаружению вторжений:

- Поставить auditd
- Мониторить целостность применённых настроек
- Мониторить reload и restart
- Мониторить отключение логирования
- Мониторить pg_stat_activity и pg_stat_replication, причём на всех серверах
- Ломать голову, как мониторить выгрузки…

Пароли – это плохо:

- Можно подобрать или подсмотреть

Пароли – это плохо:

- Можно подобрать или подсмотреть
- В нагруженной среде не так просто поменять

Пароли – это плохо:

- Можно подобрать или подсмотреть
- В нагруженной среде не так просто поменять
- Хэши паролей при методе авторизации md5 небезопасны!

Используйте application_name:

- Уникальный ID процесса-источника (8-16 символов)
- Название процесса (для HTTP-запросов – URI, для демонов и крон-задач – имя задачи)

Не всегда злоумышленнику нужны данные.
Иногда он хочет просто всё обрушить…

Не всегда злоумышленнику нужны данные.
Иногда он хочет просто всё обрушить…

По умолчанию всем доступны:

- Временные таблицы

Не всегда злоумышленнику нужны данные.
Иногда он хочет просто всё обрушить…

По умолчанию всем доступны:

- Временные таблицы
- Advisory-локи

Не всегда злоумышленнику нужны данные.
Иногда он хочет просто всё обрушить…

По умолчанию всем доступны:

- Временные таблицы
- Advisory-локи

Не содержат данных, но могут быть атакованы:

- SEQUENCE

Права доступа нужно ставить очень внимательно:

- ALTER DEFAULT PRIVILEGES – для какой роли?
- GRANT ALL ON TABLES – что значит ALL?

Заведите себе безопасника:

- Он возьмёт на себя ответственность

Заведите себе безопасника:

- Он возьмёт на себя ответственность
- Он сможет профессионально организовать систему безопасности

Заведите себе безопасника:

- Он возьмёт на себя ответственность
- Он сможет профессионально организовать систему безопасности
- Он будет вести матрицу доступа и проводить периодические проверки

Заведите себе безопасника:

- Он возьмёт на себя ответственность
- Он сможет профессионально организовать систему безопасности
- Он будет вести матрицу доступа и проводить периодические проверки
- Он тот, кто Вас понимает!

Сергей Новиков
HilltopAds

PGDAY'17 RUSSIA
КОНФЕРЕНЦИЯ ПО БАЗАМ ДАННЫХ

Вопросы?