Информационная безопасность в PostgreSQL

Валерий Попов

Введение

Стек приложений ИС

Меры по обеспечению ИБ:

- Технологические
- Административно-организационные мероприятия
- Физическая защита
- Программно-технические

ФСТЭК, ФСБ: нужны сертифицированные средства от НСД в ИС общего пользования, ГИС, и в ИС персональных данных.

Треугольник компромиссов

Одновременно со свойствами ФБП информационная система быть не может!
Нужно выбрать 2 из 3

Типичные применения:
БП — специальные системы realtime
ФП — интернет-магазин
ФБ — специальные системы

Введение

Есть проблема выбора СУБД федерального уровня.

С.Муравьев (Pgconf 2015) или «Открытые системы» 2015 №1. СУБД: проблема выбора

- Ни одна сертифицированная СУБД не обладает полным набором готовых средств для построения ИС федерального уровня.
- Наилучшими характеристиками обладают производные от PostgreSQL.

В 2015 году ситуация изменилась!
Начались пилоты и проекты по переходу на СПО в госорганизациях и компаниях.

Российское ПО

Преференции российскому ПО:

- С 01 января 2016 г. при госзакупках — российское ПО из реестра
- К 01 июня 2016 г. новые поправки — предпочтение российскому ПО и для госкомпаний

Российские СУБД

	Год выпуска	МО	ФСБ	ФСТЭК
Postgres Pro (PostgreSQL9.5+)	2016			☆
Astra Linux Special Edition (PostgreSQL 9.3)	2012	✔	✔	✔
Alt Linux СПТ6(PostgreSQL 9.3)	2011			✔
Заря (PostgreSQL 9.0)	2012	✔		✔
Линтер 6.0 (Бастион)	2011	✔		

☆ – Подана заявка на сертификацию

Используемые аббревиатуры

НСД — Несанкционированный доступ к информации

СЗИ — Средства защиты информации

КСЗ — Комплекс средств защиты

PGDG — PostgreSQL Global Development Group

Postgres Pro =

PostgreSQL 9.5 +

- Багфиксы по состоянию на 1 февраля 2016 года.
- Увеличение производительности на многоядерных системах
- Усовершенствования полнотекстового поиска
- Доработки в покрывающих индексах
- Доступ к внутреннему представлению данных таблиц
- Переносимость: однозначная обработка юникодных символов
- Нечеткое сравнение строк и нечеткий поиск подстроки
- Новые модули для сохранения/восстановления плана выполнения запроса и статистики БД
- Легко подключаемые словари для полнотекстового поиска + для **сертифицированной** версии
- Очистка памяти, контроль целостности КСЗ, тесты КСЗ

Показатели защищенности от НСД

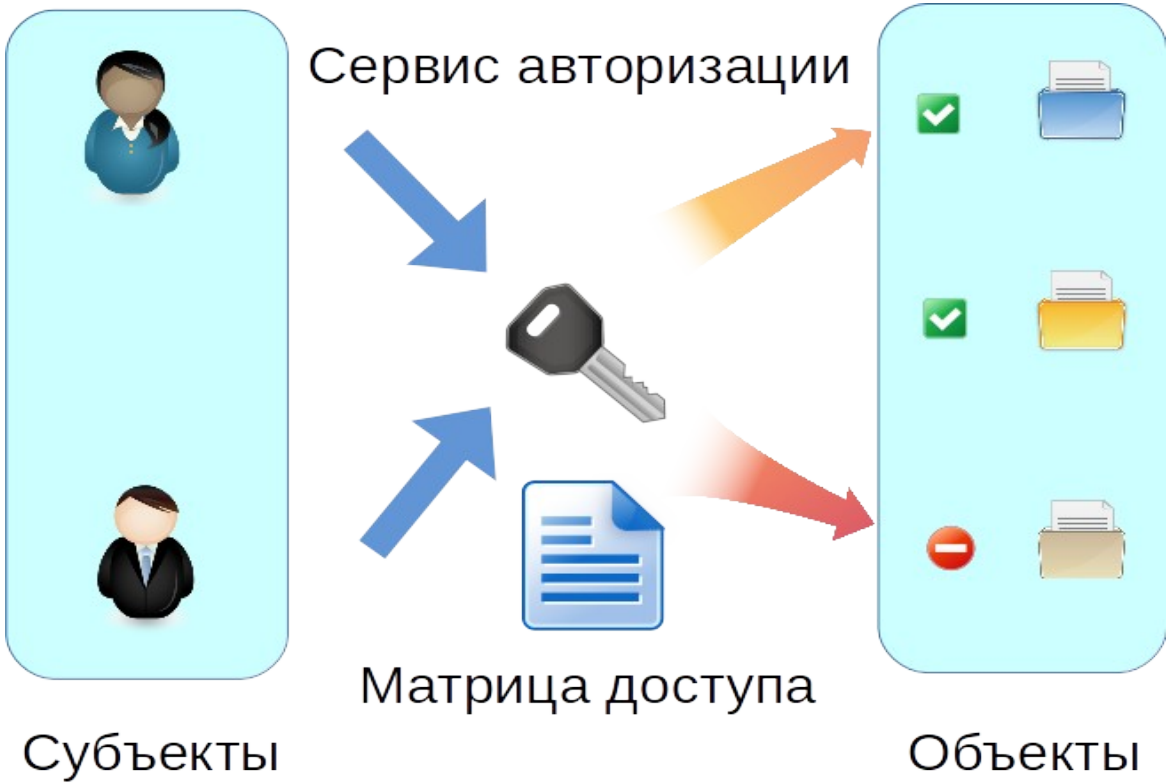
Показатель	КИ	СС
Дискреционный контроль доступа	✔	✔
Мандатный контроль доступа	✖	✔
Очистка памяти	✔	✔
Изоляция модулей	✖	✔
Идентификация и аутентификация	✔	✔
Регистрация событий	✔	✔
Надежное восстановление	✖	✔
Целостность КСЗ	✔	✔
Тестирование КСЗ	✔	✔
Документация	✔	✔

✔ - Применяется ✖ - Не применяется

Требования Общих Критериев ИБ

- Common Criteria — международный стандарт оценки защищенности ИТ, также принят у нас ГОСТ Р ИСО/МЭК 15408
- Профиль защиты СУБД соответствует требованиям по 5 классу защищенности с дополнительными требованиями
- Компания Crunchy Data Solution (*Stephen Frost*) проводит сертификацию своего дистрибутива PostgreSQL 9.5 по CC и будет первой opensource СУБД, получившей сертификат CC

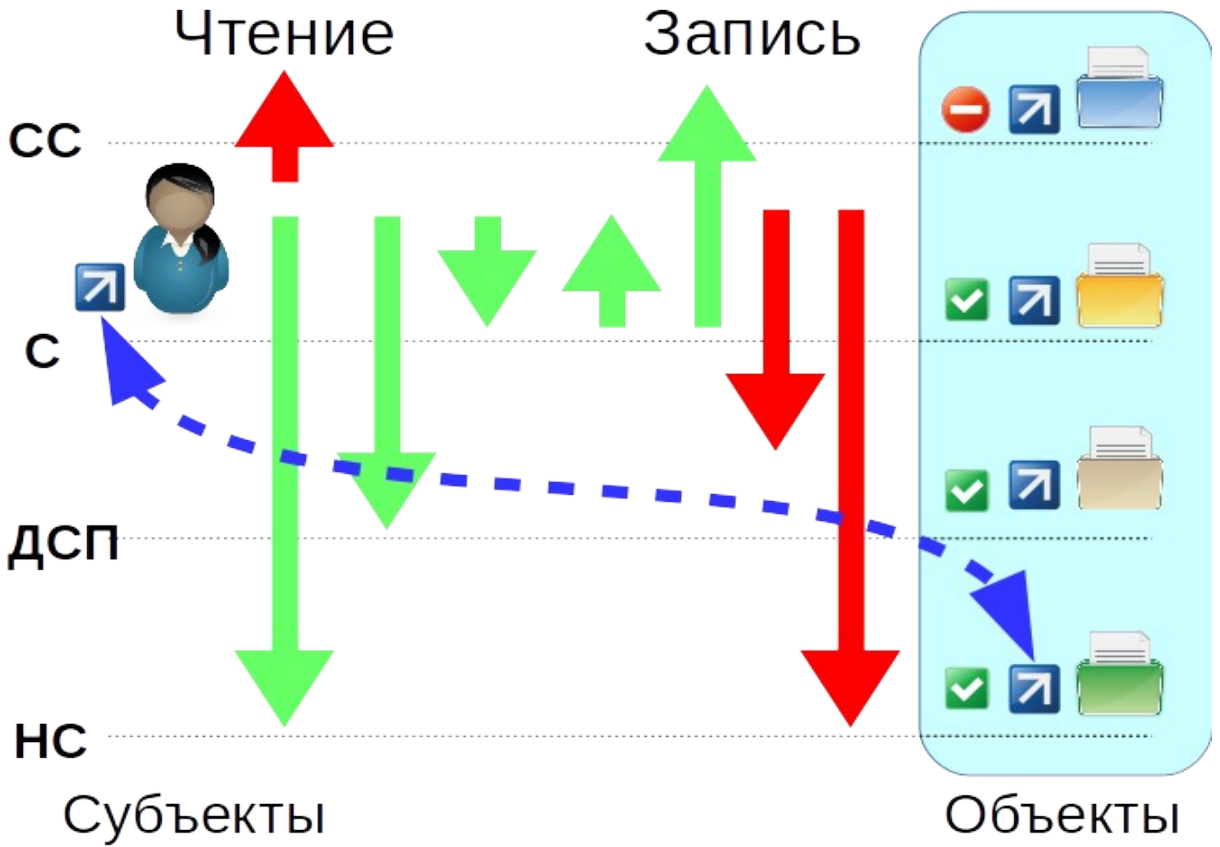
Дискреционное управление доступом (DAC)



Разграничение доступа на основе матрицы доступа. ACL, RBAC

Достаточно для конфиденциальной информации.

Мандатное управление доступом (МАС)



- Метки доступа

Разграничение доступа на основе иерархии меток доступа.

Необходим, начиная с гостайны.

Очистка памяти

Зачем нужна очистка?

Не должно быть доступа к остаточной информации после ее использования.

СУБД	Где?
Postgres Pro (PostgreSQL 9.5 +)	в СУБД
Astra Linux Special Edition (PostgreSQL 9.3)	в ОС
Alt Linux СПТ 6/ СПТ 7 (PostgreSQL 9.1)	в ОС
Заря (PostgreSQL 9.0)	в ОС
Линтер 6.0 (Бастион)	в СУБД

Очистка памяти

В силу мультиверсионности, информация в страницах только помечается удаленной, но остается на месте.

Где нужна очистка в PostgreSQL?

- Оперативная память
- При освобождении файлов (удаление/пересоздание объектов БД)
- Страницы данных на диске
- Неиспользуемые WAL-логи на диске

Целостность КСЗ

Производится подсчет контрольных сумм и сравнение с эталоном.

В Postgres Pro контролируется неизменность:

- системные бинарные файлы
- конфигурационные файлы (postgresql.conf, pg_hba.conf, pg_ident.conf,..)
- системные таблицы (pg_catalog.pg_*)

Безопасность на уровне строк (RLS)

- Появилась в PostgreSQL 9.5, создавалась на протяжении 5 лет.
- Устойчива к уязвимостям SQL-инъекций.
- Интегрируется с внешними системами, основанными на метках безопасности.
- Политика дает разрешение SELECT, INSERT, UPDATE, DELETE строк.

Пример использования RLS

```
ALTER TABLE accounts ENABLE ROW LEVEL SECURITY;
CREATE POLICY manager_policy ON accounts USING
(manager = current_user);
SELECT * FROM accounts;
```

Liza

Petr

manager text	data text	other_data
Petr	……	……
Liza	……	……
Petr	……	……
Liza	……	……

Information Security Group в PGDG

- Принципы PGDG к защите информации:
- Отказоустойчивые конфигурации (репликация, архивирование, кластеризация)
- Безопасный и устойчивый сервер базы данных
- Хорошая интеграция с инфраструктурой безопасности (LDAP, RADIUS, SSL, GSSAPI, ….)
- IS group - около 20 человек, контролируемый список рассылки
- Детали решения проблемы не публикуются, пока не выйдет патч в ближайшем выпуске минорной версии

Статистика уязвимостей в PostgreSQL с 2010 г.

http://www.postgresql.org/support/security/

Класс уязвимости

Год	A	B	C	D	Σ
2010			2		2
2012	1		5	1	7
2013	1		3	2	6
2014			7	1	8
2015		2	6	1	9

Примеры уязвимостей класса A

CVE-2012-0867. При проверке SSL сертификата имя хоста усекается до 32 символов.
Зарегистрировано 2012/01/19. Закрыто релизом 2012/02/27.

CVE-2013-1899. Позволяет повредить файлы в директории данных сервера, если имя базы в запросе начинается с «-».
Зарегистрировано 2013/02/19. Закрыто релизом 2013/04/14.

Результаты поиска уязвимостей с 2010 года

https://nvd.nist.gov/home.cfm

Продукт	Low	Medium	High	Количество
Oracle database_server	28	125	34	167
Microsoft sql_server	0	6	4	10
Mysql	80	205	12	163
PostgreSQL	1	30	6	37

Postgres Professional

- У нас есть лицензии ФСТЭК
- Наша версия дистрибутива в процессе сертификации во ФСТЭК.

Применимость сертифицированной СУБД «Postgres Pro»:

- ГИС до 1 класса защищенности включительно
- ИСПДн до 1 класса защищенности включительно
- АС до класса 1Г включительно

Спасибо за внимание!

Контакты:

v.popov@postgrespro.ru

+79032565482