Опыт эксплуатации серверов PostgreSQL в корпоративной сети

ООО «ИТСК»

Технологический центр 1С

Пучков В.В.

24.01.2020

ГАЗПРОМ НЕФТЬ

ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР 1С В ИТСК

Требования к технологическим решениям

- **Безопасность**
- **Отказоустойчивость**
- **Соответствие корпоративным стандартам**

Требования к технологическим решениям

- **Безопасность = (pg_hba.conf + Kerberos)**
- **Отказоустойчивость**
- **Соответствие корпоративным стандартам**

Требования к технологическим решениям

- **Безопасность = (pg_hba.conf + Kerberos) * Design**
- **Отказоустойчивость**
- **Соответствие корпоративным стандартам**

Безопасность – pg_hba

- pg_hba.conf – друг DBA
  - Ограничение подсетей и хостов, имеющих доступ к СУБД
  - Разделение способов аутентификации по хостами И пользователям

Безопасность – pg_hba

1. Пример pg_hba.conf:

```
# TYPE  DATABASE        USER            ADDRESS         METHOD
local   all             all                             peer
# IPv4 local connections:
host    all             tresh           127.0.0.1/32    md5
host    all             all             127.0.0.1/32    gss include_realm=1 krb_realm=GAZPROM-NEFT.LOCAL
# Linux 1C Server
host    all             all             x.x.x.x/32      md5
# Windows clients
host    all             all             x.x.x.x/32      gss include_realm=1 krb_realm=GAZPROM-NEFT.LOCAL
host    all             all             x.x.x.x/24      gss include_realm=1 krb_realm=GAZPROM-NEFT.LOCAL
host    all             all             x.x.x.x/24      gss include_realm=1 krb_realm=GAZPROM-NEFT.LOCAL
host    all             all             x.x.x.x/24      gss include_realm=1 krb_realm=GAZPROM-NEFT.LOCAL
# IPv6 local connections:
host    all             all             ::1/128         md5
```

Безопасность - Kerberos

- Работает на серверах Windows
  - сервис должен быть запущен под доменной УЗ
- и Linux
  - УЗ должна находиться в ветке AD без кириллических символов
  - При выполнении

```
ktpass -princ POSTGRES/<сервер>.gazprom-neft.local@GAZPROM-NEFT.LOCAL
-mapuser <УЗ> -pass "<пароль>" -crypto All -ptype KRB5_NT_PRINCIPAL -
out <файл.keytab>
```

  имя сервера должно быть в нижнем регистре
- Работает с 1С
  - В параметрах подключения надо указать имя УЗ, но не указывать пароль

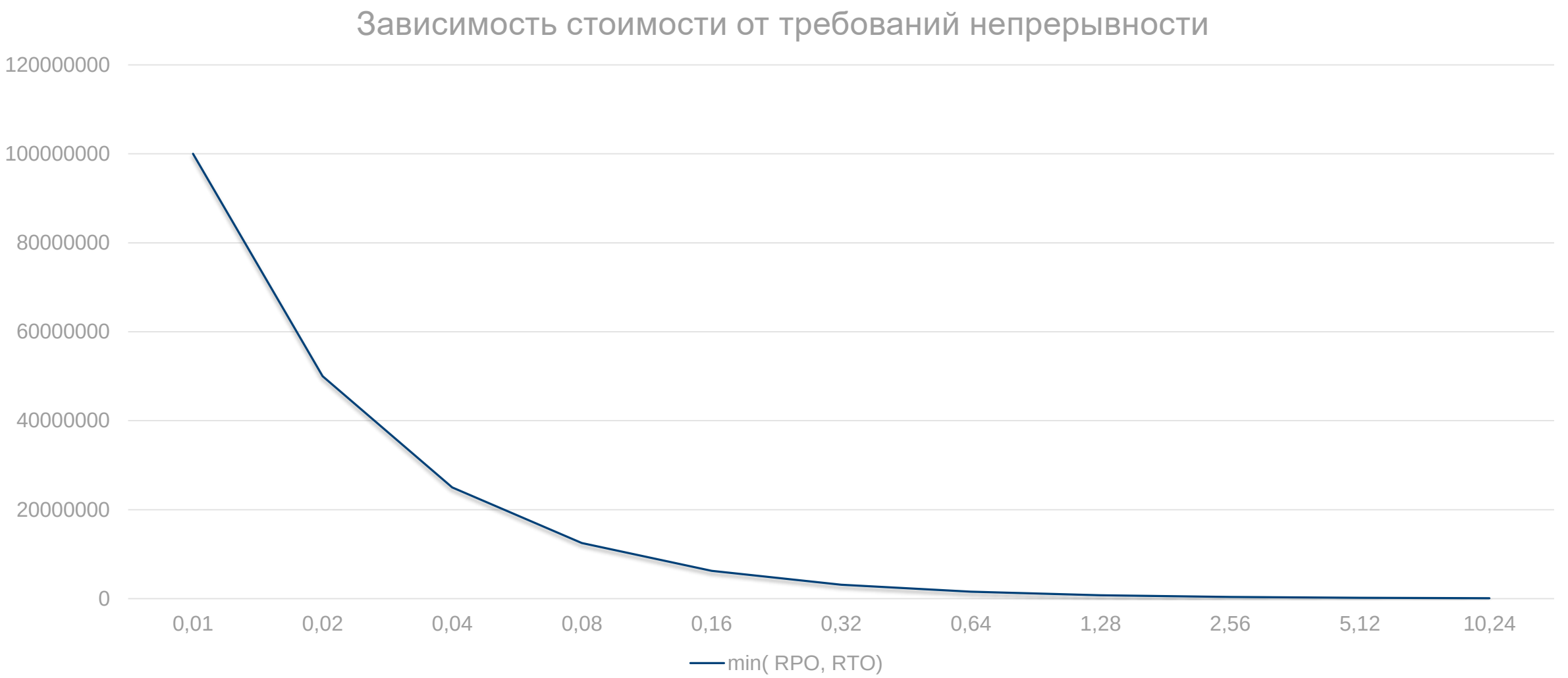
Безопасность Design (архитектура)

- Раздельные ландшафты разработки, тестирования и промышленной эксплуатации
- Минимально необходимые сетевые доступы
- Разные владельцы у промышленных БД
- У владельца БД не должно быть привилегии superuser !
- Не забыть, что по умолчанию все функции доступны роли public

Отказоустойчивость – подход к проектированию

- **Исходить из того, что нужно бизнесу**
- **Два главных слова: RTO и RPO**
- **RTO – Recovery Time Objective – допустимое время восстановления при сбое**
- **RPO – Recovery Point Objective – допустимое время потери данных**

Отказоустойчивость – подход к проектированию



Отказоустойчивость – особенности систем 1С

- **24x7, но не 99.999**
- **Сохранность данных важнее непрерывности**
- **Согласованный перерыв – не недоступность**
- **Обновление конфигурации иногда разрушает данные**

Особенности реализации

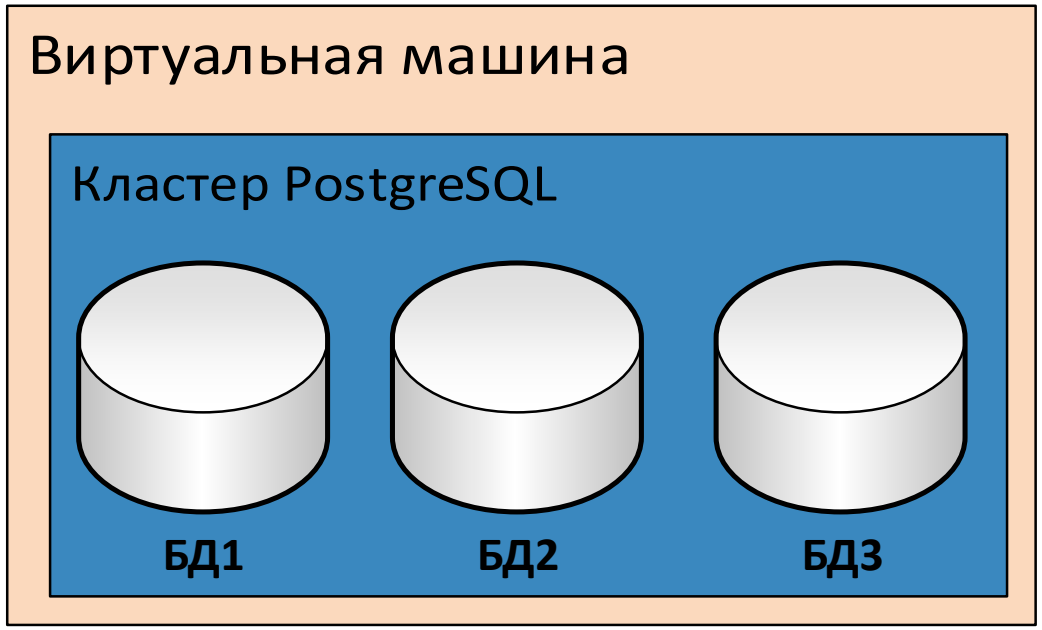
- **СХД**
- **Виртуализация без динамического перераспределения**
- **Защита от аппаратных сбоев на уровне гипервизора**
- **Централизованная система резервного копирования**

Базы данных и виртуальные машины – где разделять?

- **Простое, понятное**

…и неправильное решение

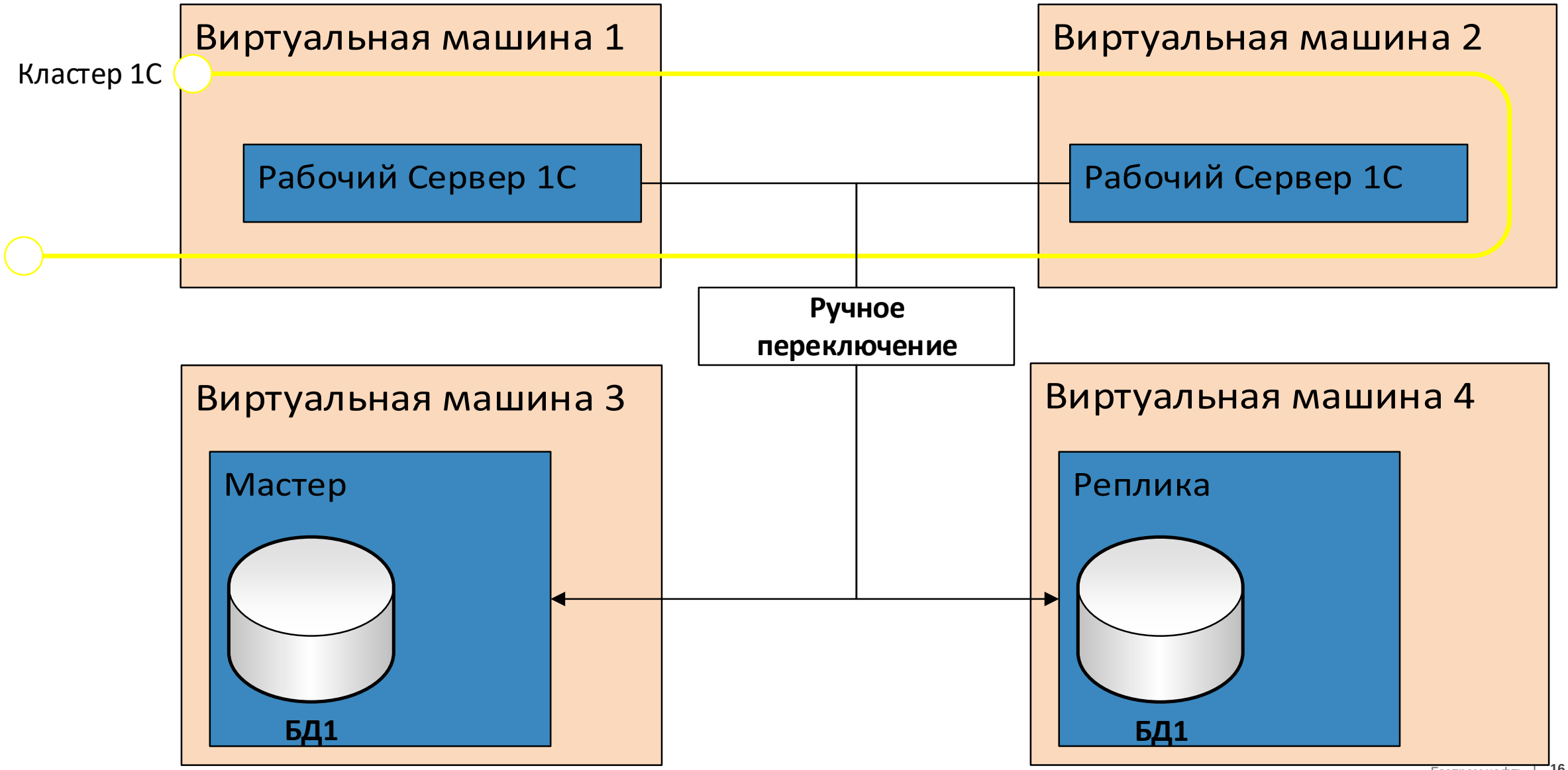
- Просто настроить
- Просто администрировать
- Конкуренция за ресурсы
- Проблемы с резервным копированием одной БД



Базы данных и физические хосты – где разделять?

- **Один кластер – одна БД**
  - Независимое выделение ресурсов
  - Независимое резервное копирование
  - Делить по кластерам или по ВМ – в зависимости от внутренних стандартов и требований

Реализация отказоустойчивости



Резервное копирование

- **pg_probackup**
- **Интеграция с корпоративными СРК с помощью pre-exec и post-exec скриптов**
  - В pre-exec выполняем backup –b FULL в локальный каталог
  - В post-exec выполняем delete –expired –delete-wal
  - Всегда есть локальная копия
- **Обязательно исключить из копирования каталога wal файлов .part**

Корпоративные стандарты

- **Внутренний репозиторий linux**
- **Единообразные каталоги (/pgcluster или D:\pgcluster)**
- **Скрипты**
  - установка postgresql
  - alter database …
  - pg_probackup
  - Создание доменных УЗ

Сравнение MS SQL и PostgreSQL с точки зрения DBA

- **MS SQL**
  - Лучше развиты средства интеграции (CPK, AlwaysOn)
  - Резервное копирование отдельных БД
  - Обратная совместимость с legacy-системами
- **PostgreSQL**
  - Актуализация БД через pg_dump | psql
  - Не требует реиндексации и принудительного сбора статистики
  - VACUUM FULL по отдельной таблице
  - pg_hba.conf

Опыт миграции систем 1С с MS SQL на PostgreSQL

- **Новые конфигурации (ERP) мигрируют бесшовно**
- **По старым конфигурациям УПП потребуется исследование**
  - Выявить проблемные отчёты и операции
  - Привлечь квалифицированных разработчиков 1С
  - Быть готовым к тому, что какой-то момент упустили
  - …но переход на PostgreSQL _более_ предсказуем, чем на новые версии MS SQL
- **Старые конфигурации ЗУП лучше не мигрировать без крайней надобности**

ВОПРОСЫ?