УТВЕРЖДЕНО

643.72410666.00067-075 31 01-ЛУ

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ «JATOBA»

Описание применения

643.72410666.00067-076 31 01

Листов 81

Инв. № подл.	Подп. и	Взам. инв.	Инв. №	Подп. и

2025

Литера O_1

АННОТАЦИЯ

В документе приведены сведения о защищенной системе управления базами данных «Jatoba» (далее − СУБД «Jatoba»). Настоящий документ содержит описание назначения СУБД «Jatoba», описание функциональных возможностей, условий применения и решаемых СУБД «Jatoba» задач.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ 6
2. Основные характеристики 7
2.1. Состав СУБД 7
2.2. Реализуемые функции СУБД 11
2.3. Основные функциональные возможности управления базами данных 12
2.4. Поддерживаемые типы данных 15
2.5. Поддерживаемые типы индексов 16
2.6. Поддерживаемые методы стандартизации и унификации 16
2.7. Расширенные функциональные возможности управления базами данных 16
2.8. Механизм защиты подключений к системе управления базами данных ... 17
2.9. Требования к среде функционирования СУБД 17
2.10. Функции по защите информации 20
2.11. Производительность СУБД 2
3. Решаемые задачи 2
3.1. Инсталлятор 4
3.1.1. Установка СУБД с рекомендуемой, генерируемой конфигурацией, компонентом «ja_tune» 6
3.2. Балансировка нагрузки 7
3.3. Кластеризация 7
3.3.1. Инженерные решения построения кластера 8
3.3.2. Отказоустойчивый кластер в Kubernetes 10
3.3.3. Управление кластером ja_Dog в JDS 11
3.4. Секционирование больших таблиц. ja_Hipe_Cluster 12
3.5. Мониторинг и управление СУБД 13
3.5.1. Раздел «Мониторинг» 13
3.5.2. Раздел «Анализ рисков» (User Risk) 14
3.5.3. Аудит и отчетность 15
3.5.4. Раздел «Кластеры» 16
3.5.5. Производительность 17
3.5.6. Раздел «LDAP синхронизация» 23

3.5.7. Раздел «Роли БД» (DB roles) 25
3.5.8. Раздел «Уведомления» (Notifications) 27
3.5.9. Раздел «Ландшафт» (Landscape) 29
3.5.10. Раздел «Парольные политики» (Password policies) 31
3.5.11. Раздел «Резервное копирование» (BACKUP) 32
3.6. Резервное копирование 34
3.6.1. Компонент «pg_ProBackup» 34
3.6.2. Компонент «ja_Backup» 35
3.7. Маскирование данных. Компонент «ja_Anonymizer» 35
3.8. Поддержки платформы Oracle 37
3.9. Поддержка платформы MS SQL 37
3.10. Совместимость платформой с 1С 38
3.10.1. Компонент совместимости 1С fasttrun 38
3.10.2. Компонент совместимости 1С fulleq 38
3.10.3. Компонент совместимости 1С mchar 39
3.10.4. Компонент совместимости 1С online_analyze 39
3.10.5. Компонент совместимости 1С plantuner 40
3.11. Управление планами запросов 40
3.11.1. Компонент ja_Plan_Manager. Управление планами запросов 40
3.11.2. Компонент pg_hint_plan. Корректировка запросов 42
3.11.3. Компонент pg_store_plans. Контроль выполненных планов запросов ... 42
3.12. Выявления и предотвращение исполнения нетипичных SQL-запросов ... 42
3.13. Регистрация событий безопасности 43
3.13.1. Расширенная регистрация событий СУБД 44
3.13.2. Компонент «ja_seceventlog» 45
3.13.3. Централизованный сбор событий СУБД 45
3.13.4. Формирование отчетов по журналам СУБД 46
3.14. Парольные политики 46
3.15. Поддержка работы СУБД с геоданными 47
3.16. Контроль целостности 47
3.17. Обфускации кода 49
3.18. Формирование HTTP/HTTPS запросов из СУБД 50

3.19. Компрессия данных. Компонент «ja_Compression» 51
3.20. Полнотекстовый поиск и определение похожих текстов.....52
3.20.1. Проверка орфографии и морфологический анализ. Компонент «hunspell».....53
3.21. Поиск ближайших соседей (KNN для B-TREE) 53
3.22. 64-битный счетчик транзакций. Компонент XID64.....54
3.23. Инвентаризация СУБД. Компонент «ja_Inventory».....55
3.24. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.....55
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ.....56
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.....57

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

СУБД «Jatoba» базируется на свободном программном обеспечении СУБД «PostgreSQL».

Поддерживает все стандартные функции «PostgreSQL», описание которых доступно на официальном сайте.

СУБД «Jatoba» предназначена для управления базами данных (далее – БД) в:

— значимых объектах критической информационной инфраструктуры 1 категории;

— государственных информационных системах 1 класса защищенности;

— автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности;

— информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных;

— информационных системах общего пользования II класса на базе электронно-вычислительных машин (далее – ЭВМ);

— коммерческих информационных системах,

под управлением операционных систем (далее – ОС), приведенных в таблице 2.2.

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

2.1. Состав СУБД

СУБД «Jatoba» реализована в виде дистрибутива с

— версией ядра «4» (далее по тексту «J4»);

— версией ядра «5» (далее по тексту «J5»);

— версией ядра «6» (далее по тексту «J6»).

и образа контейнера.

Компиляция СУБД выполняется с поддержкой SSL (Secure Socket Layer). Используется библиотека OpenSSL, пакет openssl-dev, который содержит заголовочные файлы и библиотеки для компиляции с OpenSSL.

В параметрах компиляции устанавливается флаг «-lssl» который подключает библиотеку OpenSSL.

В состав СУБД «Jatoba» входят компоненты, указанные в таблице 2.1.

Таблица 2.1 – Состав компонент

№	Наименование	Описание	J4		J5		J6	
			Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)
1	ядро СУБД		X	X	X	X	X	X
	pwgen	генератор паролей	—	—	X	X	X	X
	—	маскирование паролей	—	—	X	X	X	X
	KNN	поиск ближайших соседей	—	—	X	X	X	X
	xid64	компонент xid64	—	—	X	X	X	X
	ja_Compression	сжатие данных на уровне страниц	—	—	—	—	X	X
	WAL Recovery	восстановление поврежденных WAL записей	—	—	X	X	X	X
2	jaDog	компонент управления режимом работы узлов кластера	X	X	X	X	X	X
3	JDV (Jatoba data vault)	компонент контроля субъектов доступа	X	X	X	X	X	X
4	pgBadger	компонент формирования отчетов по журналам СУБД	X	X	X	X	X	X

№	Наименование	Описание	J4		J5		J6	
			Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)
5	pg_ProBackup	компонент расширенного резервного копирования	X	X	X	X	X	X
6	pg_Task	компонент планирования заданий СУБД	X	X	X	X	X	X
7	pg_Profile	компонент формирования отчетов производительности СУБД	X	X	X	X	X	X
8	JDS (Jatoba data safe)	компонент пользовательского веб-интерфейса для администраторов	X	—	X	—	X	—
9	ja_Sync_Ldap	компонент синхронизации учетных записей со службами каталогов	X	X	X	X	X	X
10	PlsPgSQL	компонент обфускации кода PL/pgSQL	X	—	X	—	X	—
11	ja_Hipe_Cluster	компонент высокопроизводительного кластера	X	X	X	X	X	X
12	ja_Log	компонент централизованного сбора записей событий СУБД	X	—	X	—	X	—
13	1c_support	компонент поддержки платформы 1С	X	X	X	X	X	X
14	fasttrun	компонент совместимости с 1С	X	X	X	X	X	X
15	fulleq	компонент совместимости с 1С	X	X	X	X	X	X
16	mchar	компонент совместимости с 1С	X	X	X	X	X	X
17	online_analyze	компонент совместимости с 1С	X	X	X	X	X	X
18	plantuner	компонент совместимости с 1С	X	X	X	X	X	X
19	ja_CSum	компонент контроля целостности	X	X	X	X	X	X
20	jaPooler	компонент балансировки подключений пользователей к СУБД	X	—	X	—	X	—
21	Oracle_FDW (Foreign data wrapper for oracle)	компонент доступа к данным СУБД Oracle	X	X	X	X	X	X

№	Наименование	Описание	J4		J5		J6	
			Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)
22	OraFCE (Oracle function compatibility extension)	компонент совместимости с СУБД Oracle	X	X	X	X	X	X
23	pg_Variables	компонент совместимости с системой глобальных переменных СУБД Oracle	X	X	X	X	X	X
24	SQL_Firewall	компонент выявления и предотвращения исполнения нетипичных SQL-запросов	X	X	X	X	X	X
25	JCS (Jatoba crypto access storage)	компонент сокрытия информации в файлах данных СУБД	X	X	X	X	X	X
26	pgSQL-HTTP	компонент формирования HTTP/HTTPS запросов из СУБД	X	X	X	X	X	X
27	TDS_FDW	компонент поддержки платформы Microsoft SQL Server	—	—	X	X	X	X
28	pgAudit	компонент расширенного журналирования событий СУБД	X	X	X	X	X	X
29	pgauditlogtofile	хранение событий безопасности в отдельном хранилище	—	—	X	X	X	X
30	PostGIS	компонент работы с географическими данными	X	X	X	X	X	X
31	PTrack	компонент расширенного резервного копирования	X	X	X	X	X	X
32	SecurityProfile	компонент управления парольными политиками пользователей СУБД	X	X	X	X	X	X
33	ja_Plan_Manager	компонент создания планов запросов в базах данных (БД), их оптимизации и экспорта в БД	X	X	X	X	X	X
34	pg_store_plans	контроль выполненных планов запросов	—	—	X	X	X	X
35	pg-hint-plan	компонент корректировки запросов	—	—	X	X	X	X
36	ja_Container	СУБД «Jatoba» в контейнере	—	X	—	X	—	X

№	Наименование	Описание	J4		J5		J6	
			Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)
37	node_exporter	компонент сбора аппаратных и программных показателей работы GNU/Linux	—	—	X	—	X	—
38	postgres_exporter	компонент сбора метрик СУБД	—	—	X	—	X	—
39	sql_exporter	SQL экспортёр. Компонент сбора расширенных метрик СУБД	—	—	X	—	X	—
40	prometheus	компонент мониторинга различных программных систем и сервисов Prometheus	—	—	X	—	X	—
41	Alertmanager	компонент управления и обработки оповещений в системе мониторинга Prometheus	—	—	X	—	X	—
42	—	Работа СУБД «Jatoba» в режиме ЗПС в ОС Astra Linux	X	—	X	—	X	—
43	gis-cryptoplatform	библиотека «ГИС»	X	—	X	—	X	—
44	pg_ulid	компонент поддержки лексографического идентификатора	—	—	X	X	X	X
45	ja_Seceventlog	компонент записи событий информационной безопасности	—	—	X	X	X	X
46	rum	компонент поддерживающий обратный индекс с хранением позиционной информации и полнотекстовый поиск	—	—	X	X	X	X
47	pg_repack	компонент реорганизации таблицы с минимальными блокировками	—	—	X	X	X	X
48	osnova-digsig-key	работа СУБД Jatoba в режиме ЗПС в ОС ОСНОВА	X	—	X	—	X	—
49	tsvector2	компонент полнотекстового поиска в БД	—	—	X	X	X	X
50	ja_Similar	компонент для полнотекстового поиска и	—	—	X	X	X	X

№	Наименование	Описание	J4		J5		J6	
			Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)	Дист.1)	Обр.к.2)
		определения похожих текстов						
51	ja_Inventory	компонент инвентаризации СУБД	X	—	X	—	X	—
52	ja_tune	Генератор конфигурационного файла	—	—	—	—	X	—

Примечание:

1) Дистрибутив.

2) Образ контейнера.

Возможна эксплуатация СУБД Jatoba с установленным сторонним компонентом «TimescaleDB» без установки других встроенных компонентов СУБД Jatoba.

2.2. Реализуемые функции СУБД

СУБД «Jatoba» реализует следующие функциональные возможности:

а) управление данными во внешней памяти;

б) управление данными в оперативной памяти;

в) выполнение запросов (DDL/DML);

г) управление транзакциями;

д) журнализация изменений, резервное копирование и восстановление базы данных после сбоев, репликация.

В дополнение к стандартным возможностям управления базами данных, реализует следующие функции:

а) хранение пространственных, географических и геометрических данных, поддержка запросов к ним и управление ими;

б) синтаксическая совместимость с распространенными PL/SQL Oracle;

в) расширенные возможности секционирования больших таблиц;

г) протоколирование, анализ и запрет выполнения команд манипулирования данными (DDL/DML);

д) сбор журналов аудита всех операций и загрузка конфигураций в СУБД;

е) журналирование операций доступа к защищенным таблицам;

ж) работа в составе отказоустойчивого кластера с механизмом переключения нагрузки на основной узел кластера;

з) защита от несанкционированного изменения конфигурационных файлов;

и) единый пользовательский интерфейс для управления конфигурациями компонентов СУБД и просмотра их состояния.

к) поддержка предустановленных профилей парольных политик:

— FSTEC_1_class – профиль для ИС первого класса защищенности;

— FSTEC_2_class – профиль для ИС второго класса защищенности;

— CIS – профиль, основанный на рекомендациях Center for Internet Security;

— Corporate_1 – корпоративный профиль первого уровня для учетных записей пользователей;

— Corporate_2 – корпоративный профиль второго уровня, для учетных записей администраторов программных (программно-аппаратных средств);

— Corporate_3 – корпоративный профиль третьего уровня для, технических (сервисных, служебных) учетных записей, используемых в технологических процессах ИС или встроенных производителями программных (программно-аппаратных) средств в такие средства.

л) СУБД «Jatoba» поддерживает методы аутентификации:

— PASSWORD;

— GSSAPI / SSPI (Kerberos);

— LDAP (LDAPS);

— PAM;

— RADIUS;

— по сертификатам (SSL/TLS).

м) синхронизация УЗ со службой каталогов/доменов (Active Directory, FreeIPA, ALD Pro, Samba).

н) ограничение создания ролей администраторами БД/СУБД.

о) создание защищенных таблиц, ограничивающих доступ суперпользователей СУБД.

п) полнотекстовый поиск и определение похожих текстов.

2.3. Основные функциональные возможности управления базами данных

СУБД «Jatoba» обладает следующими характеристиками:

1) Многоверсионность (Multiversion Concurrency Control (MVCC)). Реализована защита транзакций от несогласованных изменений данных, которые могли быть вызваны (другой) конкурентной транзакцией, и обеспечена изоляция транзакций.

2) Журналирование. Реализован механизм протоколирования всех транзакций Write Ahead Logging (WAL).

3) Поддержка журналирования выполнения транзакций независимо от результата выполнения родительской транзакции средствами администрирования и мониторинга.

4) Point in Time Recovery (PITR) – возможность восстановления базы данных (используя WAL) на любой момент в прошлом, что позволяет осуществлять непрерывное резервное копирование кластера.

5) Поддержка целостности данных на уровне схемы – внешние ключи (foreign keys), ограничения (constraints).

6) Поддержка стандартных индексов – B-tree, hash, R-tree, GiST (обобщенное поисковое дерево).

7) Поддержка частичных индексов (partial indices).

8) Поддержка функциональных индексов.

9) Наличие планировщика запросов, выполняющего оценку требуемых для выполнения запроса ресурсов и предоставляющего пользователю возможность отлаживать запросы и настраивать планы выполнения.

10) Организация хранения данных на уровне Tablespaces (табличные пространства).

11) Поддержка организации схем, которые обеспечивают пространство имен на уровне SQL.

12) Поддержка Subqueries – подзапросы (subselects), полная поддержка SQL92.

13) Поддержка Outer Joins – внешние связки (LEFT, RIGHT, FULL).

14) Поддержка Rules – правила, согласно которым модифицируется исходный запрос.

15) Поддержка Views – представления, виртуальные таблицы.

16) Поддержка Cursors – курсоры, позволяющие уменьшить трафик между клиентом и сервером.

17) Поддержка Table Inheritance – наследование таблиц.

18) Поддержка Prepared Statements (подготовленные запросы).

19) Поддержка Stored Procedures – серверные (хранимые) процедуры, позволяющие реализовывать бизнес-логику приложения на стороне сервера.

20) Поддержка табличных триггеров базы данных и триггеров событий.

21) Поддержка Savepoints (nested transactions), позволяющая отменять работу части транзакции, без влияния на оставшуюся часть транзакции.

22) Поддержка права доступа к объектам системы на основе системы привилегий, разграничения доступа к таблицам на уровне строк, интеграции с подсистемой SE-Linux.

23) Высокогранулярный контроль доступа к объектам БД (например - вплоть до поля в таблице или видимость строки по условию на поле).

24) Cluster table – упорядочивание записей таблицы на диске согласно индексу.

25) Поддержка массивов стандарту SQL:2003.

26) Поддержка транзакций, обеспечивающих атомарность, согласованность, изолированность, долговечность (ACID).

27) Поддержка механизма исправления повреждённых данных WAL из буферов в оперативной памяти.

28) Наличие встроенных средств для построения кластеров высокой доступности с автоматическим восстановлением узлов.

29) Поддержка размещения файлов данных на NFS.

30) Возможность передачи событий безопасности в системы информационно-технологического мониторинга и системы учета событий информационной безопасности.

31) Наличие механизма управления подключений к системе управления базами данных.

32) Наличие единого пользовательского интерфейса для оценки состояния СУБД.

33) Поддержка функциональных возможностей OLAP;

34) Поддержка механизмов прямой и обратной сортировки.

35) Поддержка механизмов сортировки по пользовательскому словарю.

36) Наличие средств мониторинга экземпляра БД в разрезе событий, сессией, процессов.

37) Поддержка параллельного экспорта/импорта данных.

38) Поддерживаемая гранулярности экспорта/импорта (при выполнении экспорта/импорта существует возможность экспортировать/импортировать как всю БД, так и отдельные схемы, таблицы, данные, метаданные).

39) Наличие механизмов оперативного обмена данными с другими БД того же типа по установленным каналам (DBLINK).

40) Поддержка 64-битного счетчика транзакций.

41) Поддержка работы в многопоточном режиме (Hyper-Threading Technology).

42) Поддержка неблокируемых операций с индексами (создание/удаление индексов без существенного влияния на другие протекающие с данной таблицей операции).

43) Поддержка проведения распределённых транзакций.

44) Поддержка синхронной и асинхронной репликации данных между несколькими БД одного и того же типа.

45) Работа в составе географически распределенного кластера с автоматическим механизмом переключения нагрузки на основной узел кластера;

46) Поддержка простого секционирования таблиц;

47) Поддержка создания зеркальной копии БД пересылкой блоков данных (так называемый «Теплый режим ожидания»).

2.4. Поддерживаемые типы данных

СУБД «Jatoba» поддерживает следующие типы данных:

1) Символьные типы данных (CHARACTER(n)), определенные в стандарте SQL, VARCHAR(n), и типа TEXT с практически неограниченной длиной.

2) Numeric – тип с произвольной точностью.

3) Числовые типы данных – знаковое целое из 8 байт, восьмибайтное целое с автоувеличением, битовая строка фиксированной длины, битовая строка переменной длины, логическое значение (true/false).

4) Типы данных времени с точностью до микросекунд:

— DATE – время суток без даты;

— TIME – дата и время с учетом часового пояса;

— TIMESTAMP – время суток с учетом часового пояса;

— TIMESTAMP WITH TIMEZONE – дата и время (без часового пояса);

— INTERVAL – интервал времени.

5) Геометрические типы данных (point, line, circle, polygon, box) – для работы с пространственными данными на плоскости.

6) Сетевые типы данных (Network types) – inet для IPv4, IPv6, а также CIDR (Classless Internet Domain Routing) блоки и macaddr.

7) Композитные типы данных (composite types).

8) Типы данных «ключ-значение» (noSQL).

9) Псевдотипы данных SERIAL и BIGSERIAL, позволяющие организовать упорядоченную последовательность целых чисел.

10) Целые типы данных: INT, SMALLINT, BIGINT.

11) Типы с плавающей точкой: REAL, DOUBLE PRESISION, FLOAT.

12) Логический тип BOOLEAN.

13) Битовые строки.

14) XML, JSON и JSONB.

СУБД обеспечивает возможность добавления новых типов данных, функций, операторов, методов доступа, языков программирования без перекомпилирования ядра системы и остановки сервера.

2.5. Поддерживаемые типы индексов

СУБД поддерживает следующие типы индексов:

1) Стандартные индексы – B-tree, hash, GiST (обобщенное поисковое дерево), B+-tree, ranked B+-trees, R-tree, partial sum trees, GIN (обобщенный инвертированный индекс).
2) Частичные индексы (partial indices).
3) Функциональные индексы.
4) Индексы типа «битовая карта».

Поддержка технологий расширенного индексирования (поддержка секционированных индексов, индексирование XML и т.д.).

Поддержка индексов типа «битовая карта» или аналогичных механизмов для эффективной обработки данных с низкой кардинальностью.

2.6. Поддерживаемые методы стандартизации и унификации

СУБД поддерживает следующие стандартные, унифицированные типы данных:

1) Доступ к данным по протоколу ODBC/JDBC.
2) Поддержка стандарта ANSI SQL (ANSI cyrillic).
3) Поддержка кодировки UTF8 (CP866, WIN1251).

СУБД поддерживает стандарт SQL от ISO/IEC 9075:2008.

СУБД обеспечивает поддержку хранения и обработки запросов к пространственным данным с помощью встроенных операторов (в том числе в соответствие со стандартами OGC (ISO 19125-1:2004 и ISO 19125-2:2004). Поддержка картографических проекций, инструментов и SQL-выражений работы с пространственными данными, включая перепроецирование, встроенные операторы (пересечение, включение и т.п.) и пространственные индексы.

2.7. Расширенные функциональные возможности управления базами данных

СУБД «Jatoba» обеспечивает:

1) Отсутствие ограничения на размер БД.
2) Отсутствие ограничения на максимальное количество записей.
3) Отсутствие ограничения на количество индексов.
4) Поддержку таблиц вплоть до 16 ТБ и более.
5) Поддержку записей (строк) до 1 ТБ и более.

6) Поддержку не менее 100 столбцов в одной таблице.

7) Поддержку BLOB (Binary Large Object) до 2 ГБ.

8) Поддержку многоядерных серверов, имеющих больше 256 ядер.

9) Возможность фонового конвертирования данных в различных кодировках.

10) Поддержку параллельных многоядерных операций (SMP).

11) Поддержку параллельного выполнения запроса несколькими процессами/ядрами.

12) Поддержку технологий VLDB/NLDB.

2.8. Механизм защиты подключений к системе управления базами данных

СУБД «Jatoba» соответствует следующим требованиям к механизму защиты подключений к системе управления базами данных:

1) Обрабатываемые команды DDL/DML должны проходить аудит и регистрироваться в журнале.

2) Должен быть реализован сбор журналов аудита всех операций и загрузка конфигураций в СУБД.

2.9. Требования к среде функционирования СУБД

Допускается установка СУБД «Jatoba» на ЭВМ, функционирующие под управлением ОС, указанных в таблице 2.2.

Таблица 2.2 – Поддерживаемые операционные системы

№	Наименование ОС	Серверная часть	Клиентская часть	Docker (ver.)	Сертификат ФСТЭК	
					№ серт.	Дата выдачи
1	Windows 10	X	X	—	—	—
2	Windows 11	X	X	—	—	—
3	Windows Server 2016	X	X	—	—	—
4	Windows Server 2019	X	X	—	—	—
5	Windows Server 2022	X	X	—		
6	Astra Linux 1.6 Special Edition Смоленск (x86-64)	X	X	25.0.5	2557	30.01.2012
7	Astra Linux 1.7 Special Edition Смоленск (x86-64)	X	X	25.0.5	2557	30.01.2012
8	Astra Linux 1.8 (x86-64)	X	X	—		

№	Наименование ОС	Серверная часть	Клиентская часть	Docker (ver.)	Сертификат ФСТЭК	
					№ серт.	Дата выдачи
9	Astra Linux 2.12 Common Edition Орел (x86-64)	X	X	24.0.2	—	—
10	Debian 10	X	X	24.0.2	—	—
11	Debian 11	X	X	24.0.2	—	—
12	Debian 12	X	X	27.1.1	—	—
13	Альт 8 СП	X	X	27.1.1	3866	10.08.2018
14	Альт 9.1 Server	X	X	—		
15	Альт 10 Server	X	X	23.0.1	—	—
16	Ubuntu 20.04	X	X	24.0.2	—	—
17	Ubuntu 22.04	X	X	24.0.2	—	—
18	Ubuntu 24.04	X	X	24.0.2	—	—
19	ОСНОВА2	X	X	20.10.5	4381	31.03.2021
20	РЕД ОС 7.3 Муром	X	X	20.10.1	4060	12.01.2019
21	РЕД ОС 8	X	X			
22	РОСА 7.9	X	X			
23	РОСА 12.4	X	X			
24	RedHat Enterprise Linux 8.2	X	X	—	—	—
25	Oracle Linux 8	X	X	—	—	—

СУБД «Jatoba» устанавливается на ЭВМ с процессорами, имеющими архитектуру x86-64, ARM64 и AMD64, удовлетворяющие следующим аппаратным требованиям, указанным в таблице 2.3.

Таблица 2.3 – Аппаратные требования к ЭВМ, на которых фукционируют клиентская и серверная части СУБД

Параметр	Характеристика	Серт-я ОС
Требования к аппаратному обеспечению сервера СУБД/JDS		
ОЗУ	Не менее 2 Гб	
Свободный объем жесткого диска	Минимальный объем от 40 Гб Рекомендуемый объем от 100 Гб	
Устройства видео вывода	Монитор и видеоадаптер с поддержкой VGA и разрешением 800x600 или выше	
Тип процессора и минимальная тактовая частота процессора	64-разрядный процессор Intel или AMD 3 ГГц или больше	
Минимальное количество ядер	4	

Параметр	Характеристика	Серт-я ОС
Устройства ввода-вывода	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB, либо PS/2 интерфейсами	
Адаптер Ethernet	100 Мбит/с	
Требования к аппаратному обеспечению АРМ управления		
ОЗУ	Не менее 4 Гб	
Свободный объем жесткого диска	От 3 Гб	
Устройства видео вывода	Монитор и видеоадаптер с поддержкой VGA и разрешением 800x600 или выше	
Тип процессора и минимальная тактовая частота процессора	64-разрядный процессор Intel или AMD Рекомендуемая частота: 2.4 ГГц или больше	
Устройства ввода-вывода	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB-интерфейсами либо PS/2 интерфейсами	
Адаптер Ethernet	100 Мбит/с	
Требования к программному обеспечению сервера		
Операционная система	Требования приведены в таблице 2.2	
Требования к программному обеспечению АРМ управления		
Операционная система	Требования приведены в таблице 2.2	
Требования к программному обеспечению сервера JDS		
Поддерживаемые платформы	• win-x86;	—
	• win-x64;	—
	• linux-x64	X
СУБД	Защищенная система управления базами данных «Jatoba»	
Веб-сервер	IIS 10	—
	nginx	X
Компоненты	ASP.NET Core 6.0 Runtime (v6.0.1) – Windows Hosting Bundle Installer	—
Internet браузеры сертифицированных ОС	• Яндекс.Браузер	X
	• Chromium	X
	• Mozilla Firefox	X
Internet браузеры ОС	• Google Chrome	—
	• Opera	—

2.10. Функции по защите информации

Функции по защите информации подробно описаны в документе «Реализация функций безопасности».

В таблице 2.4 приведены выполняемые меры защиты информации в соответствии с Приказами ФСТЭК России № 17 от 11.02.2013 (ред. от 28.08.2024), № 21 от 18.02.2013 (ред. от 04.05.2020), № 31 от 14.03.2014 (ред. от 15.03.2021), № 239 от 25.12.2017 (ред. от 28.08.2024) и ГОСТ Р 57580.1-2017 от 08.08.2017.

Таблица 2.4 – Реализуемые меры защиты информации

Наименование	**J4**		**J5**		**J6**		**Приказы ФСТЭК**		
							ГИС	**ИСПДн**	**КИИ и КВО**
	Дист.[1)]	**Обр.к.[2)]**	**Дист.[1)]**	**Обр.к.[2)]**	**Дист.[1)]**	**Обр.к.[2)]**	**№17**	**№21**	**№239, №31**
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	X	X	X	X	X	X	ИАФ.1	ИАФ.1	ИАФ.1
	X	X	X	X	X	X	ИАФ.3	ИАФ.3	ИАФ.3
	X	X	X	X	X	X	ИАФ.4	ИАФ.4	ИАФ.4
							ИАФ.4(1г)	—	—
	—	—	X		X	X	ИАФ.4(2)	—	—
	X	X	X	X	X	X	ИАФ.5	ИАФ.5	—
Управление доступом субъектов доступа к объектам доступа (УПД)	X	X	X	X	X	X	УПД.1	УПД.1	УПД.1
	X	X	X	X	X	X	УПД.1(1)	—	—
	X	X	X	X	X	X	УПД.1(2)	—	—
	X	X	X	X	X	X	УПД.1(3б)	—	—
	—	—	X	—	X	—	УПД.1(5)	—	—
	X	X	X	X	X	X	УПД.2	УПД.2	УПД.2
	X	X	X	X	X	X	УПД.2(1)	—	—
	X	—	X	—	X	—	УПД.4	УПД.4	УПД.4
	X	X	X	X	X	X	УПД.5	УПД.5	УПД.5
	X	X	X	X	X	X	УПД.6	УПД.6	УПД.6
	X	X	X	X	X	X	УПД.6(1)	—	—
	X	X	X	X	X	X	УПД.9	УПД.9	УПД.9
	X	X	X	X	X	X	УПД.9(3)	—	—
	—	—	X	—	X	—	УПД.9(4)	—	—
Регистрация событий безопасности (РСБ)	—	—	X	X	X	X	РСБ.1	РСБ.1	—
	—	—	X	X	X	X	РСБ.1(4а)	—	—
	X	X	X	X	X	X	РСБ.2(1а)	—	—
	X	X	X	X	X	X	РСБ.3	РСБ.3	АУД.4
	X	—	X	—	X	—	РСБ.3(1)	—	—
	X	X	X	X	X	X	РСБ.6	РСБ.6	АУД.3

Наименование	J4		J5		J6		Приказы ФСТЭК		
							ГИС	ИСПДн	КИИ и КВО
	Дист.[1]	Обр.к.[2]	Дист.[1]	Обр.к.[2]	Дист.[1]	Обр.к.[2]	№17	№21	№239, №31
	X	X	X	X	X	X	РСБ.7	РСБ.7	АУД.6
	X	X	X	X	X	X	РСБ.8	—	АУД.9
							РСБ.8(1)	—	—
Обеспечение целостности информационной системы и информации ОЦЛ)	X	X	X	X	X	X	ОЦЛ.1	ОЦЛ.1	ОЦЛ.1
	X	X	X	X	X	X	ОЦЛ.2	ОЦЛ.2	ОЦЛ.2
	X	X	X	X	X	X	ОЦЛ.7	ОЦЛ.7	ОЦЛ.4
Обеспечение доступности информации (ОДТ)	X	—	X	—	X	—	ОДТ.4	ОДТ.4	ОДТ.4
	X	—	X	—	X	—	ОДТ.5	ОДТ.5	ОДТ.5
	X	—	X	—	X	—	ОДТ.6 (2)	—	ОДТ.7

Примечание:

1) Дистрибутив

2) Образ контейнера.

Сопоставление выполняемых меры защиты информации в соответствии с Приказами ФСТЭК России № 17 от 11.02.2013, № 21 от 18.02.2013, № 31 от 14.03.2014, № 239 от 25.12.2017 и требований по безопасности информации по Приказу ФСТЭК России № 64 от 14.04.2023 приведено в таблице 2.5.

Таблица 2.5 – Функции и требования по защите информации

№	J4		J5		J6			Приказы ФСТЭК		
								ГИС	ИСПДн	КИИ и КВО
	Дист.[1]	Обр.к.[2]	Дист.[1]	Обр.к.[2]	Дист.[1]	Обр.к.[2]	№64	№17	№21	№239, №31
1	X	X	X	X	X	X	Идентификация и аутентификация пользователей в СУБД (ИАФ)	Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
2	X	X	X	X	X	X	Управление доступом в СУБД (УПД)	Управление доступом субъектов доступа к объектам доступа (УПД)		
3	X	X	X	X	X	X	Контроль целостности в СУБД (ОЦЛ)	Обеспечение целостности информационной системы и информации (ОЦЛ)		

№	J4		J5		J6			Приказы ФСТЭК		
								ГИС	ИСПДн	КИИ и КВО
	Дист.[1]	Обр.к.[2]	Дист.[1]	Обр.к.[2]	Дист.[1]	Обр.к.[2]	№64	№17	№21	№239, №31
4	X	X	X	X	X	X	Регистрация событий безопасности в СУБД (РСБ)	Регистрация событий безопасности (РСБ)		
5	X	—	X	—	X	—	Резервное копирование и восстановление в СУБД (ОДТ)	Обеспечение доступности информации (ОДТ)		
6	X	—	X	—	X	—	Обеспечение доступности СУБД (ОДТ)	Обеспечение доступности информации (ОДТ)		
7	X	X	X	X	X	X	Ограничение программной среды в СУБД (ОПС)			

Примечание:

1) Дистрибутив.
2) Образ контейнера.

2.11. Производительность СУБД

СУБД должна обеспечивать требования по производительности, указанные в таблице 2.6.

Таблица 2.6 – Требования к производительности СУБД

№	Параметр производительности	J4		J5		J6	
		Серверная часть, исполнение		Серверная часть, исполнение		Серверная часть, исполнение	
		Дист.	Обр.к.	Дист.	Обр.к.	Дист.	Обр.к.
1	Количество пользовательских сессий, поддерживаемых параллельно	800	750	800	750	800	750
2	Количество обрабатываемых стандартных запросов в единицу времени (сек)	3650	3475	3520	3305	3540	3420
		(256 сессий)	(128 сессий)	(256 сессий)	(128 сессий)	(256 сессий)	(128 сессий)
3	Количество транзакций в единицу времени (ед/сек)	730	695	704	661	725	643
		(256 сессий)	(128 сессий)	(256 сессий)	(128 сессий)	(256 сессий)	(128 сессий)
4	Задержка в выполнении стандартного запроса (сек)	мин. 13,5 (1 сессия)	мин. 14,4 (1 сессия)	мин. 13,9 (1 сессия)	мин. 15,9 (1 сессия)	мин. 13,6 (1 сессия)	мин. 15,8 (1 сессия)
		макс. 5558 (800 сессий)	макс. 5724 (750 сессий)	макс. 5222 (800 сессий)	макс. 7475 (700 сессий)	макс. 5222 (800 сессий)	макс. 7475 (700 сессий)
		348 (256 сессий)	210 (128 сессий)	441 (256 сессий)	191 (128 сессий)	446 (256 сессий)	198 (128 сессий)
5	Количество экземпляров системы управления базами данных, которые могут совместно	2 – 8	2 – 8	2 – 8	2 – 8	2 – 8	2 – 8

№	Параметр производительности	J4		J5		J6	
		Серверная часть, исполнение		Серверная часть, исполнение		Серверная часть, исполнение	
		Дист.	Обр.к.	Дист.	Обр.к.	Дист.	Обр.к.
	работать в режиме балансировки нагрузки						

№ изменения:_____	Подпись отв. лица:_____	Дата внесения изм.:_____

3. РЕШАЕМЫЕ ЗАДАЧИ

Использование СУБД «Jatoba» позволяет решать следующий ряд задач:

— Установка с помощью инсталлятора СУБД и компонента «Jatoba Data Safe» под ОС Windows и GNU/Linux (п. 3.1);

- Установка СУБД с рекомендуемой, генерируемой конфигурацией, компонентом «ja_tune»;

— Балансировка нагрузки на СУБД (п. 3.2);

— Кластеризация СУБД (п. 3.3):

- Кластеры на основе компонента ja_Dog. Инженерные решения (3.3.1);
- Отказоустойчивый кластер в Kubernetes (п. 3.3.2);
- Управление кластером ja_Dog через веб-интерфейс JDS (п. 3.3.3).

— Секционирование (шардирование) больших таблиц (п. 3.4);

— Мониторинг и управление СУБД (п. 3.5):

- Раздел «Мониторинг» (п. 3.5.1);
- Раздел «Анализ рисков» (User Risk) (п. 3.5.2);
- Раздел «Матрица доступа» (Access matrix) (п. 3.5.3.1);
- Раздел «Кластеры» (п. 3.5.4);
- Раздел «Список событий» (Event List) (п. 3.5.3.2);
- Раздел «Снимки и отчеты» (Snapshots & Reports) (п. 3.5.5.1);
- Раздел «Проблемы и решения» (Problems & Solutions) (п. 3.5.5.2);
- Раздел «Анализ запросов» (Query analysis) (п. 3.5.5.3)
- Раздел «Активность БД» (п. 3.5.5.4);
- Раздел «LDAP синхронизация» (п. 3.5.6);
- Раздел «Роли БД» (DB roles) (п. 3.5.7);
- Раздел «Уведомления» (Notifications) (п. 3.5.8)
- Раздел «Парольные политики» (п. 3.5.10);
- Раздел «Ландшафт» (Landscape) (п. 3.5.10);
- Раздел «Резервное копирование» (BACKUP) (п. 3.5.11).

— Резервное копирование (п. 3.6);

— Маскирование данных (п. 3.7);

— Поддержки платформы Oracle (п. 3.8);

- Поддержка платформы MS SQL (п. 3.9);
- Совместимость платформой с 1С (п. 3.10);
- Управление планами запросов (п. 3.11);
- Выявления и предотвращение исполнения нетипичных SQL-запросов (п. 3.11.1);
- Регистрация событий безопасности (п. 3.13);
  - Расширенная регистрация событий (п. 3.13.1);
  - Регистрация событий безопасности в соответствии с ГОСТ-Р-59548-2022 (п. 3.13.3);
  - Централизованный собор событий безопасности (3.13.3).
- Парольные политики (п. 3.14);
- Поддержка работы СУБД с геоданными (п. 3.15);
- Контроль целостности (п. 3.16);
- Обфускации (маскирование) кода хранимых процедур на языке PL/pgSQL (п. 3.17);
- Формирование HTTP/HTTPS запросов из СУБД (п. 3.18);
- Компрессия данных (п. 3.19);
- Полнотекстовый поиск и определение похожих текстов (п. 3.20);
- Метод поиска KNN (п. 3.21);
- 64-битный счетчик транзакций (п. 3.22);
- Инвентаризация СУБД (п. 3.22);
- Разрешение или запрет действий пользователей (п. 3.24).

3.1. Инсталлятор

Процесс установки СУБД облегчен входящими в поставку инсталляторами, которые автоматизируют рутинные операции.

Под ОС семейства Windows ядро СУБД и компоненты устанавливаются при помощи инсталлятора.

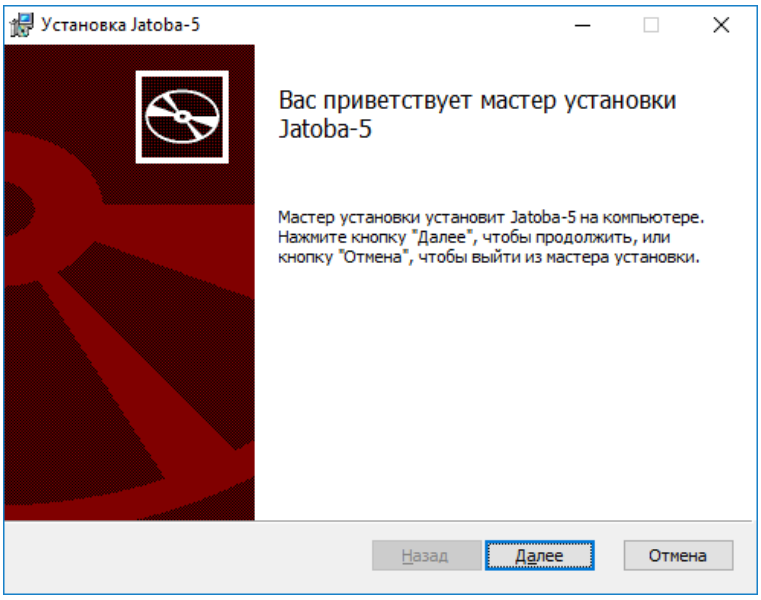


Рисунок 3.1 – Запуск мастера установки

Основные пакеты ядра СУБД под ОС GNU/Linux могут устанавливаться инсталлятором.

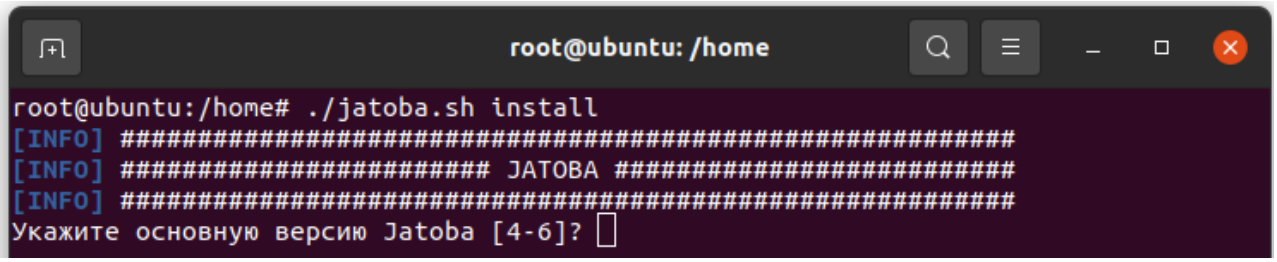


Рисунок 3.2 – Окно инсталлятора ОС GNU/Linux

Сохранен режим установки СУБД под GNU/Linux из локального репозитория.

```
root@ubuntu: /localrepo
File  Edit  View  Search  Terminal  Help
root@ubuntu:/localrepo# apt-get install jatoba4-client jatoba4-contrib jatoba4-l
ibs jatoba4-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  gis-activator11 libevent-core-2.1-6 libevent-pthreads-2.1-6
The following NEW packages will be installed:
  gis-activator11 jatoba4-client jatoba4-contrib jatoba4-libs jatoba4-server
  libevent-core-2.1-6 libevent-pthreads-2.1-6
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 91.1 kB/10.5 MB of archives.
After this operation, 50.0 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Рисунок 3.3 – Установка основных пакетов

Установка компонента пользовательского веб-интерфейса для администраторов «Jatoba data safe» может выполняться:

1) Инсталлятором компонента на ОС Windows.

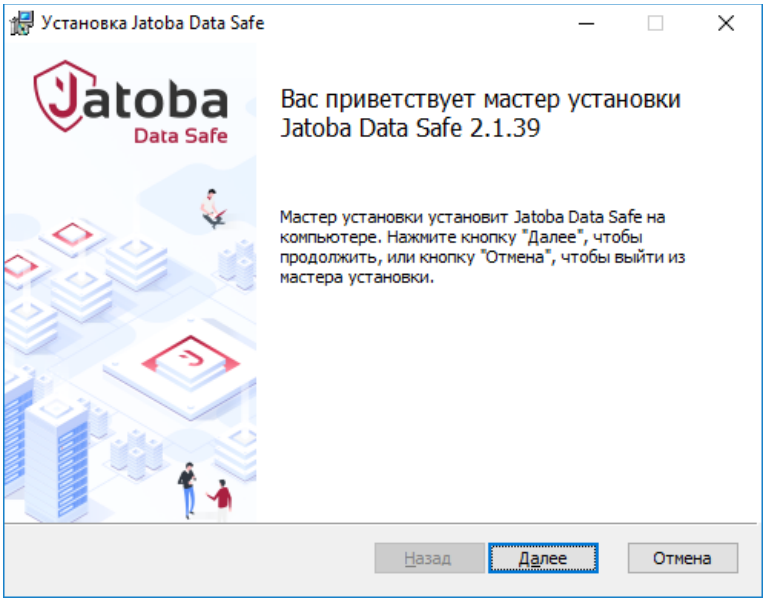


Рисунок 3.4 – Окно инсталлятора JDS на ОС Windows

2) Вручную из архива.

3) Инсталлятором компонента JDS под ОС GNU/Linux.

```
root@jds-virtual-machine: /usr/share/jds
File  Edit  View  Search  Terminal  Help
root@jds-virtual-machine:/usr/share/jds#
root@jds-virtual-machine:/usr/share/jds# cd ./utils/
root@jds-virtual-machine:/usr/share/jds/utils# sudo bash nginx.sh install -y
[INFO] Nginx installation is started.
dpkg-query: package 'nginx' is not installed and no information is available
Use dpkg --info (= dpkg-deb --info) to examine archive files,
and dpkg --contents (= dpkg-deb --contents) to list their contents.
Reading package lists... Done
Building dependency tree
Reading state information... Done
ca-certificates is already the newest version (20211016ubuntu0.18.04.1).
wget is already the newest version (1.19.4-1ubuntu2.2).
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
[INFO] Add nginx local repository to /etc/apt/sources.list.d/nginx.list
mv: cannot stat 'tmp': No such file or directory
OK
Get:1 file:/localrepo stable InRelease [2,125 B]
Get:2 file:/usr/share/jds/jds-deb ./ InRelease
Ign:2 file:/usr/share/jds/jds-deb ./ InRelease
Get:3 file:/usr/share/jds/jds-deb ./ Release
```

Рисунок 3.5 – Инсталлятор JDS под ОС GNU/Linux

3.1.1. Установка СУБД с рекомендуемой, генерируемой конфигурацией, компонентом «ja_tune»

Установка СУБД с рекомендуемыми, генерируемыми параметрами возможна при ручной установке.

Компонент «ja_tune», на основе данных об аппаратной платформе, на которой предполагается запускать экземпляр СУБД, данных операционной системы, предполагаемом профиле нагрузки СУБД и некоторых дополнительных параметрах генерирует рекомендуемые параметры конфигурационного файла «postgresql.conf».

Например

Вывод результатов в файл с добавлением результатов в конец файла

```
./ja_tune --workload web --os Linux -- ram 2 GB --cpu 2 --
maxconn 10 --pgversion 14.0 --strgtype ssd --replication
true --syncommit true >> pairwise1_web.cfg
```

3.2. Балансировка нагрузки

Помимо базовых механизмов СУБД для балансировки и оптимизации запросов пользователей к СУБД используется компонент «jaPooler».

Компонент имеет функциональную возможность оптимизировать запросы от пользователя(ей) к серверу при их подключении к серверу СУБД на указанный порт, как представлено на рисунке 3.6.

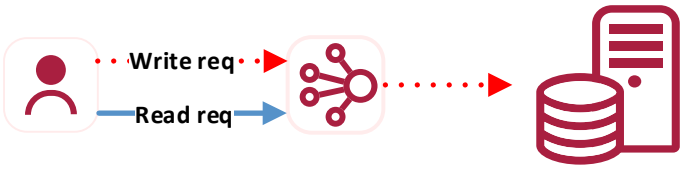


Рисунок 3.6 – Балансировка запросов пользователя

Также компонент обладает функциональной возможностью балансировки подключений множества пользователей к серверам СУБД, как представлено на рисунке 3.7.

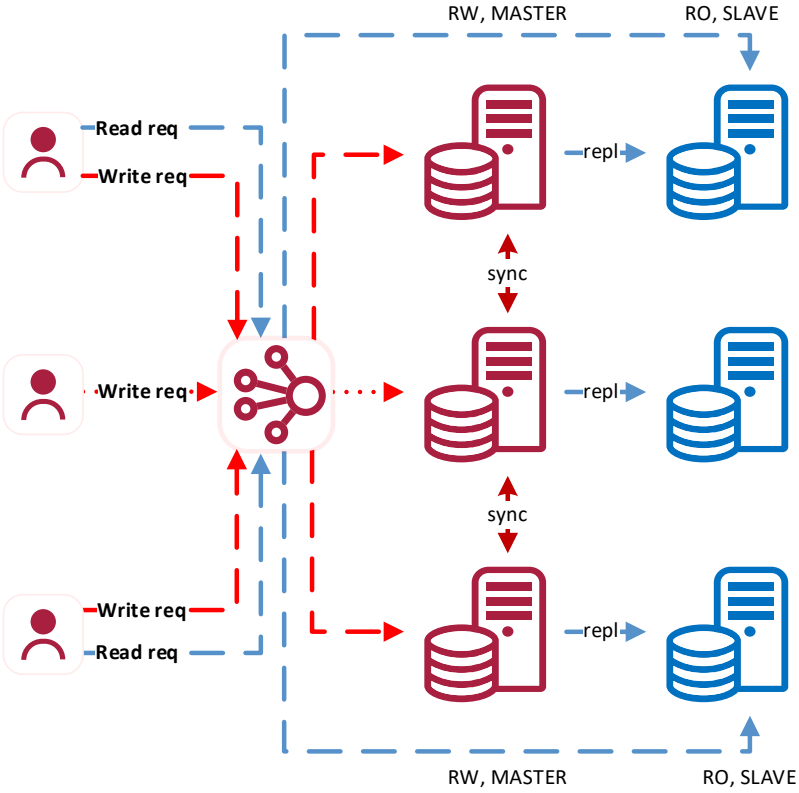


Рисунок 3.7 – Балансировка запросов пользователей к серверам СУБД

Подключения формируются как от пользователей, так и от пользовательских приложений.

3.3. Кластеризация

Отказоустойчивость в СУБД «Jatoba» реализуется средствами репликации данных компонентом «ja_Dog». Экземпляр СУБД может выступать в роли ведущего

или ведомого сервера. Роль сервера определяется соответствующими конфигурационными параметрами, заданными администратором СУБД. Ведомый сервер всегда зависит от ведущего и получает от него все изменения данных, которые накапливаются в журнале транзакций. В случае выхода из строя ведущего сервера, ведомый сервер может автоматически или по команде администратора принять на себя роль ведущего. После восстановления функционирования сервера ему снова может быть возвращена роль ведущего.

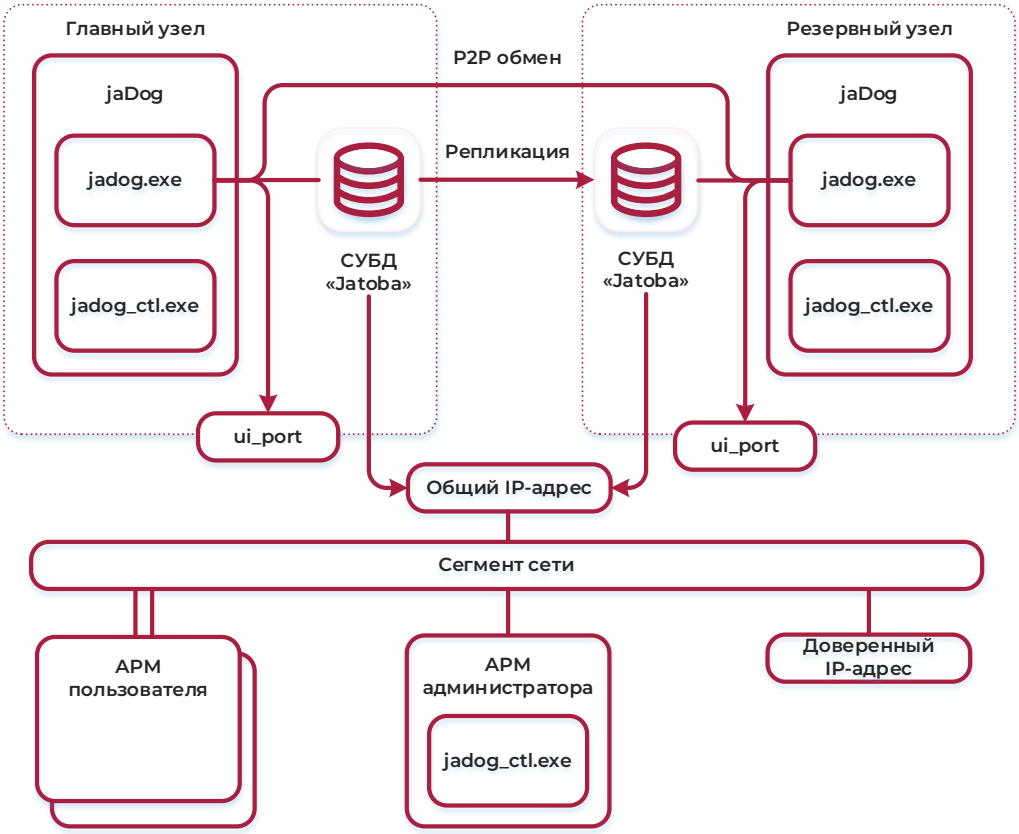


Рисунок 3.8 – Физическая структура узлов кластера

Базовые функциональные возможности кластера расширены до полнофункциональных инженерных решений катастрофоустойчивого и георасределенного кластера.

3.3.1. Инженерные решения построения кластера

Функциональные возможности компонента ja_Dog позволяют построить кластер различных конфигураций и приведенных в таблице 3.2. настоящего документа.

Развёртывание кластеров может проходить как в ручном, так и в полуавтоматическом режиме с использованием файлов ответов *.yml.

Таблица 3.1 – Инженерные решения компонента «ja_Dog»

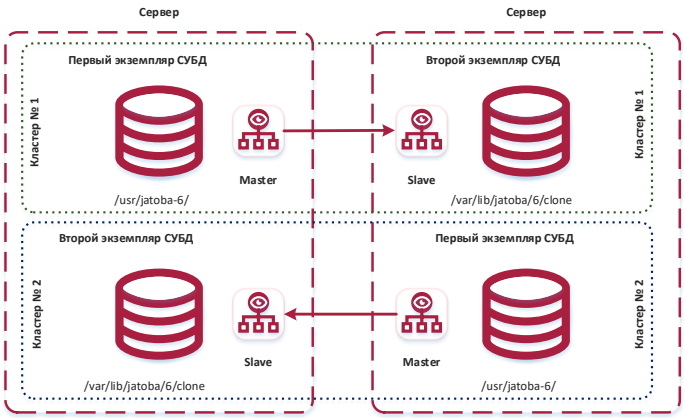
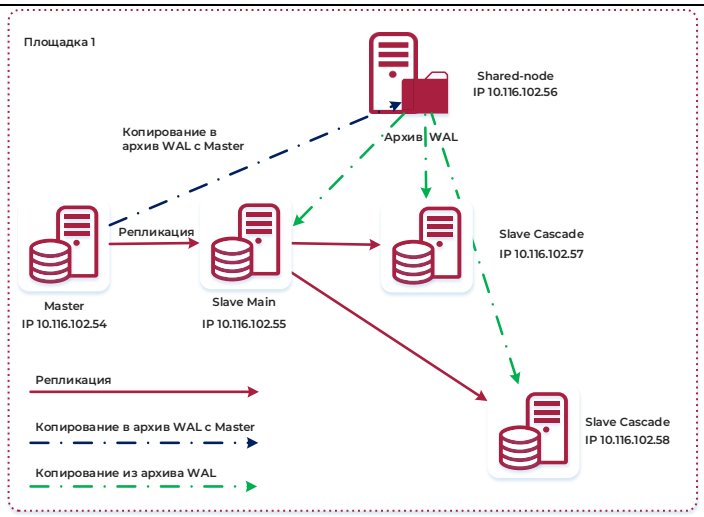
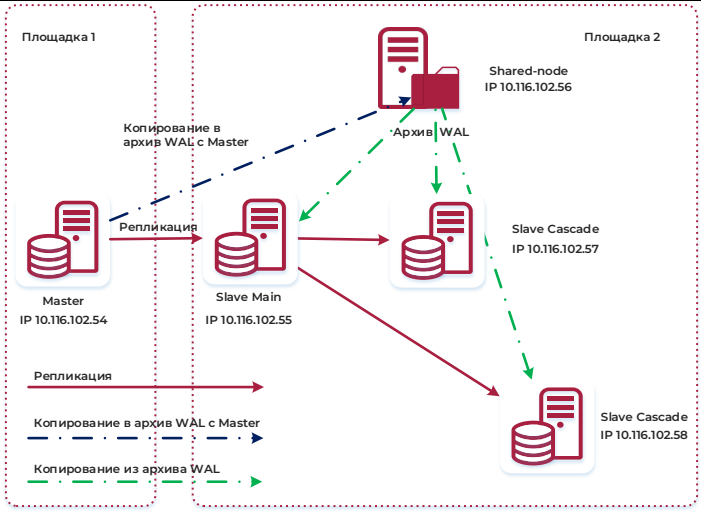
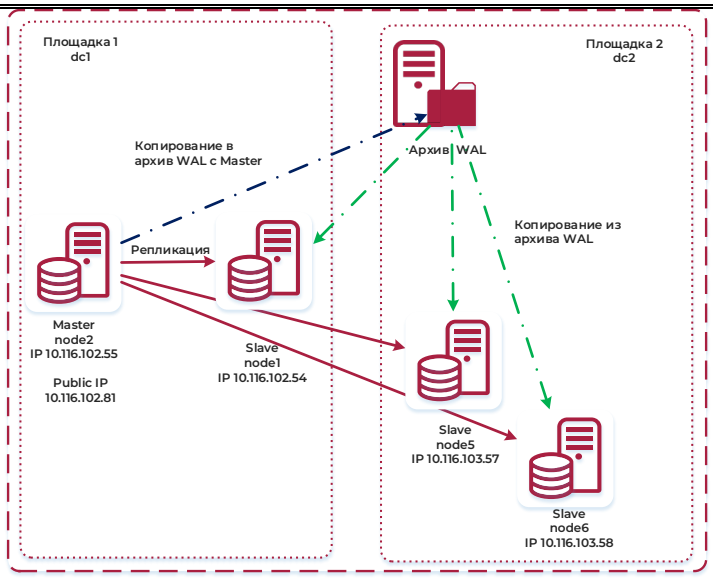
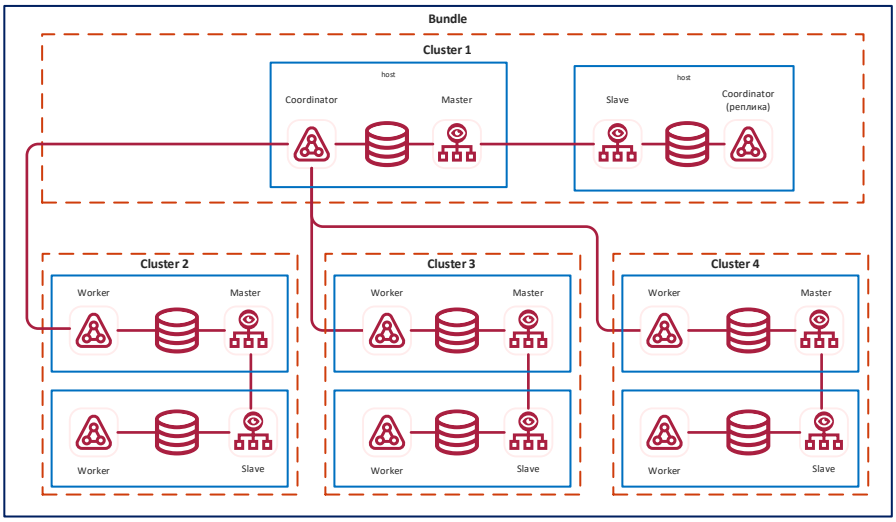
Схема работы компонента	**Разделы описания инженерного решения во 2-ой части руководства ja_Dog**
	1. Перекрестная репликация. Использование файлов ответов 2. Перекрестная репликация. Настройка в ручном режиме
	3. Каскадная репликация. Использование файлов ответов 4. Каскадная репликация. настройка в ручном режиме
	4.4. Работа кластера с каскадной репликацией в дата-центрах

Схема работы компонента	Разделы описания инженерного решения во 2-ой части руководства ja_Dog
	5. Георасределенный, отказоустойчивый кластер. Решение JA_DTC_AS
	Кластер на основе компонентов ja_Dog и ja_Hipe_Cluster 8. Настройка общего кластера (bundle) с компонентом «jadog» в ручном режиме.

3.3.2. Отказоустойчивый кластер в Kubernetes

СУБД «Jatoba» может применяться в составе продукта CloudNativePG, позволяющего развертывать предварительно сконфигурированный отказоустойчивый кластер в окружении Kubernetes. Текущая реализация кластера CNPG использует физическую потоковую репликацию.

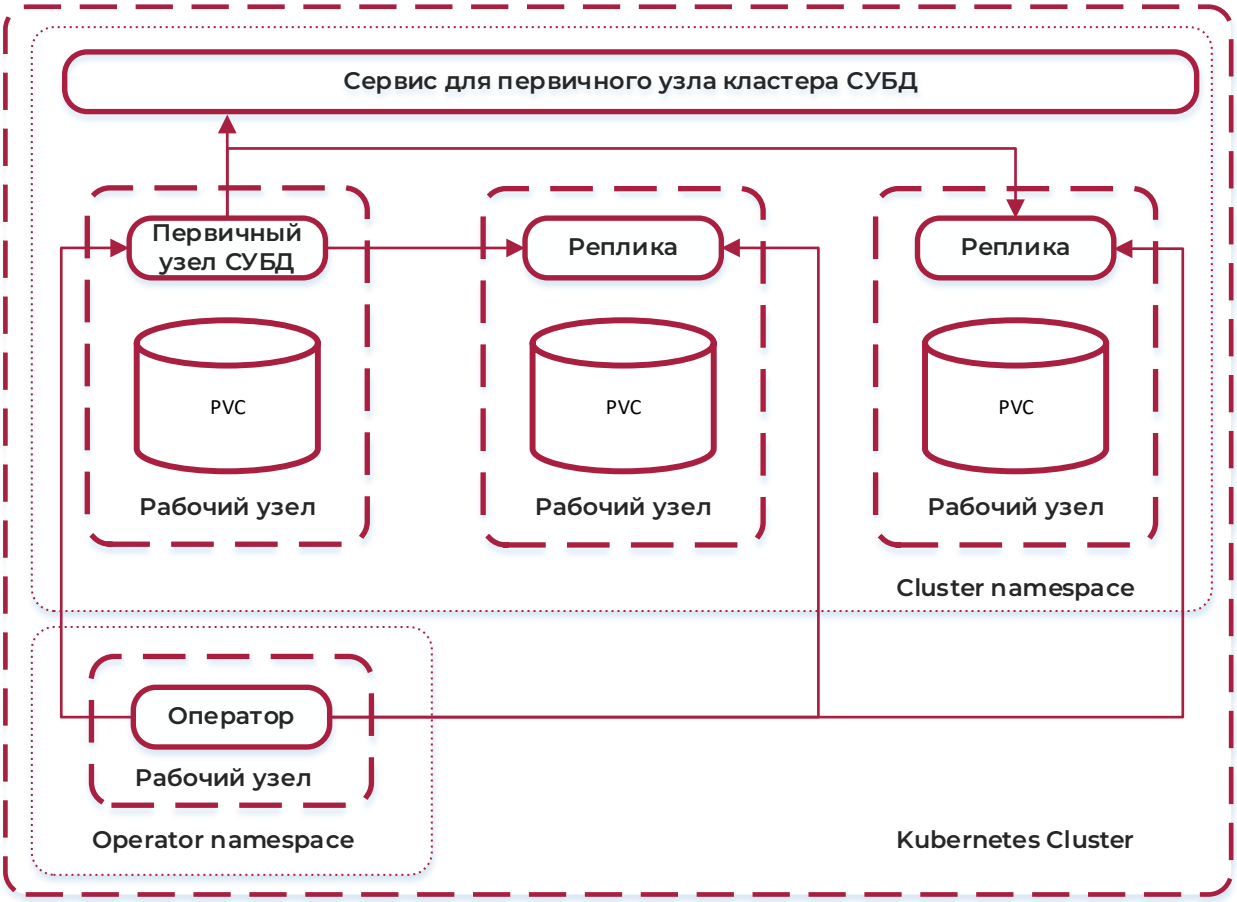


Рисунок 3.9 – Архитектура кластера, устанавливаемого с помощью CloudNativePG

3.3.3. Управление кластером ja_Dog в JDS

На уровне компонента пользовательского веб-интерфейса для администраторов «Jatoba data safe» поддерживаются функциональные возможности:

— создание кластера (Create cluster);

— назначение роли «Мастер» (Make a master);

— добавление узла в кластер (Add new node);

— удаление выбранного узла (Delete selected node);

— активация PUBLIC IP;

— деактивация PUBLIC IP;

— управление параметрами кластера.

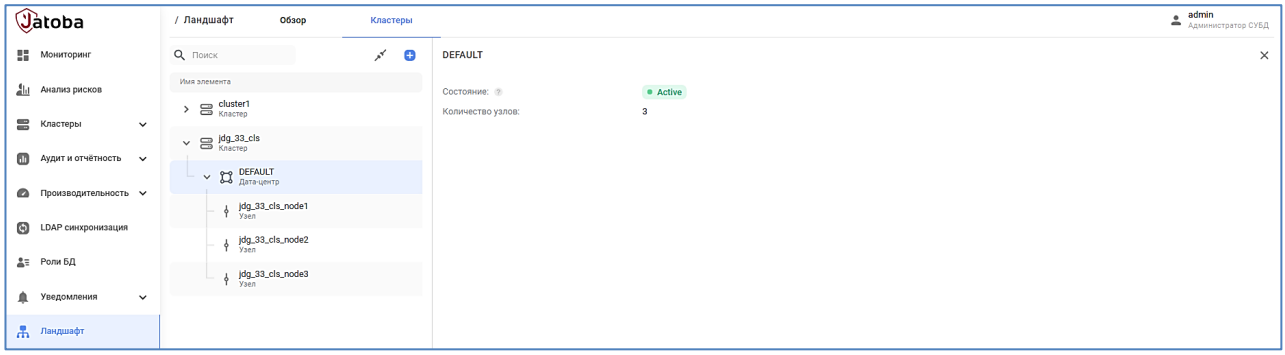


Рисунок 3.10 – Вид раздела «Список кластеров» (Cluster list)

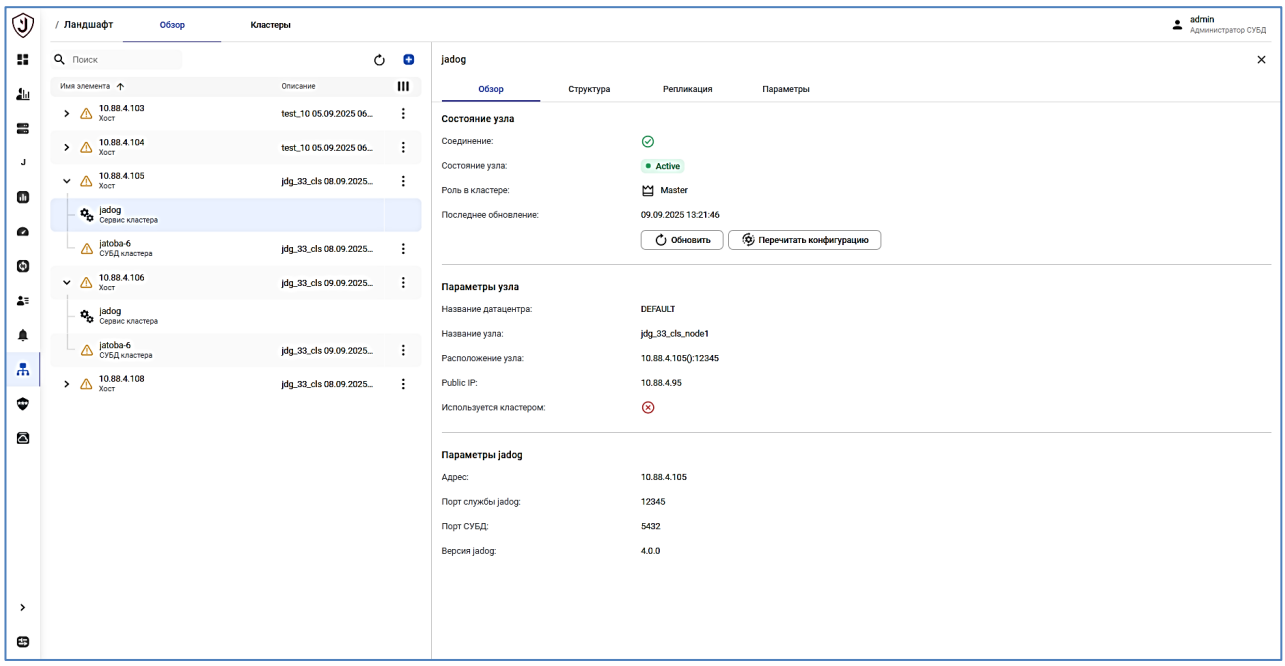


Рисунок 3.11 – Вкладка «Обзор» параметров кластера

Подключение к кластеру доступно через REST API.

3.4. Секционирование больших таблиц. ja_Hipe_Cluster

Компонент «ja_Hipe_Cluster» реализует функциональную возможность, позволяющую обычным серверам баз данных (называемым узлами) координировать свои действия друг с другом в архитектуре «ничего общего» («shared nothing»). Узлы образуют кластер, который позволяет СУБД хранить больше данных и использовать больше ядер центрального процессора, чем это было бы возможно на одном компьютере. Эта архитектура также позволяет масштабировать базу данных, просто добавляя дополнительные узлы в кластер. Данное расширение позволяет выполнять распределение таблиц и запросов по рабочим узлам, входящим в кластер.

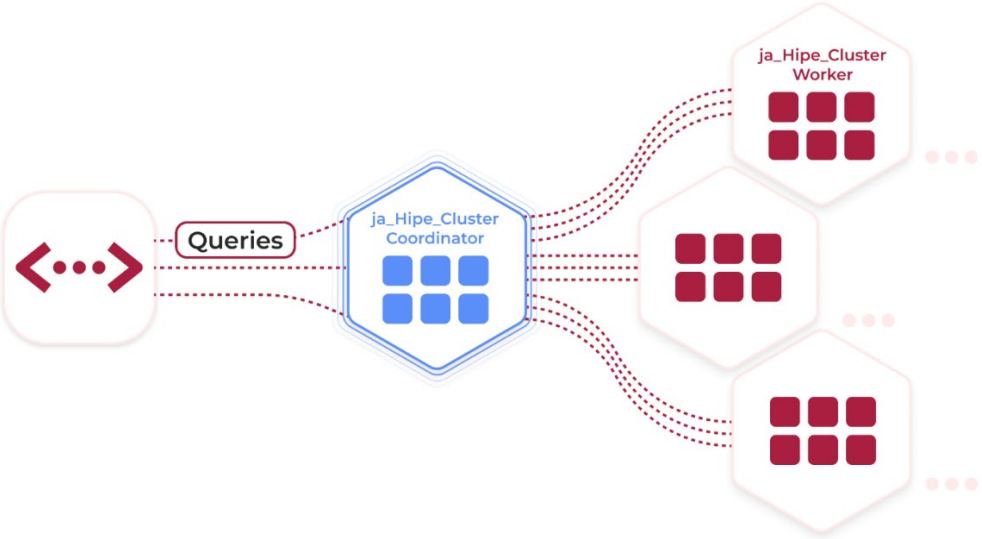


Рисунок 3.12 – Отправка запросов на рабочие узлы

3.5. Мониторинг и управление СУБД

Компонент пользовательского веб-интерфейса для администраторов «Jatoba data safe» предназначен для администраторов СУБД и БД, специалистов по безопасности и аудиторов безопасности.

Обладает следующими функциональными возможностями:

— управление и конфигурирование хоста СУБД и самой СУБД;

— просмотр событий безопасности;

— управление кластером СУБД;

— формирование матрицы привилегий пользователей;

— формирование матрицы системных привилегий пользователей;

— формирование отчетов о СУБД;

— синхронизация учетных записей пользователей;

— управление резервными копиями.

Безопасность внутри компонента обеспечивается реализованной двухкомпонентной ролевой моделью доступа, в которой пользователь компонента не знает и не может использовать учетную запись в СУБД.

3.5.1. Раздел «Мониторинг»

В комплект поставки СУБД «Jatoba» с версией ядра «5» и выше в компонент JDS включен раздел «Мониторинг».

Раздел «Мониторинг» предназначен для отображения оперативной информации в форме графических и цифровых панелей (виджетов) о целевой СУБД и ОС, на которой она установлена.

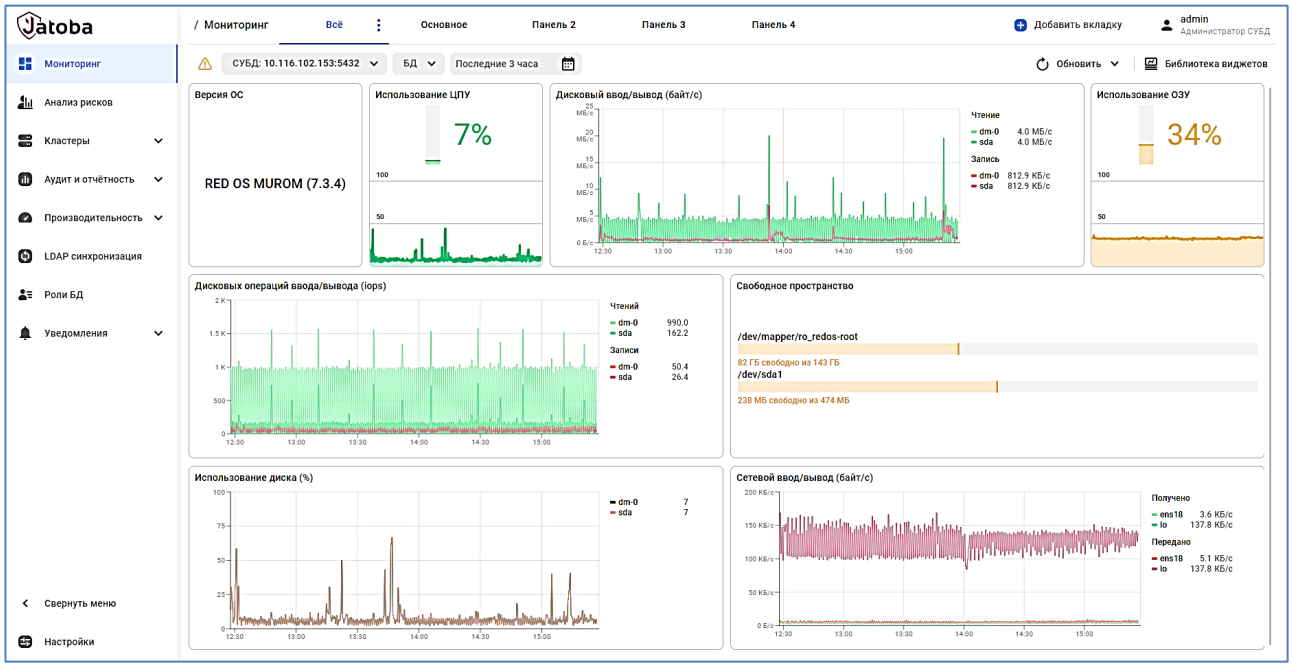


Рисунок 3.13 – Предустановленные виджеты

Виджеты имеют функциональную возможность контроль над пороговыми значениями и рассылку уведомлений

3.5.2. Раздел «Анализ рисков» (User Risk)

Разработанная функциональность раздела не имеет аналогов на рынке информационных технологий.

Раздел в графическом формате отображает системные привилегии ролей, предоставленные относительно объектов доступа.

Рисунок 3.14 – Вид раздела «Анализ рисков» (User Risk)

3.5.3. Аудит и отчетность

3.5.3.1. Раздел «Матрица доступа» (Access matrix)

Раздел также уникален и не имеет аналогов. В нем отображаются атрибутов пользователей относительно субъектов доступа.

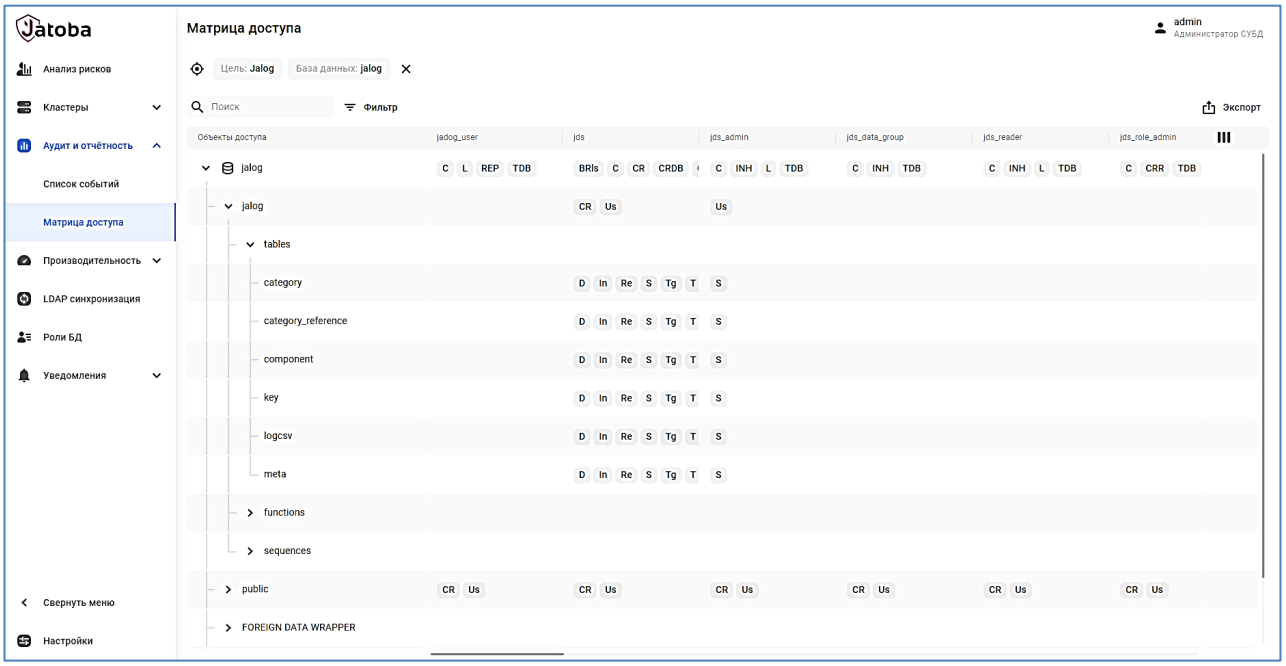


Рисунок 3.15 – Вид раздела «Матрица доступа» (Access matrix)

Полученные результаты возможно экспортировать в файл MS Excel.

3.5.3.2. Раздел «Список событий» (Event List)

Раздел «Список событий» (Event List) предназначен для просмотра событий безопасности в выбранной инсталляции (Target).

Для функционирования раздела требуется, чтобы на целевой СУБД был установлен компонент «ja_Log», обеспечивающий передачу событий безопасности в служебную СУБД. Компонент «pgAudit» при этом обеспечивает расширенную регистрацию событий безопасности.

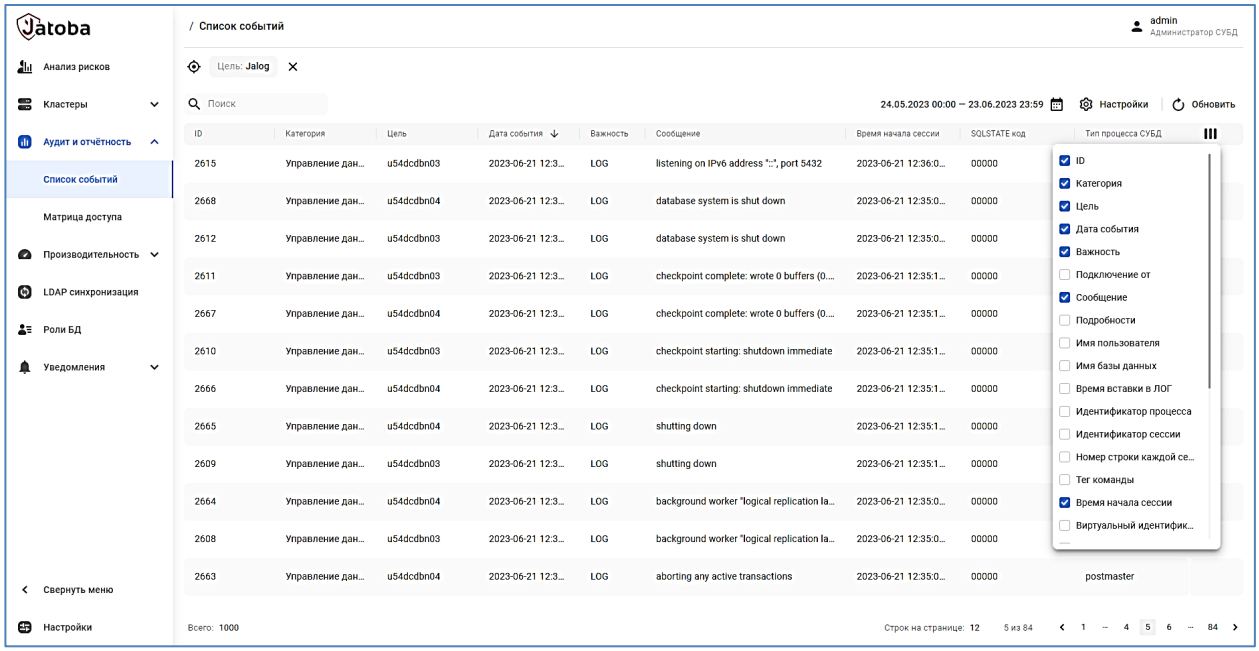


Рисунок 3.16 – Вид раздела «Список событий» (Event List)

Раздел JDS «Event List» оснащен:

- полем контекстного поиска;
- набором фильтров;
- механизмом выбора отображаемых полей;
- механизмом автоматического обновления.

Время хранения журналов событий СУБД ограничено только выделенным дисковым пространством для служебной БД «ja_log».

3.5.4. Раздел «Кластеры»

Функциональные возможности раздела описаны в п. 3.3.3 настоящего документа.

3.5.5. Производительность

3.5.5.1. Раздел «Снимки и отчеты» (Snapshots & Reports)

Подраздел «Снимки и отчеты» (Snapshots & Reports) предназначен для создания снимков состояния БД (Snapshots) и получения отчетов. Формирование статической информации выполняется компонентом «pg_Profile».

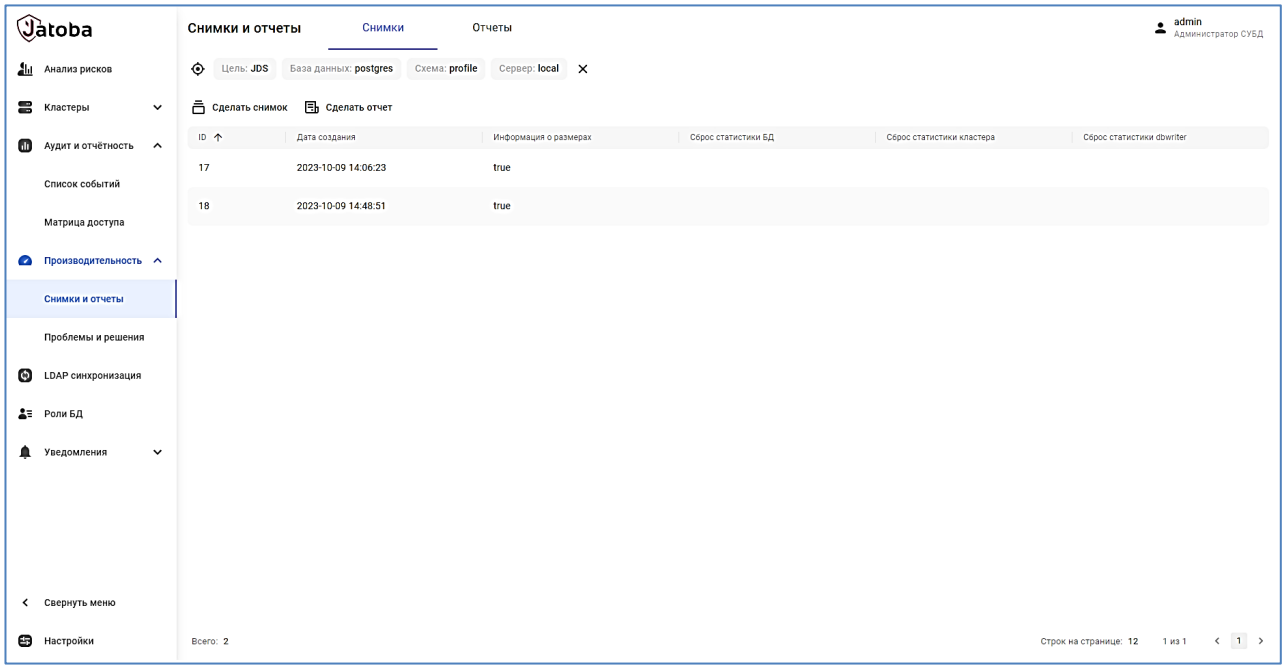


Рисунок 3.17 – Вкладка «Снимки»

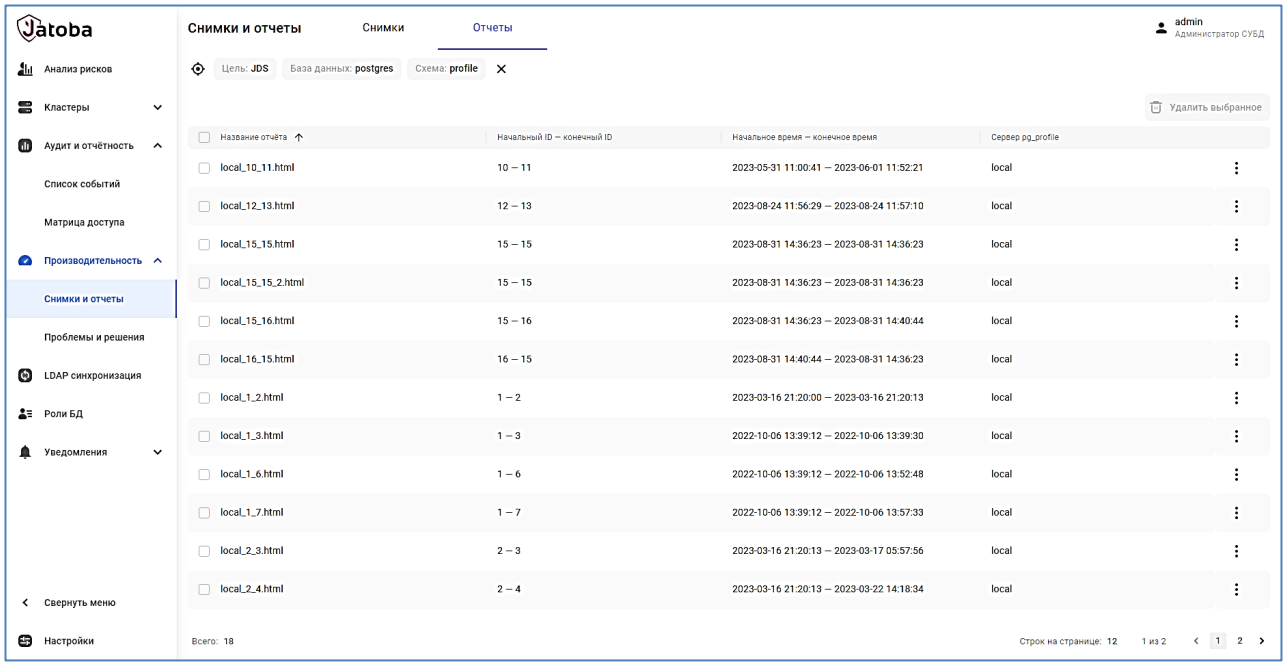


Рисунок 3.18 – Вкладка «Отчеты»

3.5.5.2. Раздел «Проблемы и решения» (Problems & Solutions)

Подраздел «Проблемы и решения» (Problems & Solutions) представляет собой интеллектуальный инструмент, который позволяет определять ряд проблем, существующих в целевой СУБД и разрешать их.

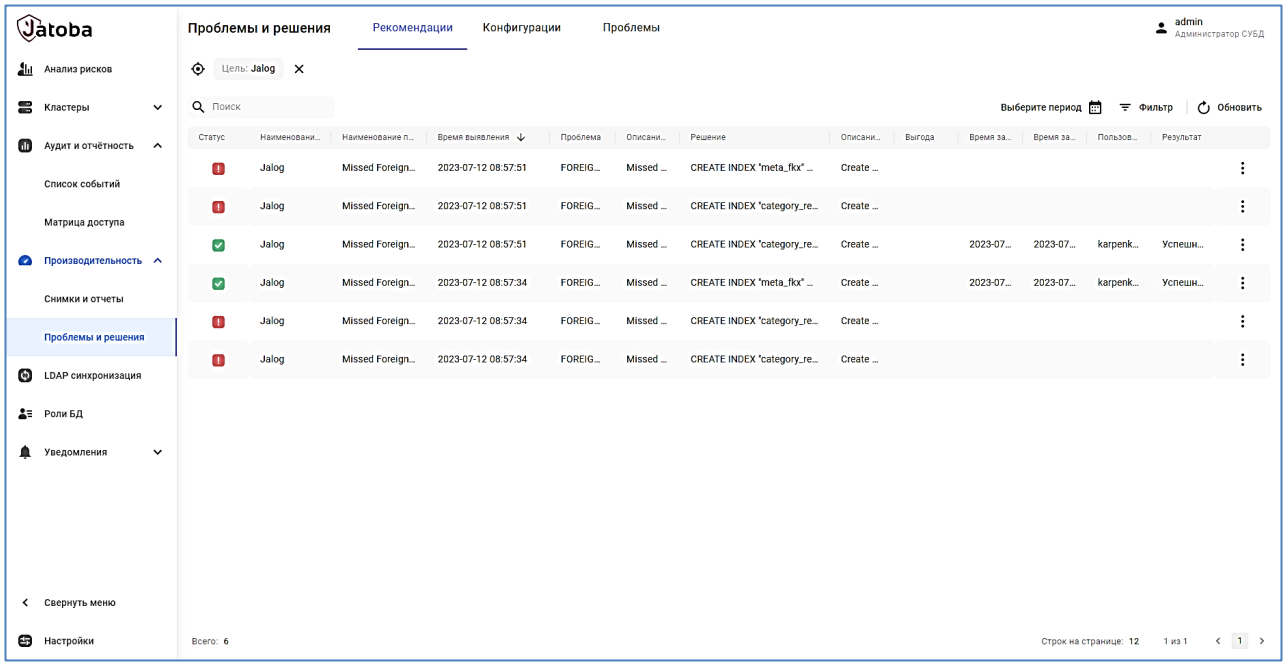


Рисунок 3.19 – Вкладка рекомендации

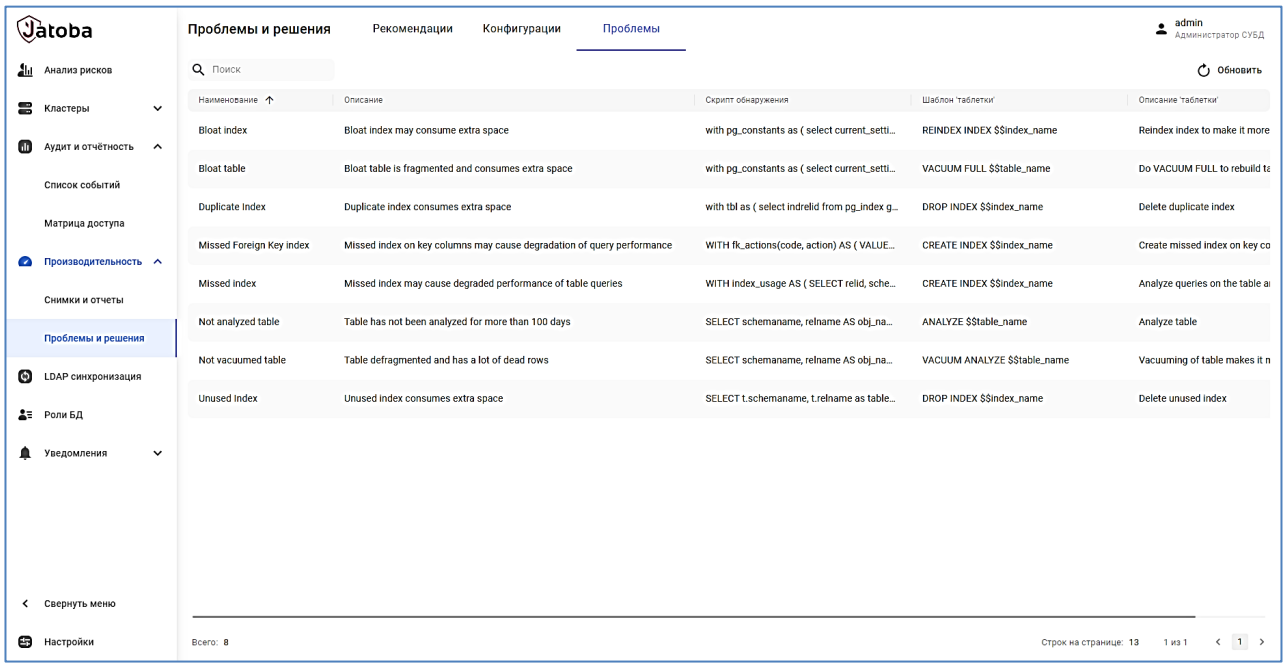


Рисунок 3.20 – Вкладка проблемы

3.5.5.3. Раздел «Анализ запросов» (Query analysis)

Подраздел «Анализ запросов» предоставляет пользователю с ролью «Администратор СУБД»:

— отображение визуализации плана запроса средствами Pg-explain;

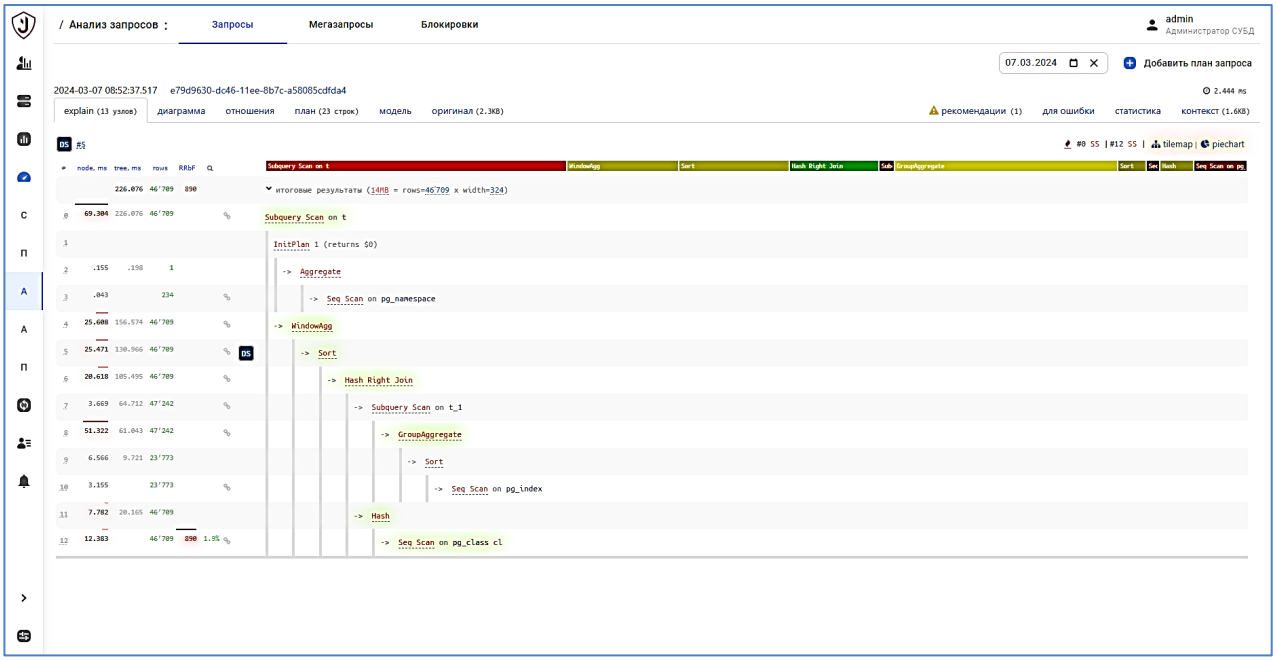


Рисунок 3.21 – Визуализация explain по узлам

— отображение списка планов запросов по нескольким критериям отбора и переход по ссылке из выбранного плана запроса на страницу анализа плана запроса;

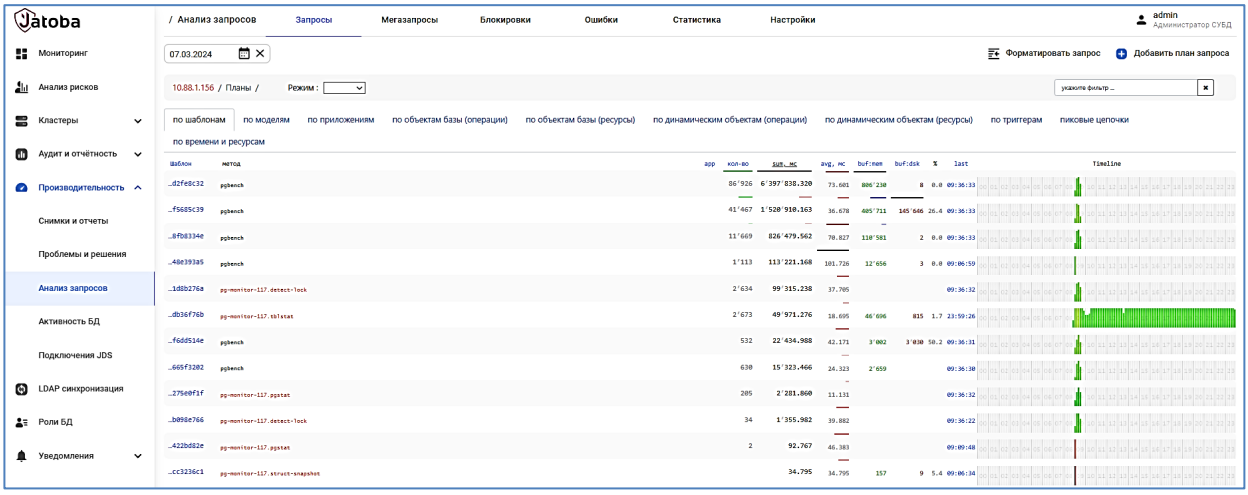


Рисунок 3.22 – Вкладка «по шаблонам»

— возможность ручного ввод плана запроса.

3.5.5.4. Раздел «Активность БД»

Подраздел «Активность БД» (DB Activity) предназначен для:

— мониторинга активности в СУБД;

— получения информации о выполняющихся сессиях/процессах, существующих блокировках;

— завершения сессий;

— выявления подозрительной активности пользователей.

Может использоваться в случаях, когда пользователь(и) СУБД сообщает(ют), что:

— операция «зависла»;

— СУБД потеряла производительность;

— типичные операции, выполняются дольше обычного;

— зависла сессия, не позволяющая подсоединиться повторно и требуется ее снять

— требуется разобраться по каким причинам «зависла» его операция.

При выборе цели компонент JDS автоматически отобразит текущие сессии.

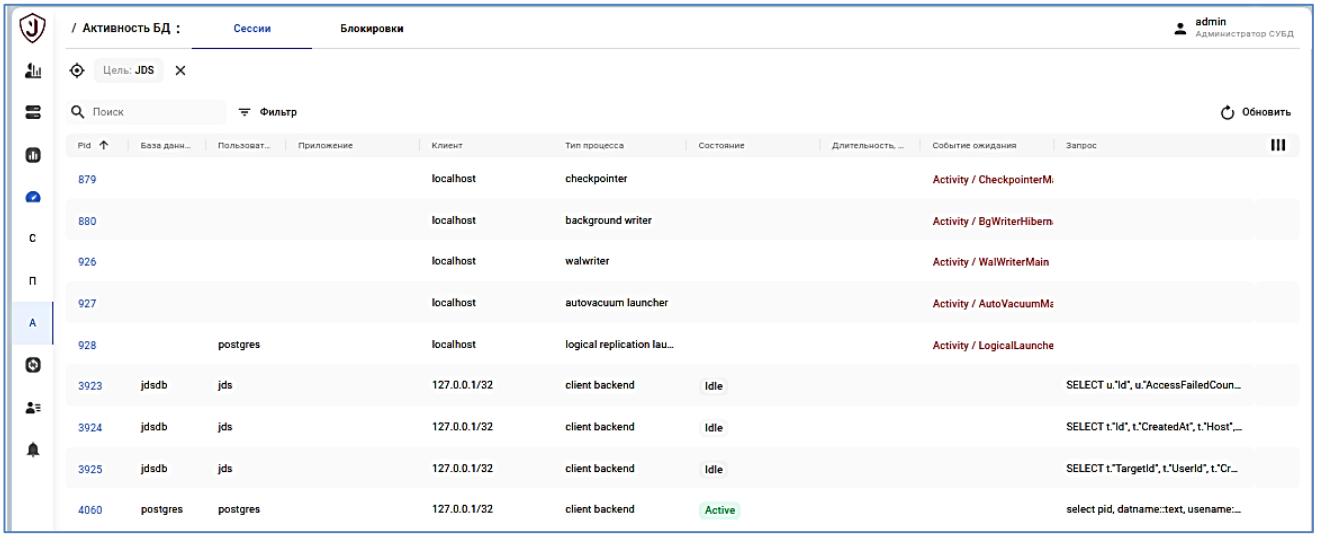


Рисунок 3.23 – Отображение текущих сессий

Во вложенном окне «Запрос» отражается выполняемый запрос, который возможно скопировать в буфер обмена, либо завершить.

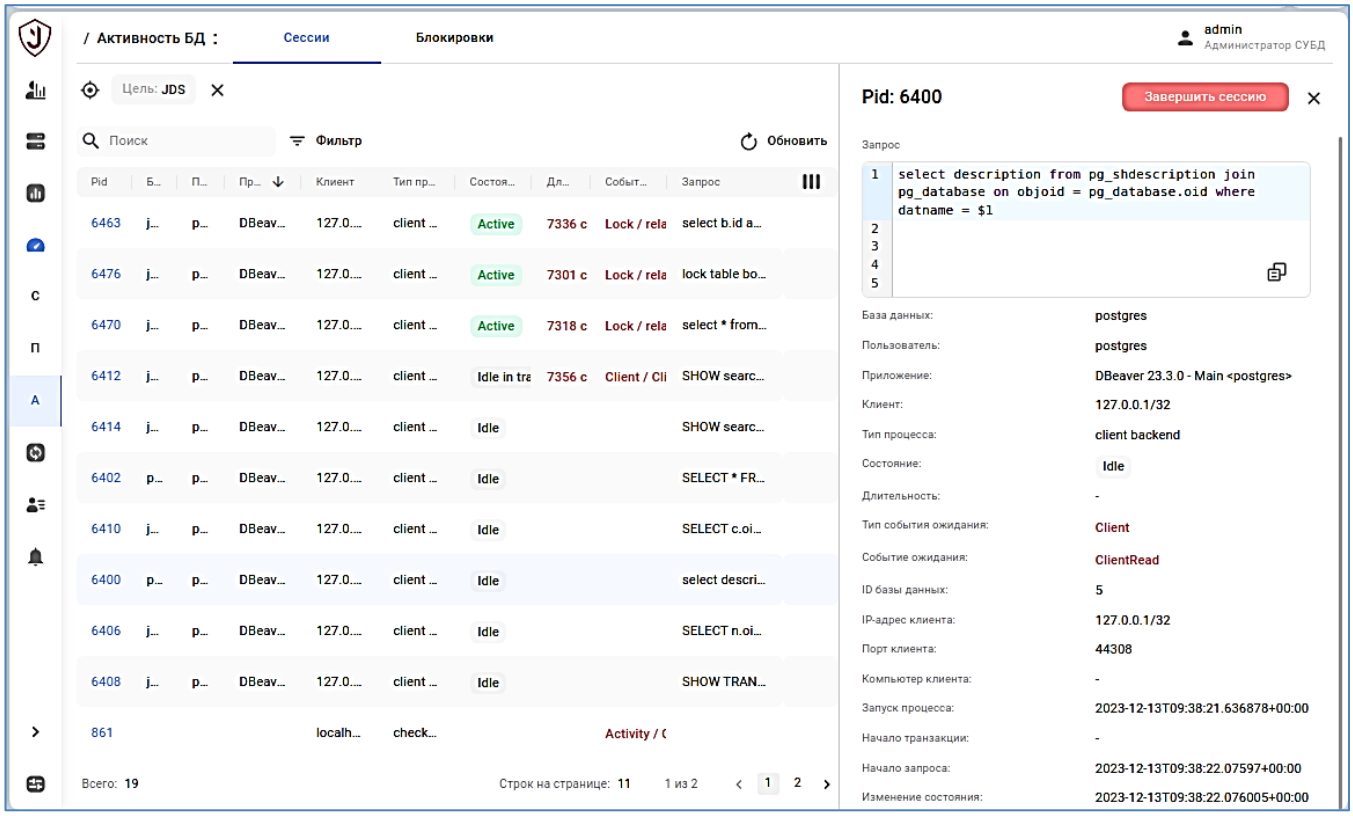


Рисунок 3.24 – Дополнительное окно «Завершение сессии» в вкладке «Сессии»

3.5.5.4.1. Вкладка «Подключения»

Вкладка «Подключения» отображает количество подключений к выбранной СУБД.

После выбора цели отображаются столбцы:

— Пользователь/роль;

— Количество подключений;

— Квота подключений.

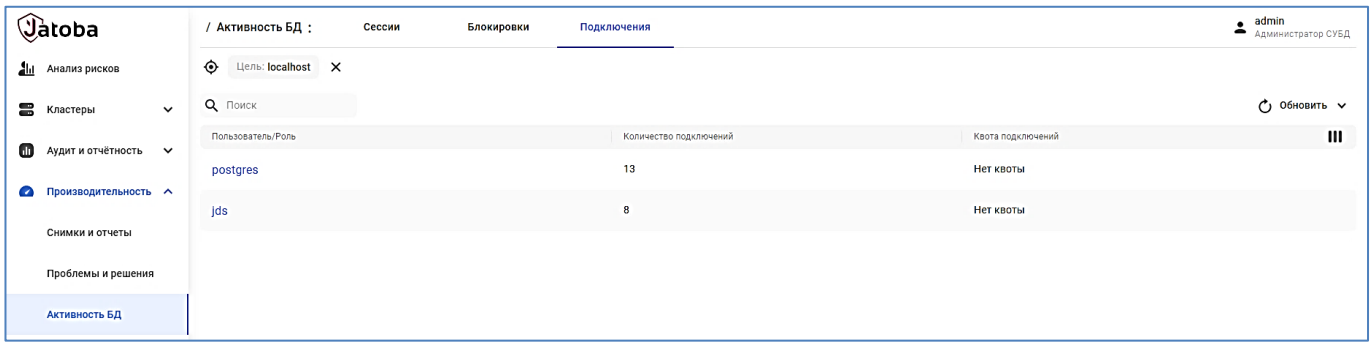


Рисунок 3.25 – Вкладка «Подключения»

3.5.5.4.2. Подраздел «Подключения JDS»

Вкладка «Подключения JDS» отображает количество подключений к компоненту пользовательского веб-интерфейса для администраторов «Jatoba data safe»

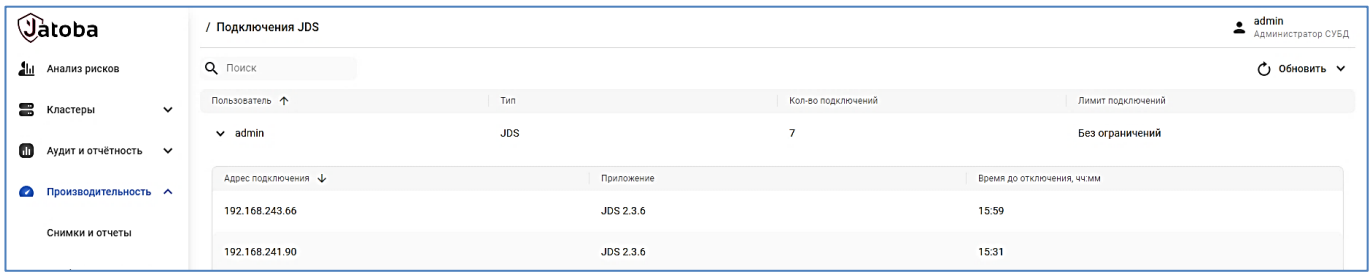


Рисунок 3.26 – Отображение дополнительной информации о подключении пользователя JDS

После выбора цели отображаются столбцы:

- Пользователь;
- Тип:
  - JDS (подключение к компоненту);
  - БД (подключение к служебной БД компонента);
- Количество подключений;
- Лимит подключений.

3.5.6. Раздел «LDAP синхронизация»

В разделе «LDAP синхронизация» используется уникальный компонент собственной разработки «ja_Sync_LDAP».

Раздел «LDAP синхронизация» автоматизирует и визуализирует работу компонента «ja_Sync_LDAP» используемого для синхронизации учетных записей служб каталогов и СУБД, таких как:

— Active Directory;

— ALD Pro;

— FreeIPA;

— SAMBA.

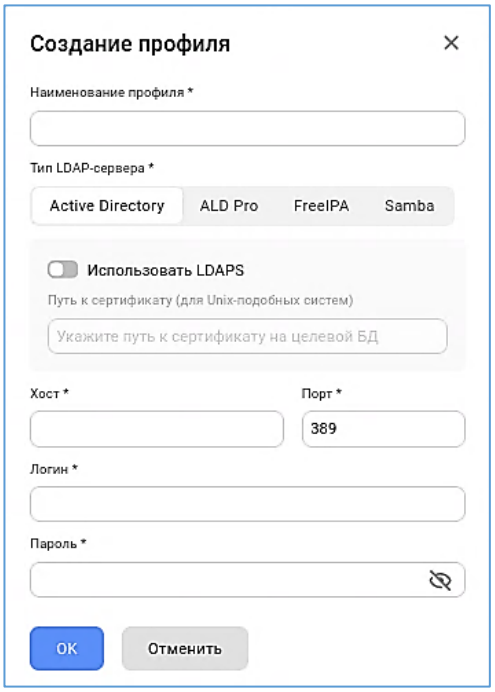


Рисунок 3.27 – Окно создания профиля синхронизации в версии JDS 2.2

Во избежание ошибок аутентификации в компоненте применяется механизм преобразования имен пользователей.

Примеры использования механизма приведены в таблице 3.2.

Таблица 3.2 – Примеры преобразования имен

Значение параметра	Наименование УЗ в LDAP	Наименование УЗ в СУБД	Комментарий
none (по умолчанию)	j.USER01@cntr.gazPROM.Loc	j.USER01@cntr.gazPROM.Loc	ни каких преобразований не производится.

Значение параметра	Наименование УЗ в LDAP	Наименование УЗ в СУБД	Комментарий
			УЗ в LDAP и СУБД идентичны.
lower	j.USER01@cntr.gazPROM.Loc	j.user01@cntr.gazprom.loc	все символы переводятся в нижний регистр

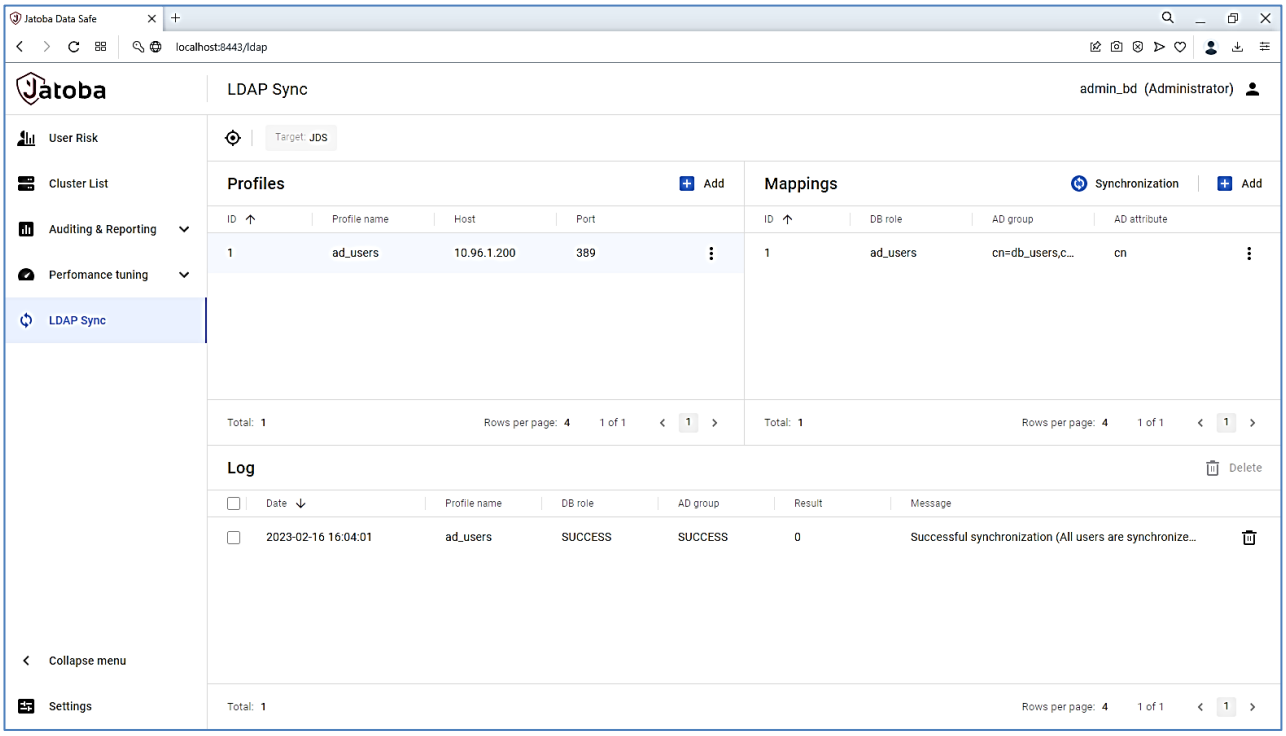


Рисунок 3.28 – Раздел «LDAP Sync»

3.5.7. Раздел «Роли БД» (DB roles)

Раздел «Роли БД» позволяет:

— просматривать список пользователей СУБД;

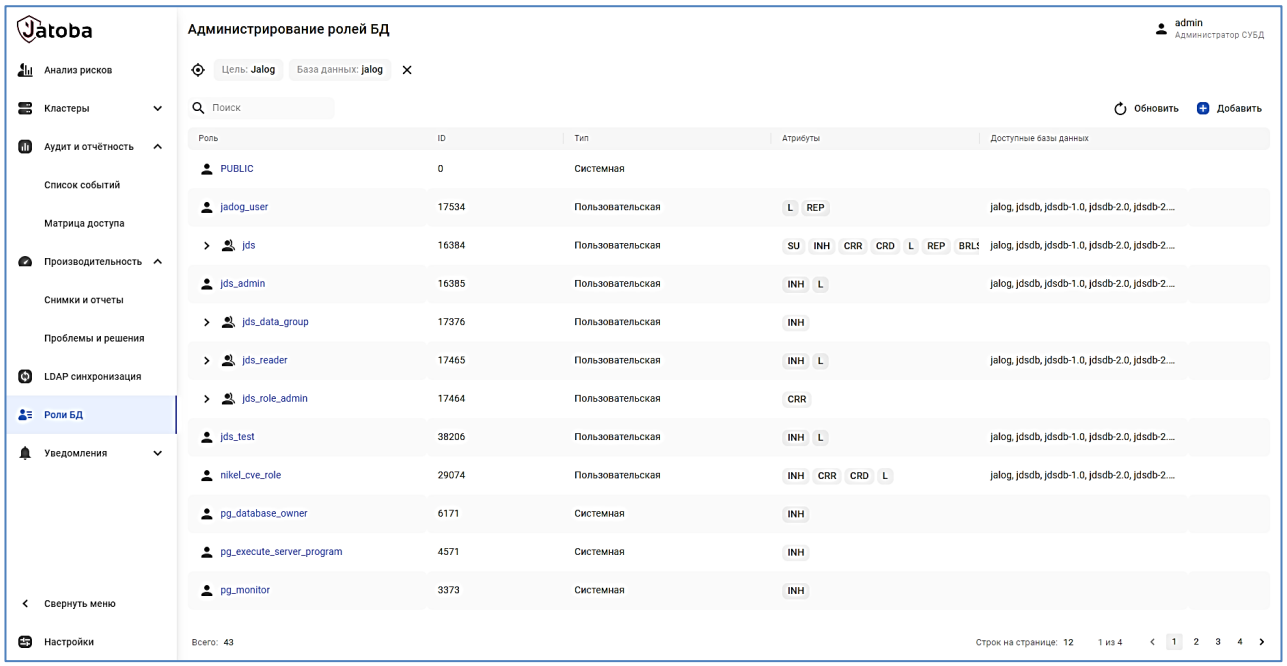


Рисунок 3.29 – Вкладка «Роли БД»

— создавать и удалять роли;

— редактировать роли;

— назначать атрибуты роли;

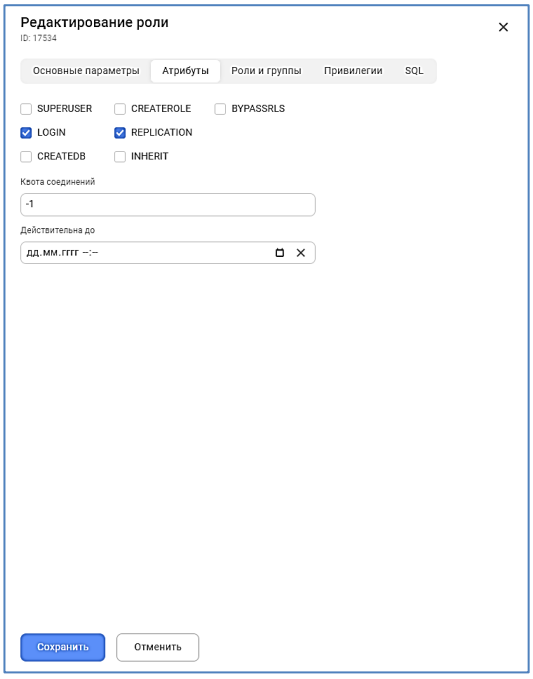


Рисунок 3.30 – Вкладка «Атрибуты»

— включать и исключать роль в групповые роли;

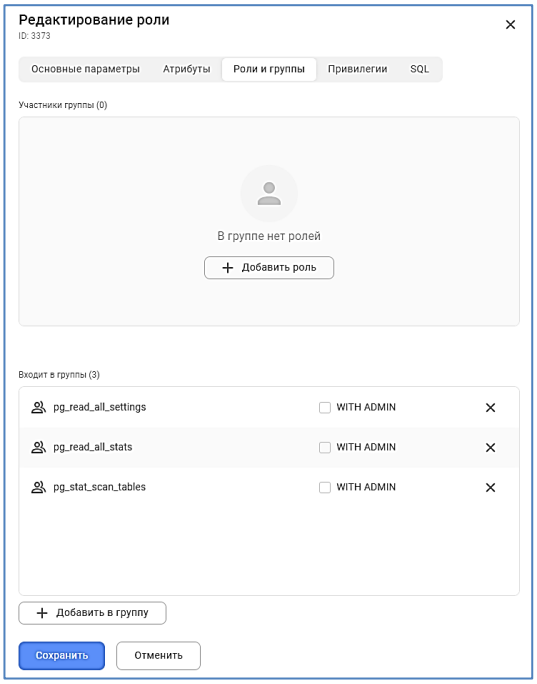


Рисунок 3.31 – Вкладка «Роли и группы»

— назначать привилегии роли;

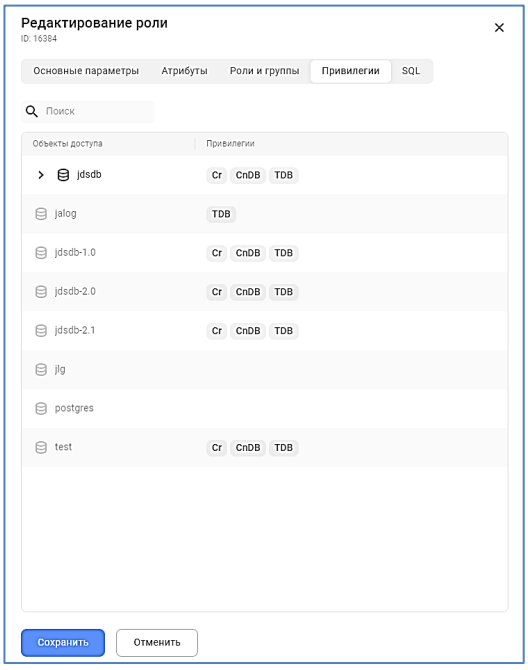


Рисунок 3.32 – Вкладка «Привилегии»

В совокупности с функциональными возможностями раздела «Уведомления» становится возможным установить контроль над действиями, связанными с учетными записями пользователей в СУБД.

3.5.8. Раздел «Уведомления» (Notifications)

Раздел «Уведомления» предназначен для оповещения администраторов о событиях целевой СУБД и компонента JDS.

Механизм уведомлений содержит в себе три типа поиска сообщений:

— ошибки БД;

Поиск выполняется по классу события или по коду события.

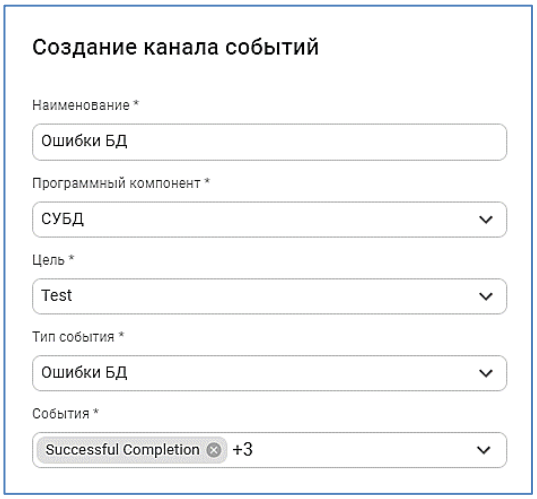


Рисунок 3.33 – Поле «Тип события»

— события учетных записей;

Поиск выполняется по ключевым фразам.

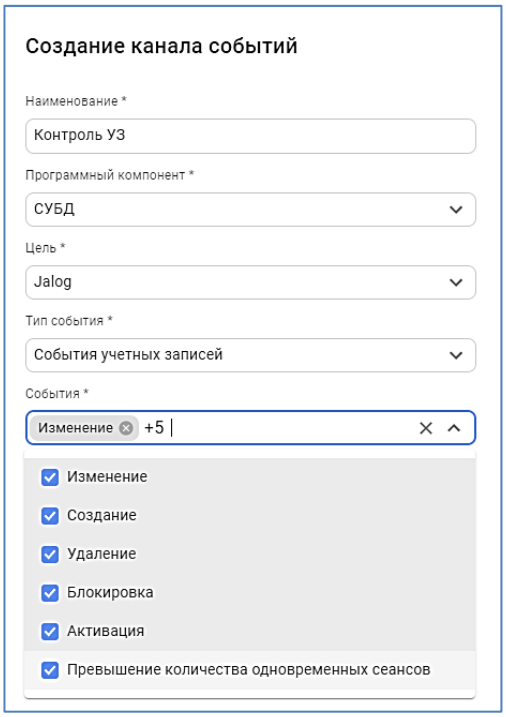


Рисунок 3.34 – Поле «События» при выбранном типе события «События учетных записей»

— произвольный текст;

Поиск выполняется, по ключевым словам, задаваемым пользователем JDS.

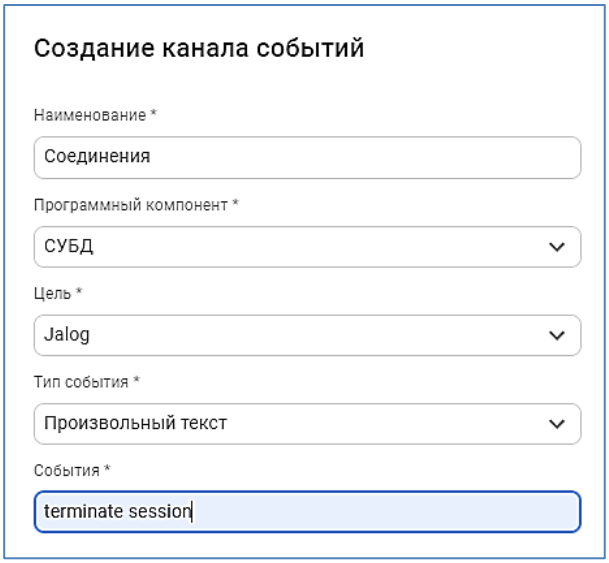


Рисунок 3.35 – Тип события «Произвольный текст»

Таким образом реализована функциональная возможность контроля и оповещения ответственных сотрудников о любых событиях СУБД средствами:

— электронной почты (SMTP);

— мессенджера Zulip.

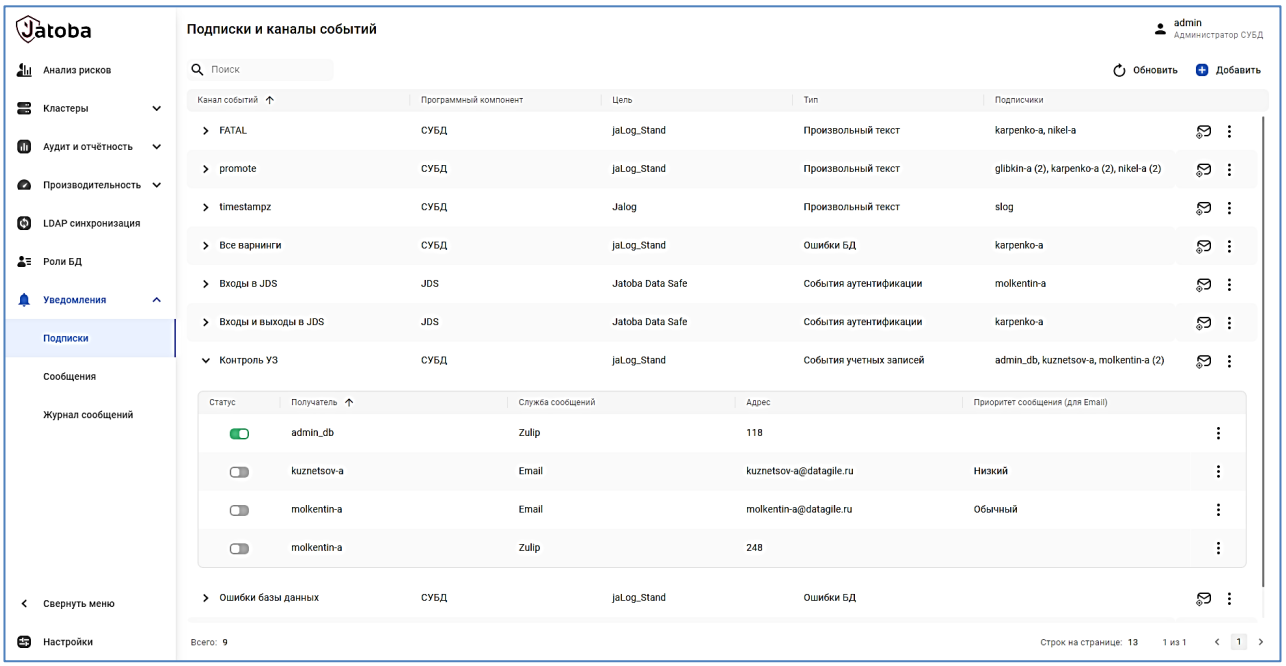


Рисунок 3.36 – Список каналов событий

Совокупностью реализованных механизмов выполняются функциональные возможности по оперативному контролю и мониторингу событий СУБД.

3.5.9. Раздел «Ландшафт» (Landscape)

Раздел «Ландшафт» предназначен для:

— получения общей информации о хосте СУБД;

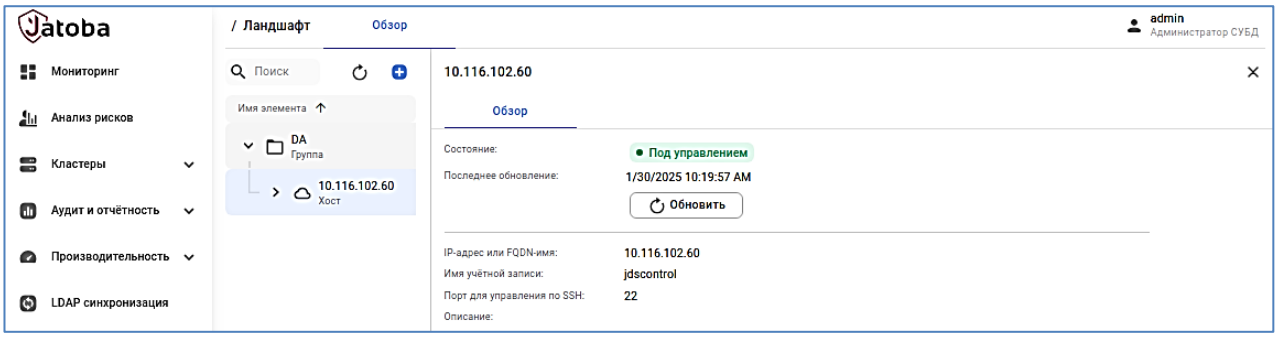


Рисунок 3.37 - Хост. Вкладка «Обзор»

— получения общей информации о СУБД;

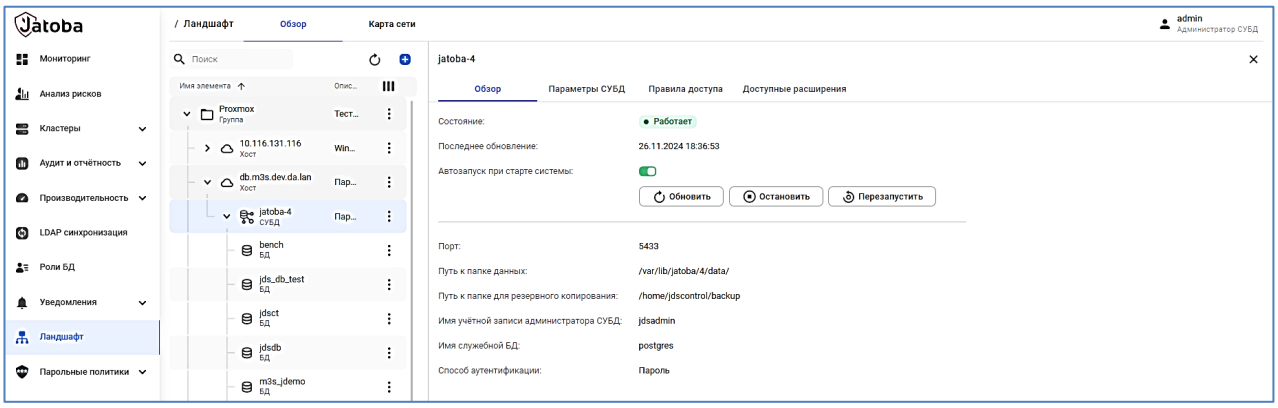


Рисунок 3.38 – Вкладка «Обзор»

— управления конфигурационными файлами СУБД;

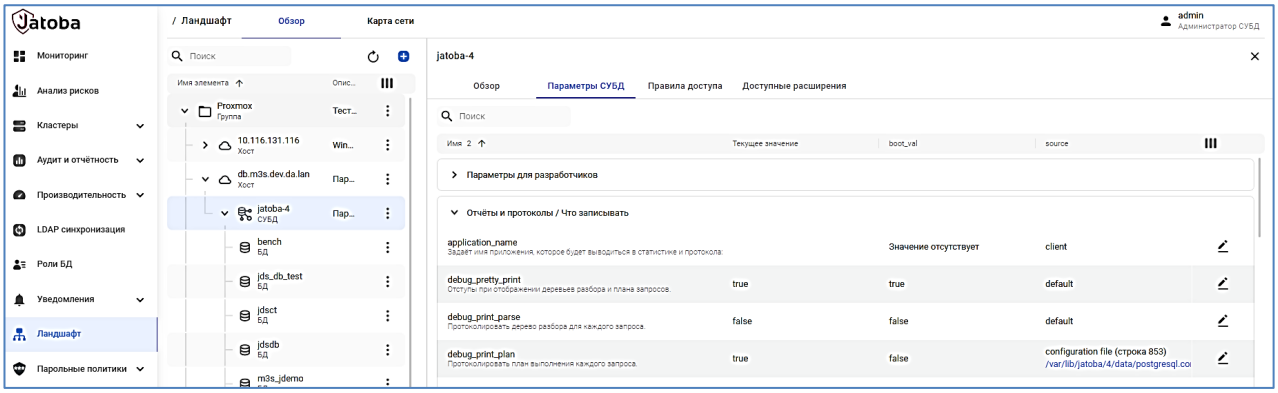


Рисунок 3.39 - Вкладка «Параметры СУБД»

— установки и управления расширениями СУБД;

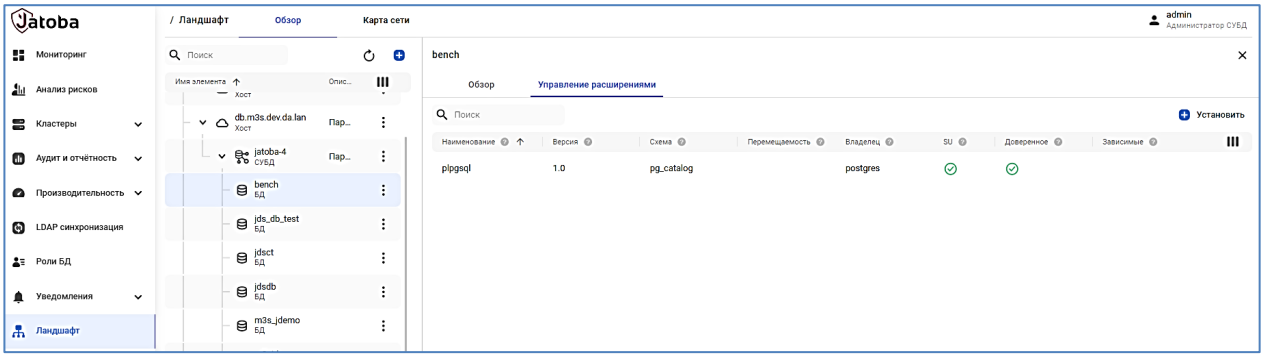


Рисунок 3.40 – Вкладка «Управление расширениями»

— управлением кластером (п. 3.3.3).

3.5.10. Раздел «Парольные политики» (Password policies)

В комплект поставки СУБД «Jatoba» с версией ядра «5» и выше в компонент JDS включен раздел «Парольные политики».

Раздел «Парольные политики» предназначен для автоматизации и упрощения работы с парольными политиками и блокировками пользователей целевой СУБД.

Раздел включает в себя подразделы:

— Управление политиками (Policy management);

— Привязка ролей (Role Binding);

— Работа с блокировками.

Корректная работа раздела обеспечивается установленными и настроенными на целевой СУБД компонент:

SecurityProfile, описанного в документе «Руководство администратора»;

ja_CSum, описанного в документе «Руководство по настройке. Часть 14. Контроль целостности. Компонент «ja_CSum».

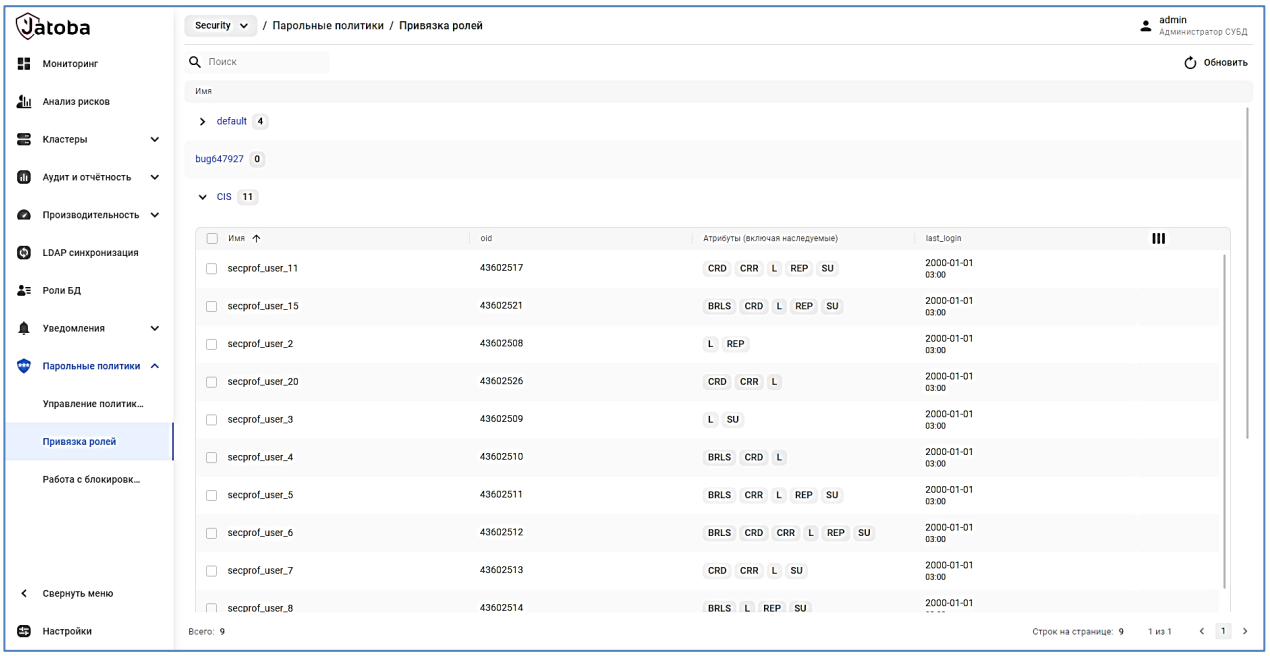


Рисунок 3.41 – Список пользователей привязанных к парольной политике

3.5.11. Раздел «Резервное копирование» (BACKUP)

Раздел предназначен для:

— настройки и управления компонентом «probackup»;

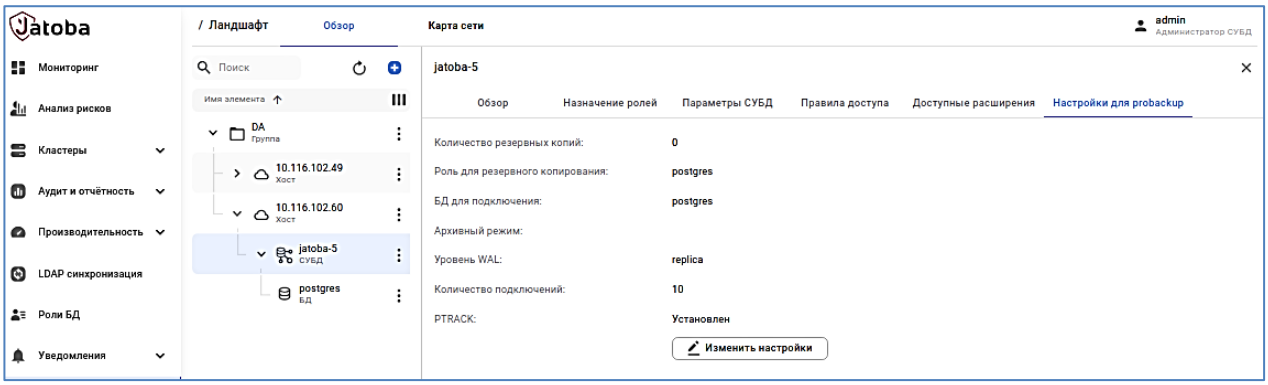


Рисунок 3.42 - Вкладка «Настройки для probackup»

— управления хранилищем резервных копий;

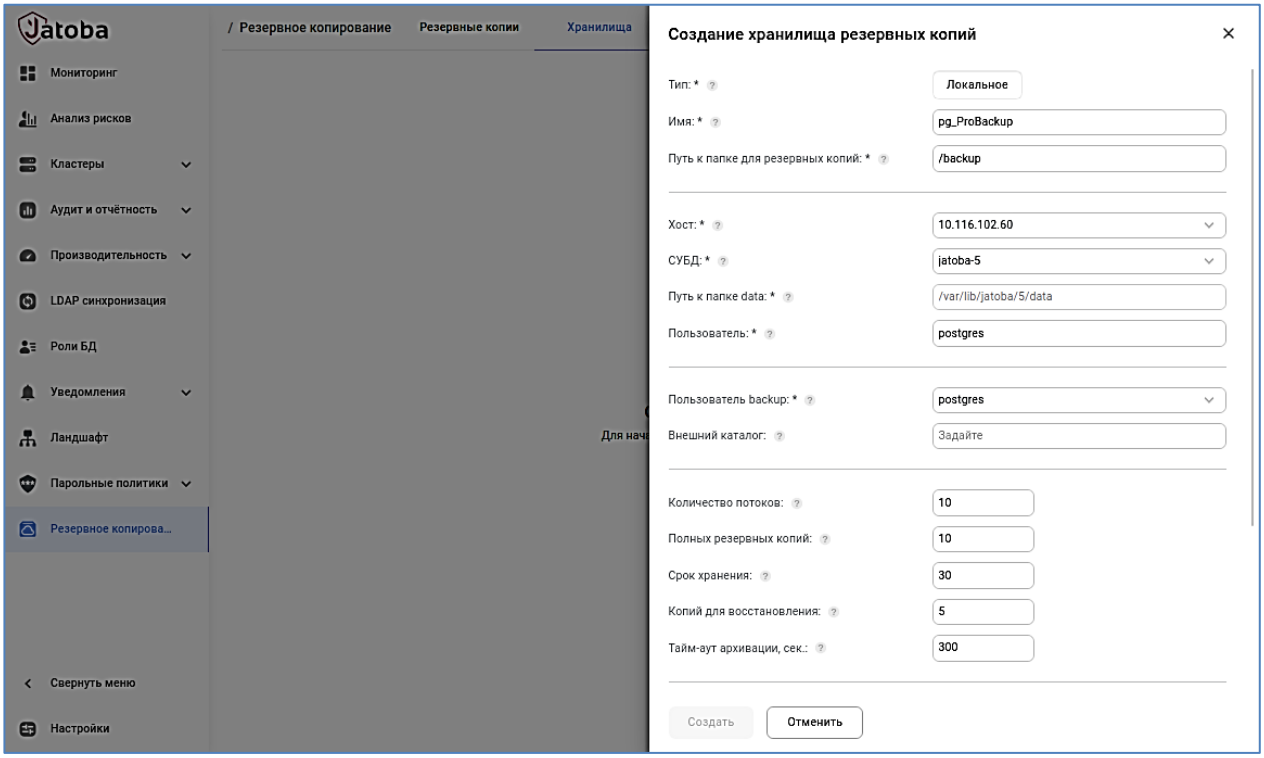


Рисунок 3.43 – Создание хранилища резервных копий

— создания резервных копий.

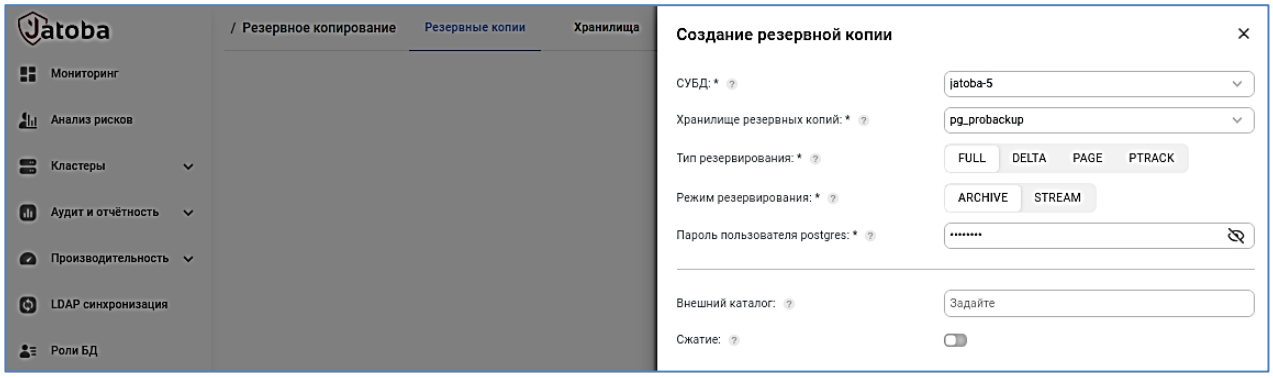


Рисунок 3.44 – Создание резервной копии

3.6. Резервное копирование

3.6.1. Компонент «pg_ProBackup»

Отказоустойчивость СУБД «Jatoba» реализуется применением полного или инкрементального резервного копирования, выполняемого компонентом «pg_ProBackup».

Полные резервные копии содержат все файлы данных, необходимые для восстановления сервера баз данных с нулевой точки.

Инкрементальные копии создаются на уровне страниц данных и включают только ту информацию, которая изменилась со времени последнего резервного копирования.

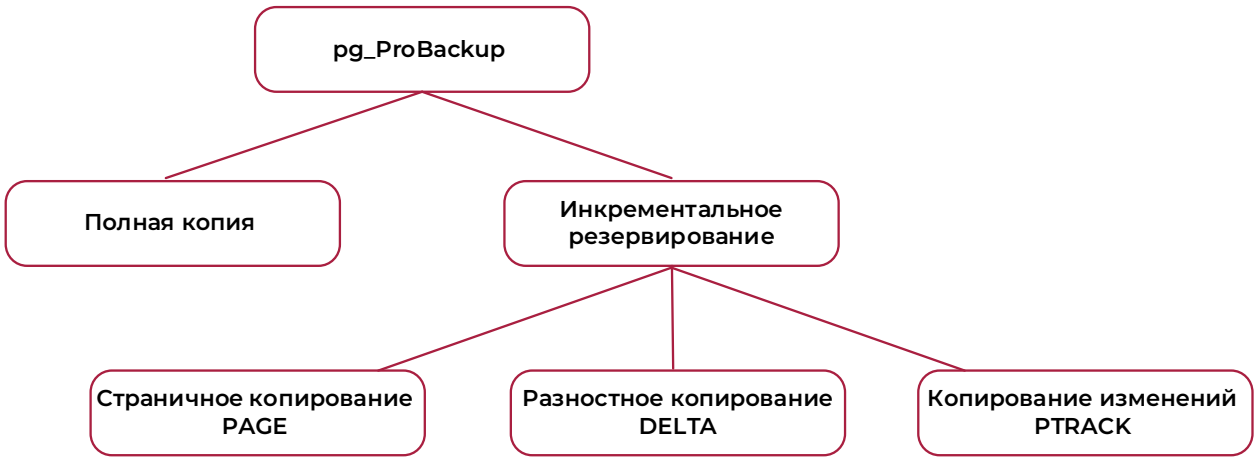


Рисунок 3.45 – Реализуемые способы резервного копирования

Поддерживается полное и инкрементальное резервное копирование, и восстановление в облачном хранилище S3.

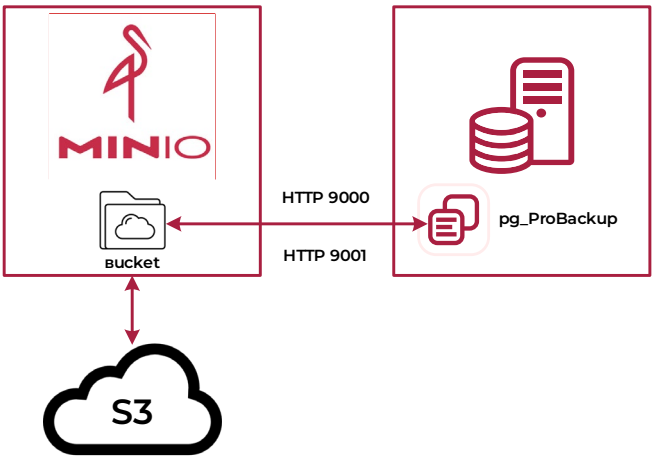


Рисунок 3.46 – Схема работы компонента pg_ProBackup с хранилищем MinIO

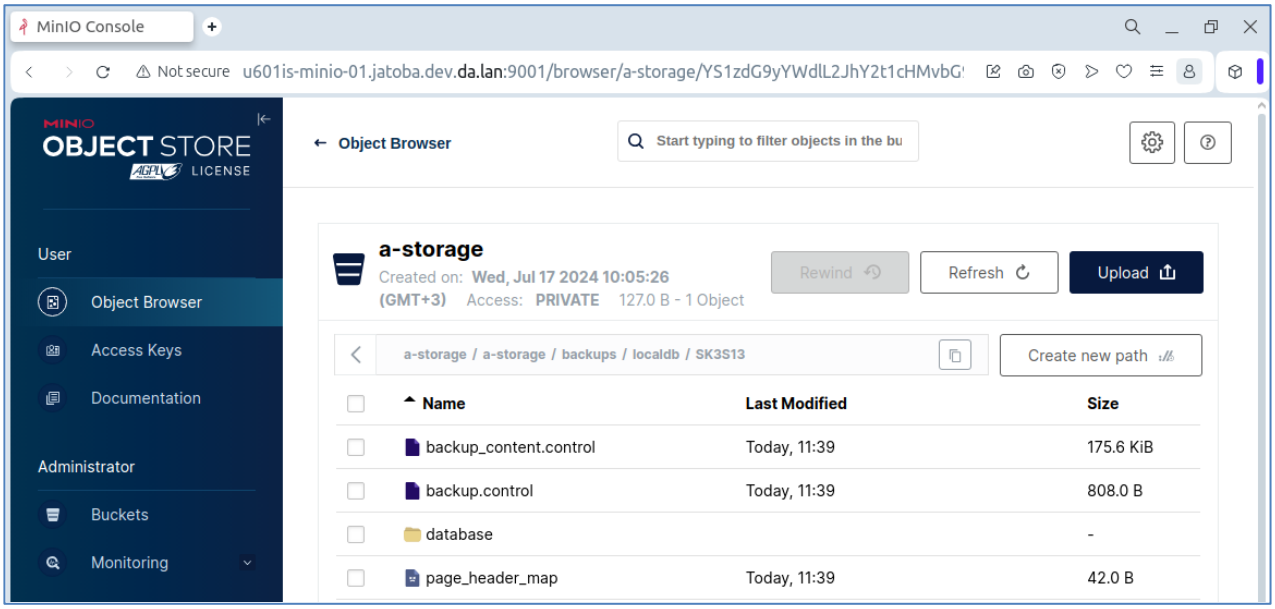


Рисунок 3.47 - Созданная резервная копия в хранилище S3

3.6.2. Компонент «ja_Backup»

Компонент «ja_backup» — представляет собой расширение функционала СУБД «Jatoba» и предназначен для управления резервным копированием и восстановлением баз данных СУБД «Jatoba», для регулярного создания резервных копий, позволяющих восстанавливать работу СУБД в случае аварийной ситуации, порчи или потери данных.

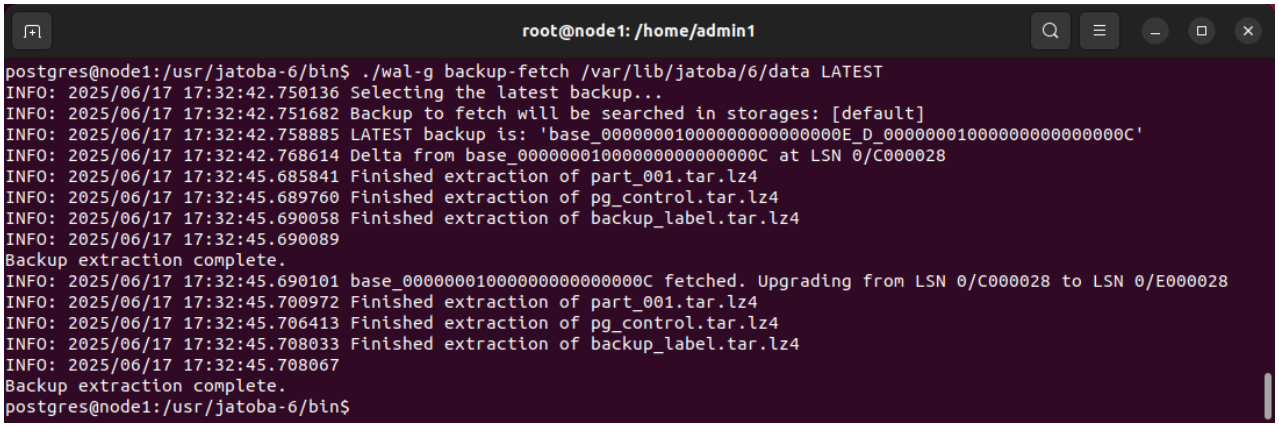


Рисунок 3.48 – Запуск и успешное восстановление СУБД из РК

3.7. Маскирование данных. Компонент «ja_Anonymizer»

Компонент «ja_Anonymizer» — представляет собой расширение СУДБ «Jatoba», которое предоставляет механизм маскировки и анонимизирования данных.

Обладает функциональными возможностями

— **Статическое маскирование** (Static Masking): безвозвратно замаскировать все персональные данные, хранящиеся в БД, заменив их другими значениями, сохранив структуру для дальнейшего анализа;

— **Динамическое маскирование** (Dynamic Masking): включить «прозрачную» маскировку для определённых (MASKED) пользователей, чтобы они не имели возможности доступа к маскируемым реальным персональным данным;

— **Анонимные дампы** (Anonymous Dumps): экспортировать замаскированную версию данных в внешний SQL-файл. SQL-файл с замаскированными данными возможно использовать для тестов или передачи другим пользователям;

— **Маскирующие представления** (Masking Views): создание специальных представлений (views), в которых конфиденциальные поля уже замаскированы;

— **Маскирующие обертки данных** (Masking Data Wrappers): применение правил маскировки к данным, поступающим в БД из внешних источников.

Например

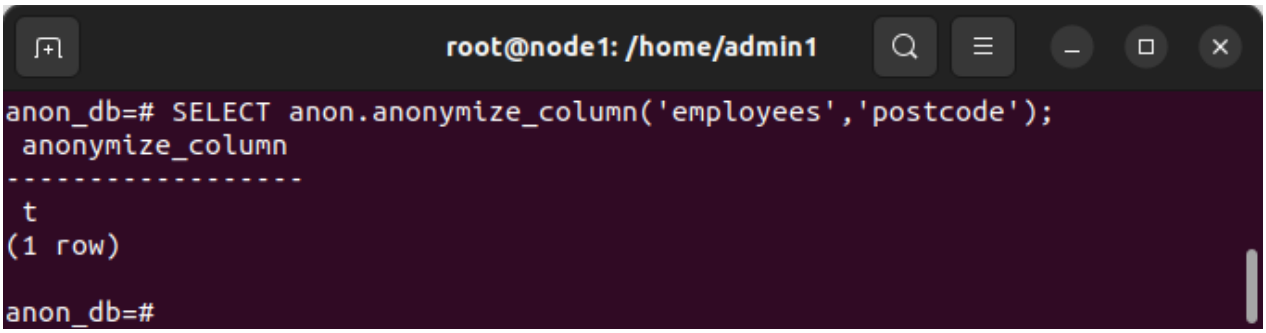


Рисунок 3.49 – Применение правила anon.anonymize_column статического маскирования исходных данных таблицы employees к столбцу postcode

```
root@node1: /home/admin1
anon_db=# SELECT * FROM employees;
 id  | firstname | lastname |     company     | postcode
-----+-----------+----------+-----------------+----------
 111 | Maria     | Belova   | Bank of Saratov | 4****7
 222 | Pavel     | Petrov   | Head and Hands  | 6****5
(2 rows)

anon_db=#
```

Рисунок 3.50 – Данные таблицы employees после использования статического маскирования к столбцу postcode

3.8. Поддержки платформы Oracle

В СУБД «Jatoba» реализован набор расширений, обеспечивающий интеграцию СУБД «Jatoba» с СУБД «Oracle». Расширения предоставляют дополнительные функции, повышающие синтаксическую совместимость и упрощающие перенос хранимых процедур, и предоставляют дополнительные методы прозрачного доступа к данными из одной СУБД в другую.

Компонент «OraFCE» выполнен в виде расширения и имеет дополнительные функции и операторы для работы текстовыми и временными строками. Может применяться для миграции данных из Oracle в СУБД «Jatoba».

Компонент «pg_Variables» выполнен в виде расширения и предназначен для работы с переменными различных типов. Созданные переменные существуют только в рамках текущей пользовательской сессии.

Компонент «Oracle_FDW» дает возможность создать обертку (Foreign-Data Wrapper, FDW) для доступа к базе данных Oracle.

3.9. Поддержка платформы MS SQL

Компонент «TDS_FDW» предназначен для импорта данных из БД MS SQL в СУБД «Jatoba», который помогает сопоставить типы данных.

Сопоставляемые типы данных приведены в таблице 3.3.

Таблица 3.3 – Сопоставляемые типы данных

MS SQL	СУБД «Jatoba»
bingint	bingint
integer	integer
smallint	Smallint
Real	Real

MS SQL	СУБД «Jatoba»
Numeric(18,0)	Numeric(18,0)
Binary(10)	Bytea
Bit	Smallint
Char(8)	Character(8)
nchar(8)	Character(8)
Float	Double precision
Decimal(18,0)	Numeric(18,0)
Ntext	Text
Text	Text
Nvarchar(8)	Character varying(8)
Date	Date
Datetime	Timestamp without time zone
Time	Time without time zone
Timestamp	Bytea
Money	Money
Tinyint	Smallint
Smallmoney	money

3.10. Совместимость платформой с 1С

Совместимость с платформой 1С и СУБД «Jatoba» подтверждена сертификатом.

3.10.1. Компонент совместимости 1С fasttrun

Платформа 1С для выполнения своих обработок очень часто пользуется временными таблицами. Компонент fasttrun предоставляет транзакционно-небезопасную (изменения нельзя откатить) функцию, предназначенную для быстрого удаления содержимого заданной временной таблицы (по имени) и своевременного обновления статистики этой таблицы после удаления ее содержимого. Это предотвращает разрастание системного каталога pg_class, положительно сказывается на производительности системы при работе с большим количеством временных таблиц, создаваемых 1С в СУБД. Установку и вызов функций данного расширения Платформа 1С производит самостоятельно. Администратору надо только обеспечить установку данного расширения в составе СУБД.

3.10.2. Компонент совместимости 1С fulleq

Платформа 1С может использоваться на большом количестве разных СУБД. В разных СУБД имеются разные трактовки отдельных параграфов стандарта языка SQL.

Компонент fulleq предоставляет дополнительный оператор сравнения значений базовых типов данных, совместимый с СУБД MS SQL Server. А именно, обеспечивается совместимость сравнения двух NULL-значений, результат которого в MS SQL Server должен быть TRUE. По умолчанию в СУБД на основе PostgreSQL результат сравнения с NULL-значением равно NULL, что идет в разрез совместимости с 1С. Установку и вызов функций данного расширения Платформа 1С производит самостоятельно. Администратору надо только обеспечить установку данного расширения в составе СУБД.

3.10.3. Компонент совместимости 1С mchar

Компонент mchar предоставляет дополнительные строковые типы данных и операторы для работы с ними, совместимые с аналогичными строковыми типами данных CHAR и VARCHAR в MS SQL Server (совместимая обработка пробельных символов в конце строк; совместимое сравнение и преобразование регистра символов в строках и т.п.). Установку данного расширения и использование соответствующих строковых типов данных Платформа 1С производит самостоятельно. Администратору надо только обеспечить установку данного расширения в составе СУБД.

3.10.4. Компонент совместимости 1С online_analyze

Поддержание статистики таблиц в актуальном состоянии – важная функция СУБД, отвечающая за своевременный выбор оптимальных планов выполнения запросов. Учитывая, что 1С использует большое количество таблиц и индексов для своей работы, то рекомендуется использовать компонент online_analyze для повышения производительности работы 1С Платформы. Расширение предоставляет функциональную возможность немедленного обновления статистики таблиц после операций добавления, удаления или изменения записей в таблицах. Установку и настройку данного расширения администратор должен проводить самостоятельно в случае падения производительности отдельных обработок.

Примечание:

В последних версиях 1С отмечено, что Платформа 1С сама посылает команду ANALYZE для своевременного обновления статистики нужных таблиц. Применение этого расширения может быть уже не актуально.

3.10.5. Компонент совместимости 1С plantuner

Платформа 1С содержит большое количество таблиц и индексов для хранения своих данных, выполняет очень сложные SQL-запросы для получения итоговых или промежуточных результатов обработок. Для получения оптимальных планов сложных запросов, особенно часто возникающих при написании собственных обработок, иногда возникает необходимость адаптировать планировщик на использование тех или иных индексов таблиц. Данный компонент предназначен для расширения функций планировщика запросов. Он позволяет подключать или отключать использование определенных индексов при выполнении запросов поддержкой переменных:

— plantuner.disable_index — список индексов, которые не будет видеть планировщик;

— plantuner.enable_index — список индексов, которые будет видеть планировщик, даже если они скрыты параметром plantuner.disable_index.

Установку и настройку расширения администратор должен проводить самостоятельно в случае обнаружения фактов неправильной генерации планов запросов, ухудшающих скорость выполнения запросов.

3.11. Управление планами запросов

3.11.1. Компонент ja_Plan_Manager. Управление планами запросов

Компонент «ja_Plan_Manager» предназначен для создания, оптимизации, экспорта/импорта и подмены планов запросов в БД.

Компонент «ja_Plan_Manager» предназначен для управления процессом выполнения заранее определенных запросов с заранее определенными (альтернативными) планами в обход стандартного планировщика. Также, модуль позволяет записывать, хранить, выбирать для использования варианты планов. Полезен в случаях сложных по конструкции запросов, когда планировщик выбирает нерациональный план выполнения.

Схема работы компонента представлена на рисунке 3.51.

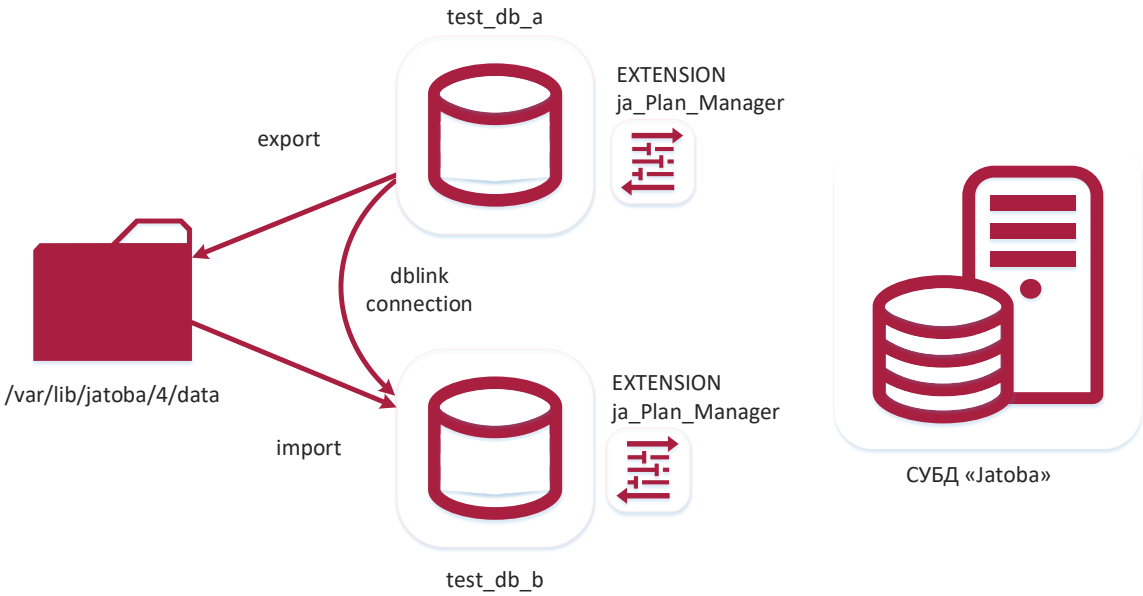


Рисунок 3.51 – Схема работы компонента

Применение к 1С: в некоторых случаях планировщик СУБД «Jatoba» выбирает неоптимальный план выполнения для SQL-запросов в 1С, несмотря на собранную статистику по соответствующим объектам БД. Это приводит к увеличению времени выполнения запросов и созданию непродуктивной нагрузки на оборудование.

Пример: длительно выполняющийся (более 40 минут) запрос в 1С, для которого планировщиком СУБД «Jatoba» выбран план выполнения с использованием конструкций Group+Sort вместо более оптимальной в данном случае конструкции HashAggregate. С помощью компонента «ja_Plan_Manager» можно прикрепить к запросу более оптимальный план с использованием конструкции HashAggregate, полученный в определенных синтетических условиях для данного проблемного запроса.

Функциональные возможности компонента позволяют:

— включать/отключать режим сохранения запросов;

— включать/отключать режим использования сохраненных запросов;

— экспортировать планы запросов в формате:

  - json;
  - text;
  - xml;
  - yaml;

— экспортировать планы запросов через:

  - домашний каталог пользователя;

- строку соединения с другой БД (dblink connection);

— импортировать планы запросов.

При использовании компонента есть возможность использовать кириллицу в именах объектов СУБД «Jatoba».

3.11.2. Компонент pg_hint_plan. Корректировка запросов

Компонент «pg_hint_plan» предназначен для корректировки планов выполнения, применяя так называемые «указания», записываемые в виде простых описаний в SQL-комментариях особого вида.

Компонент считывает указания в комментариях особого вида, заданных оператором SQL. Эта особая запись начинается с последовательности символов /*+ и заканчивается последовательностью */. Фразы указаний состоят из имени указания и последующих параметров, которые заключаются в скобки и разделяются пробелами. Такие указания могут размещаться в нескольких строках для улучшения читаемости.

3.11.3. Компонент pg_store_plans. Контроль выполненных планов запросов

Компонент «pg_store_plans» предназначен для контроля выполнения планов запросов статистическими методами всех операторов SQL, выполняемых сервером СУБД, выполненного в форме расширения.

В результате установки расширения сформируются два представления «pg_store_plans» и «pg_store_plans_info».

В представление «pg_store_plans» аккумулирует в себе основную информацию, а представление «pg_store_plans_info» содержит в себе статистику расширения «pg_store_plans».

3.12. Выявления и предотвращение исполнения нетипичных SQL-запросов

Для выявления и предотвращения исполнения нетипичных SQL-запросов используется компонент «SQL_Firewall». Компонент предназначен для защиты базы данных от SQL-инъекций или неожиданных запросов.

Компонент «SQL_Firewall» функционирует в режимах:

— "learning" – режим обучения;

— "enforcing" – режим применения;

— "permissive" – режим разрешающий любые SQL запросы;

— "disabled" – режим отключенного модуля.

Накопленные SQL-запросы хранятся и их можно просмотреть и скорректировать.

```
Администратор: Командная строка - psql -h localhost -d postgres -U postgres
postgres=# select userid, queryid, calls, substring (query from 0 for 90) from sql_firewall.sql_firewall_statements;
 userid |  queryid   | calls |                                          substring

--------+------------+-------+-------------------------------------------------------------------------------------------
-
     10 |  416111272 |     2 | SELECT c.oid, a.attnum, a.attname, c.relname, n.nspname, a.attnotnull OR (t.typtype = 'd'
     10 | 3337577423 |     1 | SELECT p.oid as poid,p.*,pg_catalog.pg_get_expr(p.proargdefaults, 0) as arg_defaults,d.de
     10 | 3203136618 |     1 | select userid, queryid, calls from sql_firewall.sql_firewall_statements;
     10 | 1448787127 |     8 | SHOW search_path
     10 |  716865367 |     1 | SELECT c.relname,a.*,pg_catalog.pg_get_expr(ad.adbin, ad.adrelid, true) as def_value,dsc.
     10 | 3492580944 |     1 | SELECT n.nspname = ANY(current_schemas(true)), n.nspname, t.typname FROM pg_catalog.pg_ty
     10 | 2325728049 |     1 | select c.oid,pg_catalog.pg_total_relation_size(c.oid) as total_rel_size,pg_catalog.pg_rel
     10 | 3886090111 |     1 | select userid, queryid, query from sql_firewall.sql_firewall_statements;
     10 | 1395260778 |     3 | SET application_name = 'PostgreSQL JDBC Driver'
     10 | 1315065821 |     1 | SET SESSION CHARACTERISTICS AS TRANSACTION ISOLATION LEVEL READ COMMITTED
     10 | 4235059156 |     2 | insert into table_a values(1, 2, 'Lorem ipsum dolor sit amet, consectetur adipiscing elit
     10 | 2279677621 |     1 | create database test_db
```

Рисунок 3.52 – Просмотр правил брандмауэра в ОС Windows

```
root@ubuntu: /usr/jatoba-4/bin
File  Edit  View  Search  Terminal  Help
postgres=# select * from sql_firewall.sql_firewall_statements;
 userid |  queryid   |          query          | calls
--------+------------+-------------------------+-------
     10 | 3226304309 | select * from table_b; |     1
     10 | 2886906670 | select * from table_c; |     1
(2 rows)

postgres=#
```

Рисунок 3.53 – Просмотр правил брандмауэра в ОС GNU/Linux

В полученном списке отражены поля:

— userid – идентификационный номер пользователя (идентификационный номер 10 присваивается роли postgres);

— Qweryid – идентификационный номер запроса;

— Qwery – тело запроса;

— Calls – вызовы.

3.13. Регистрация событий безопасности

В комплект поставки СУБД входят компоненты регистрации событий:

— «pgAudit» – компонент расширенного журналирования событий СУБД;

— «ja_Log» – компонент централизованного сбора записей событий СУБД;

— «ja_seceventlog» - компонент записи событий безопасности;

— «pgBadger» – компонент формирования отчетов по журналам СУБД.

В зависимости от поставленных задач перечень используемых компонентов может меняться.

3.13.1. Расширенная регистрация событий СУБД

Компонент «pgAudit» обеспечивает расширенное журналирование событий дополняя поле «Error message». Таким образом регистрируются дополнительные SQL-команды.

Сравнение регистрируемых SQL-команд при стандартной регистрации событий СУБД и с применением компонента «pgAudit» приведены в таблице 3.4.

Таблица 3.4 – Сравнительная таблица регистрируемых SQL-команд

log_statement		**pg_Audit**	
Параметр	**SQL-команды записывать в журнал**	**Параметр**	**SQL-команды записывать в журнал**
ALL		ALL	
		READ	SELECT
			COPY TO
MOD	INSERT	WRITE	INSERT
	UPDATE		UPDATE
	DELETE		DELETE
	TRUNCATE		TRUNCATE
	COPY FROM		COPY FROM
	PREPARE		
	EXECUTE		
	EXPLAIN ANALYZE		
DDL	CREATE	DDL	CREATE
	ALTER		ALTER
	DROP		DROP
		FUNCTION	CALL
			DO
		ROLE	GRANT
			REVOKE
			ALTER DEFAULT PRIVILEGES
			SET ROLE
		MISC	DISCARD
			FETCH
			CHECKPOINT
			VACUUM

log_statement		pg_Audit	
Парамет р	**SQL-команды записывать в журнал**	**Параметр**	**SQL-команды записывать в журнал**
			SET
		MISC_SET	SET
NONE		NONE	

3.13.2. Компонент «ja_seceventlog»

Компонент «ja_seceventlog» формирует событий безопасности СУБД в соответствии с ГОСТ-Р-59548-2022 «Национальный стандарт Российской Федерации. Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации» и хранения их в отдельном каталоге.

Компонент устанавливает собственные и независимые параметры регистрации событий и вырезает события безопасности из журнала аудита СУБД, складывая их

— в свой журнал (в отдельном каталоге);

— во временную таблицу в БД.

При этом параметры регистрации событий безопасности гораздо шире чем в компоненте «pg_audit».

Перечень регистрируемых событий регулируется установленными фильтарми.

Для передачи событий безопасности в JDS используются компонент «ja_Log»

3.13.3. Централизованный сбор событий СУБД

Компонент «ja_Log» предназначен для сбора событий безопасности с целевых СУБД «Jatoba» в служебную СУБД «Jatoba data safe».

При клиент-серверной установке на серверах целевых СУБД устанавливается агент компонента, а на сервере служебной СУБД серверная часть компонента. Передача данных осуществляется по протоколу Libpq или TLS.

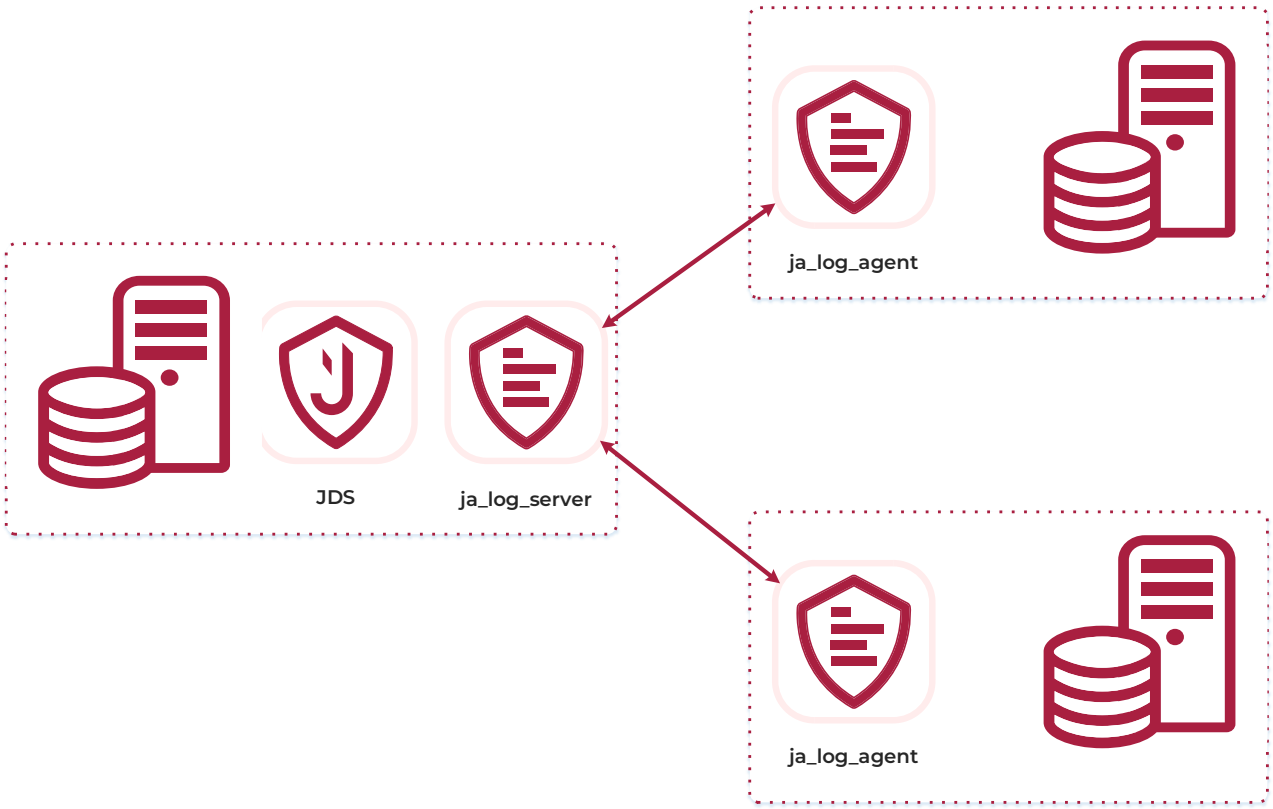


Рисунок 3.54 – Схема работы компонента при клиент-серверной установке

3.13.4. Формирование отчетов по журналам СУБД

Компонент «pgBadger» обладает следующими функциональными возможностями:

— сбор общих данных о работе СУБД из файлов регистрации событий, в том числе о сессиях пользователя (выполненные SQL-запросы), и предоставление данных администратору в виде HTML-отчетов;

— выявление проблемных мест в производительности СУБД;

— поиск и анализ запросов, подлежащих оптимизации.

3.14. Парольные политики

Парольные политики реализуются компонентом «SecurityProfile» при методе идентификации PASSWORD.

Привилегированный пользователь имеет возможности:

— смены пароля пользователя;

— снятия блокировки пользователя;

— создания профиля парольной политики;

— назначения пользователю профиля парольной политики;

— смены параметров профиля парольной политики и т.д.

Компонент «SecurityProfile» имеет функциональную возможность распределять учетные записи по применяемым к ним парольным политикам. Как было описано ранее, возможно применять парольные политики по умолчанию, создавать собственные, либо использовать преднастроенные профили парольных политик.

Роли (пользователи) СУБД могут прикрепляться к вновь создаваемым или к преднастроенным профилям парольных политик:

— FSTEC_1_class – профиль для ИС первого класса защищенности;

— FSTEC_2_class – профиль для ИС второго класса защищенности;

— CIS – профиль, основанный на рекомендациях Center for Internet Security;

— Corporate_1 – корпоративный профиль первого уровня для учетных записей пользователей;

— Corporate_2 – корпоративный профиль второго уровня для учетных записей администраторов программных (программно-аппаратных средств);

— Corporate_3 – корпоративный профиль третьего уровня для технических (сервисных, служебных) учетных записей, используемых в технологических процессах ИС или встроенных производителями программных (программно-аппаратных) средств в такие средства.

3.15. Поддержка работы СУБД с геоданными

В СУБД «Jatoba» реализован набор расширений PostGIS, обеспечивающий управление пространственными данными для построения на базу СУБД геоинформационных систем. Набор расширений включает дополнительные типы данных и процедуры обработки данных этих типов.

3.16. Контроль целостности

СУБД «Jatoba» на уровне ядра поддерживает несколько механизмов обеспечения целостности данных.

Первый встроенный механизм СУБД позволяет проводить проверки корректности данных, которые пользователь вносит в базу данных. Реализована программная возможность включения этих проверок для отдельных полей таблиц по выбору пользователя. Также реализована система ограничений, накладываемая на

данные, помещаемые в таблицы. Данные ограничения позволяют обеспечивать ссылочную целостность данных в разных таблицах.

Вторым механизмом контроля целостности является компонент «ja_CSum» предназначенный для выполнения периодических фоновых проверок фалов, расположенных в ключевых директориях СУБД, а также:

— конфигурации системы управления базами данных;

— конфигураций баз данных;

— процедур (программного кода) системы управления базами данных;

— процедур (программного кода), хранимых в базах данных.

Компонент «ja_CSum» опосредовано может взаимодействовать с другими компонентами СУБД «Jatoba», такими как:

— пользовательский веб-интерфейс для администраторов, компонент «Jatoba data safe» (643.72410666.00067-075 98 01-07 Руководство по настройке. Часть 7);

— компонент централизованного сбора записей событий СУБД «ja_Log» (643.72410666.00067-075 98 01-12 Руководство по настройке. Часть 12).

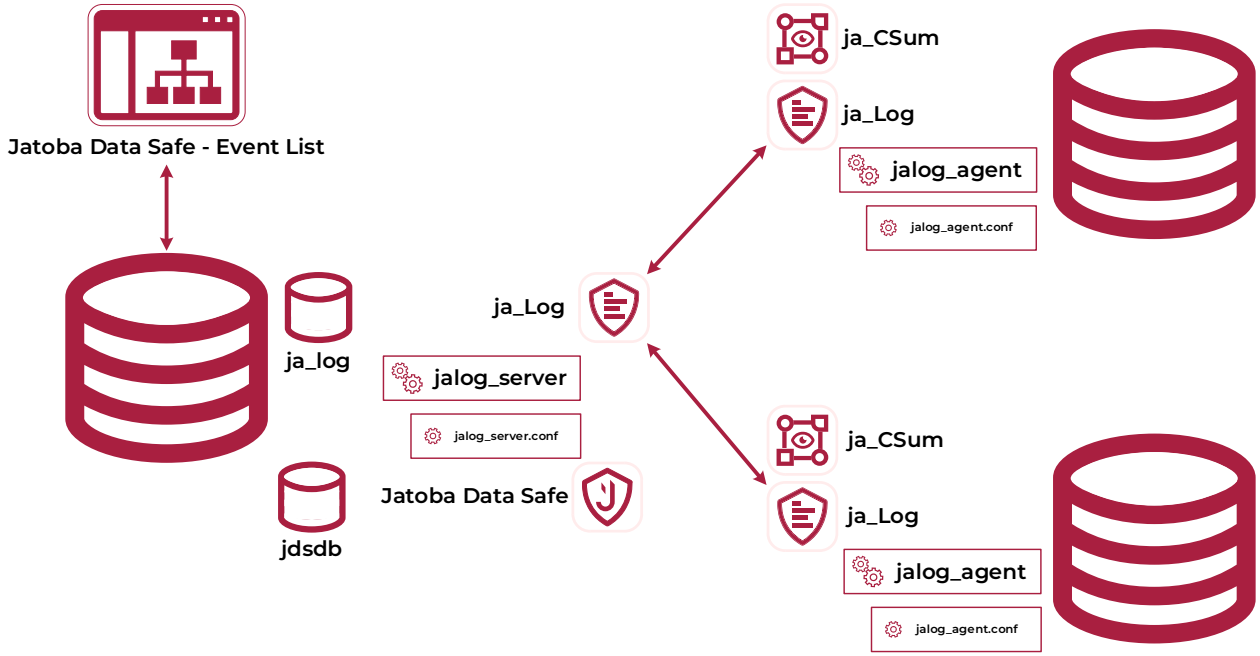


Рисунок 3.55 – Схема взаимодействия компонентов

В процессе работы «ja_CSum» записывает сгенерированные события безопасности в СУБД (в хранилище событий).

Компонент централизованного сбора записей событий СУБД «ja_Log», получив указание от сервера, собирает события безопасности базы данных «ja_Log» в служебную СУБД компонента «Jatoba data safe».

Из базы данных события безопасности передаются в пользовательский веб-интерфейс для администраторов компонента «JDS», который передает события безопасности в разделе «Event List».

Отфильтровать события безопасности можно при помощи текстового поиска, как представлено на рисунке 3.56.

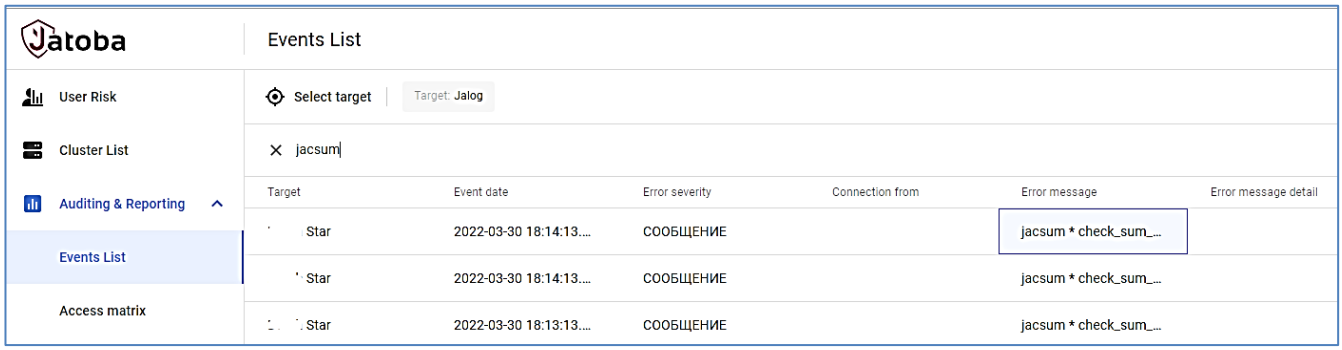


Рисунок 3.56 – Отображение событий безопасности в веб-интерфейсе

3.17. Обфускации кода

Компонент обфускации кода PL/pgSQL добавляет в СУБД новый язык plspgsql, обеспечивающий разработчику дополнительные функции безопасности при создании хранимых процедур.

В состав СУБД «Jatoba» включена утилита обфускации wplpgsql, которая создает в dst-dir обфусцированную версию src-dir с заменой процедур и функций с языка 'plpgsql' на 'plspgsql'.

Утилита обфускации использует серверную часть СУБД для обфускации отдельных SQL-команд.

Процесс сокрытия исходных текстов, процедур и функций в СУБД «Jatoba» отображен на рисунке 3.57.

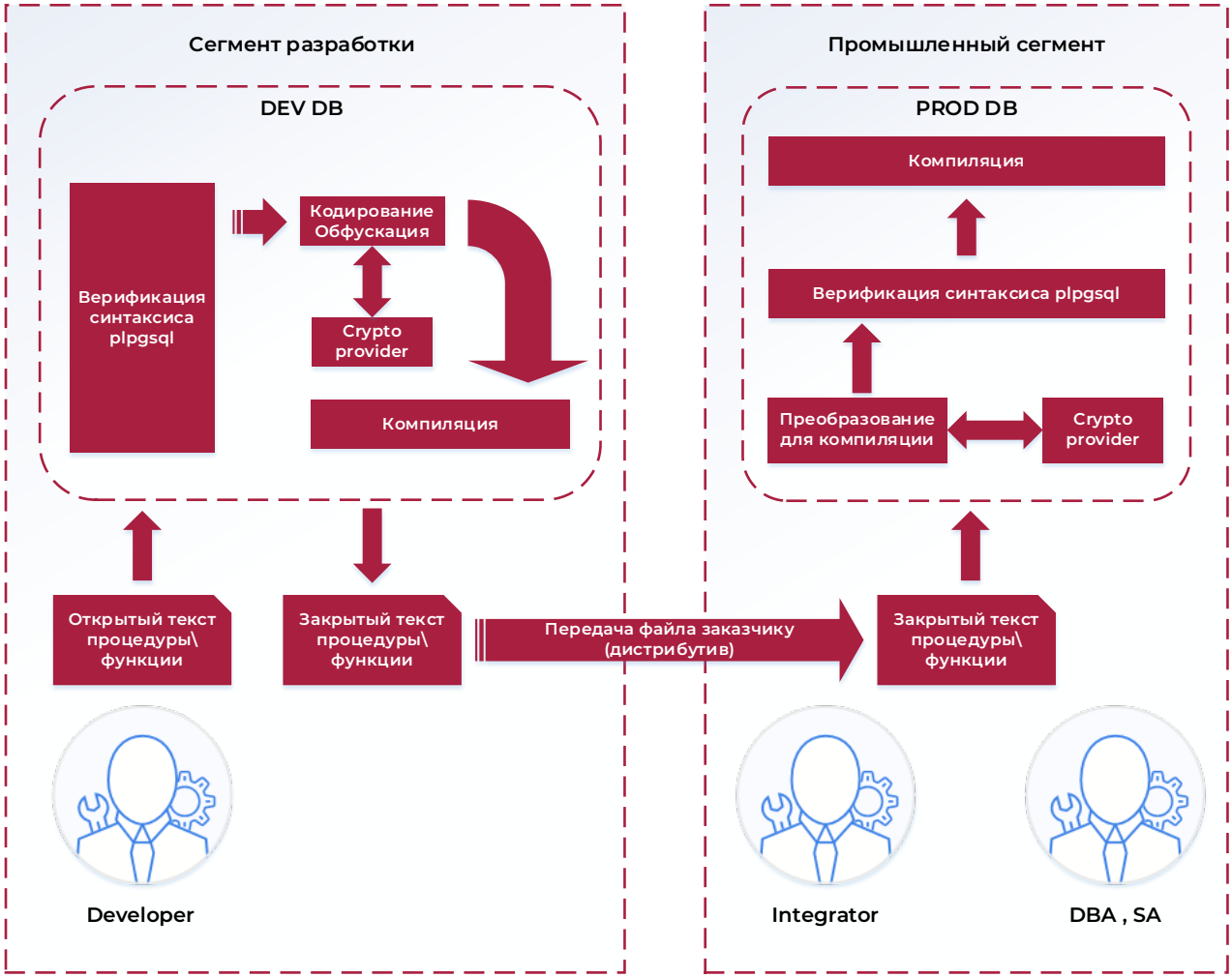


Рисунок 3.57 – Процесс сокрытия процедур и функций в СУБД «Jatoba»

3.18. Формирование HTTP/HTTPS запросов из СУБД

Компонент формирования HTTP/HTTPS запросов из СУБД «pgSQL-HTTP» поддерживает формирование HTTP-запросов (http_request) к СУБД и формирование HTTP-ответов (http_response) из СУБД.

В частности, поддерживает функции:

— http_header;

— http;

— http_get;

— http_post;

— http_put;

— http_patch;

— http_delete;

— http_head;

— http_set_curlopt;

— http_reset_curlopt;

— http_list_curlopt;

— urlencode.

Например

Для отправки простого документа JSON на веб-сервер формируется SQL-команда:

```
SELECT status, content_type, content::json->>'data' AS data
  FROM http_patch('http://httpbin.org/patch',
'{"this":"that"}', 'application/json');
```

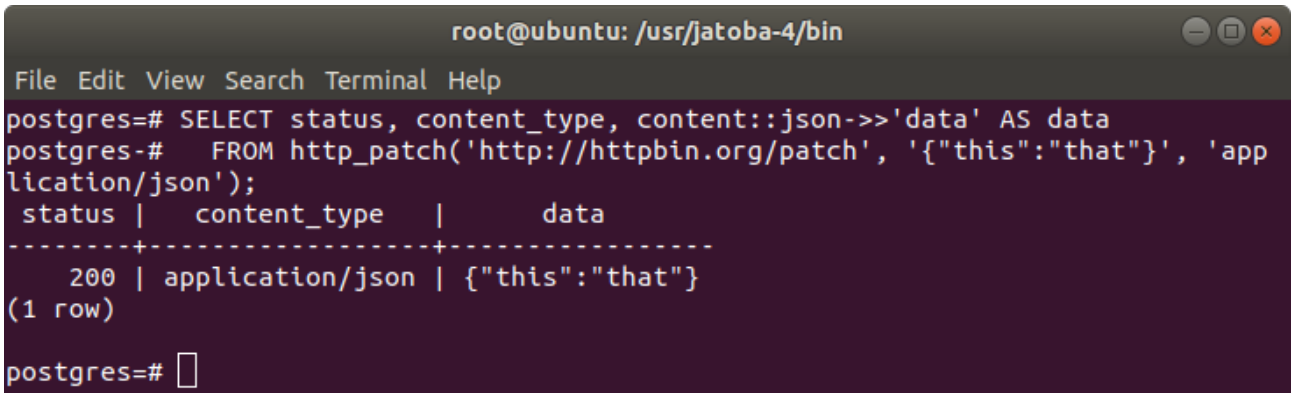


Рисунок 3.58 – Отправка простого документа JSON

3.19. Компрессия данных. Компонент «ja_Compression»

Компонент «ja_Compression» предназначен для экономии имеющегося дискового пространства физического сервера СУБД.

Для каждой таблицы СУБД «Jatoba», соответствуют определённые файлы на диске. В файлы данные поступают в следующих обстоятельствах: после операций commit, checkpoint и вытеснения буфера из памяти на диск.

Табличные пространства стоят выше по иерархии чем БД, поэтому возможны следующие варианты использования компрессии:

- табличные пространства с компрессией;

Все включенные и/или перенесенные таблицы, индексы и БД будут подвергнуты компрессии:

— таблицы с компрессией;

— индексы с компрессией.

Компонент совместим с БД 1С и может использоваться с любыми конфигурациями.

3.20. Полнотекстовый поиск и определение похожих текстов

Компонент «ja_Similar» предназначен для предоставления функции и операторы для определения схожести текстов на основе техники хеширования, чувствительного к близким значениям (Locally-Sensitive Hashing, или LSH).

Решение такого типа задачи ранее не было доступно в PostgreSQL. С помощью этого расширения решаются типы задач:

- поиск плагиата;
- сравнение содержания статей;
- дедупликация документов;
- поиск аномалий в типовых документах;
- сравнение с эталоном на схожесть.

Загружая в БД искомый текст и дамп текстов, применяя стандартный SQL-запрос получается список статей, содержимое которых имеет схожесть с нашим искомым куском текста, и эту самую расчетную схожесть.

```
SELECT t.id, minhash_similarity(t.text_col, :'query_text')
AS similarity
     FROM user_tbl AS t
     WHERE t.content <~> :'query_text'
     ORDER BY similarity DESC;
```

```
admin1@ubuntu: ~
postgres=# SELECT t.id, t.title, minhash_similarity(t.content, :'query_text') AS
 similarity
postgres-#     FROM articles AS t
postgres-#     WHERE t.content <~> :'query_text'
postgres-#     ORDER BY similarity DESC;
 id |   title    | similarity
----+-----------+------------
 71 | Aristotle |      0.875
(1 row)

postgres=#
```

Рисунок 3.59 – Запрос и вывод схожести текстов

3.20.1. Проверка орфографии и морфологический анализ. Компонент «hunspell»

Компонент «hunspell» - это свободная библиотека для проверки орфографии и морфологического анализа.

обеспечивает:

— Проверку правописания;

— Поддержку множества языков за счёт внешних словарей.

При совместном использовании компонентов tsvector2 и hunspell доступно:

— Искать слово в любом падеже (например, "проверка" → найдёт и "проверки", и "проверку");

— Игнорировать стоп-слова (если они заданы в конфигурации);

— Строить эффективные индексы для быстрого поиска.

3.21. Поиск ближайших соседей (KNN для B-TREE)

Метод K-ближайших соседей (K-nearest neighbors, KNN) — это метод, используемый для решения задач классификации и регрессии. KNN основан на идее, что объекты, которые находятся рядом в пространстве признаков, вероятно относятся к одной категории.

При использовании KNN для классификации нового объекта вычисляются расстояния до всех известных объектов в наборе. Затем выбирается K объектов с наименьшими расстояниями (ближайшие соседи).

Области применения метода KNN:

— предварительная обработка данных;

— механизмы рекомендаций;

— финансы: (прогнозирование фондового рынка, курсы валют, торговые фьючерсы и анализ отмывания денег);

— здравоохранение;

— распознавание образов: (идентификация шаблонов, например, при классификации текста и цифр).

Когда выполняется поиск на основе этого индекса, он проходит вниз по дереву, чтобы найти ключ, по которому дерево построено, а затем возвращает искомые данные. Использование индекса гораздо быстрее, чем последовательное сканирование.

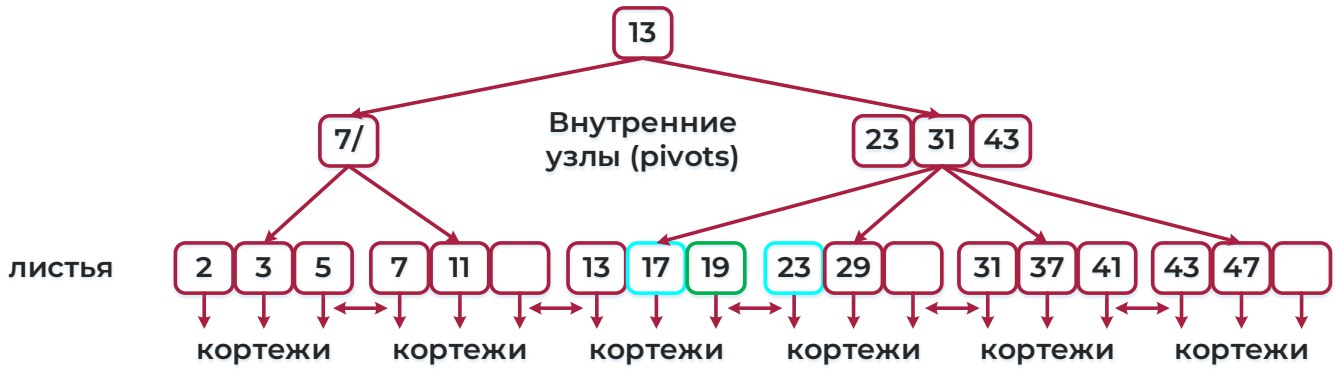


Рисунок 3.60 – K Nearest Neighbors для B-tree

3.22. 64-битный счетчик транзакций. Компонент XID64

Для обеспечения работы механизма MVCC (управление параллельным доступом посредством многоверсионности транзакций) СУБД «Jatoba» отслеживает, какие транзакции уже завершены, а какие еще активны.

Для этого каждой транзакции в СУБД «Jatoba» присваивается уникальный номер — идентификатор (xid). Его можно узнать, используя функцию txid_current().

Применяемый 64-битный счетчик транзакции xid64 в СУБД «Jatoba» в условиях высокой транзакционной нагрузки, позволяет избежать его «переполнения» (как в случае использования 32-битного счетчика и риска остановки работы БД) и дает гораздо большую свободу администраторам БД.

3.23. Инвентаризация СУБД. Компонент «ja_Inventory»

Компонент «ja_Inventory» предназначен для сбора информации об установленных СУБД «Jatoba» в форме отчета в формате JSON. В отчет включается информация о:

— версии СУБД;

— количествах ядер сервера;

— используемых расширениях.

Отчет имеет вид, показанный на рисунке 3.61.

```
{
    "utilName": "ja_inventory",
    "utilVersion": "1.0.0",
    "orgName": "Datagile",
    "reportDate": "2024-12-19T02:23:41.761-0800",
    "hostName": "ubuntu",
    "jatobaVersion": "Jatoba 6.6.1-57250 (build-id: 606f0792; build-os: UBUNTU20.04)",
    "coreCount": "1",
    "extensionsInstalled": [
        {
            "extensionName": "ja_plan_manager"
        },
        {
            "extensionName": "plpgsql"
        }
    ]
}
```


Рисунок 3.61 – Вид отчета о хосте

3.24. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации

Выполнение условий эксплуатации, в частности исключение применения метода аутентификации «Trust», который предполагает, что любой подключающийся к серверу пользователь авторизован для доступа к базе данных вне зависимости от указанного имени пользователя базы данных, позволяет запретить любые действия пользователей, разрешенных до идентификации и аутентификации.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

DDL	–	Data Definition Language, язык описания данных
DML	–	Data Manipulation Language, язык манипулирования данными
SQL	–	Structured Query Language, язык структурированных запросов
БД	–	База данных
ГИС	–	Государственные информационные системы
Дист.	–	Дистрибутив
ИСПДн	–	Информационная система персональных данных
КВО	–	Критически важный объект
КИИ	–	Критическая информационная инфраструктура
Обр.к	–	Образ контейнера
ОС	–	Операционная система
СУБД	–	Система управления базами данных
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
ЭВМ	–	Электронно-вычислительная машина

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

№ изменения:____________	Подпись отв. лица:___________	Дата внесения изм.:__________