УТВЕРЖДЕН
643.72410666.00067-07 98 01-ЛУ

ЗАЩИЩЕННАЯ СИСТЕМА УПРАВЛЕНИЯ
БАЗАМИ ДАННЫХ «JATOBA»

Руководство по настройке. Часть 7. Пользовательский веб-интерфейс для администраторов. Компонент «Jatoba data safe»

643.72410666.00067-07 98 01-07

Листов 250

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

2024

Литера O_1

АННОТАЦИЯ

В данном руководстве приведены сведения, необходимые для установки и эксплуатации компонента пользовательского веб-интерфейса для администраторов «Jatoba data safe» (далее по тексту – компонент или JDS).

Степени важности примечаний, применяемые в документе:

Важная информация – указания, требующие особого внимания

Дополнительная информация – указания, позволяющие упростить работу с изделием

Для СУБД «Jatoba» версии ядра 4, 5, 6 и 18 используется версия компонента — 2.10.

Важная информация

Для сертифицированной версии СУБД «Jatoba» поддерживается работа только на ОС, указанных в формуляре на поставку!

СОДЕРЖАНИЕ

1. Назначение компонента ... 8
1.1. Структура документации компонента ... 10
1.2. Функциональны возможности ... 10
1.3. Требования к среде функционирования ... 12
1.4. Компоненты, используемые для работы JDS ... 15
1.5. Разделы JDS совместимые с СУБД PostgreSQL ... 16
2. Установка и настройка ... 20
2.1. Аутентификация пользователей JDS ... 20
2.1.1. Ролевая модель JDS ... 21
2.1.2. Модель ролевой консолидации JDS и целевой СУБД ... 24
2.1.3. Создание пользователей JDS ... 24
2.1.4. Подключения LDAP ... 26
2.2. Вкладка «Безопасность». Парольная политика JDS ... 31
2.2.1. Смена пароля пользователя JDS администратором ... 34
2.2.2. Смена пароля пользователем JDS ... 34
2.2.3. Блокирование пользователя JDS администратором ... 35
2.2.4. Разблокирование пользователя JDS ... 36
2.3. Вкладка «Источники данных» ... 37
2.3.1. Информирование о неполном перечне наблюдаемых СУБД ... 39
2.4. Установка прав доступа к конфигурационным файлам ... 39
2.4.1. Установка прав доступа к конфигурационному файлу appsettings.json ... 39
2.4.2. Установка параметров в конфигурационного файле appsettings.json JDS ... 40
3. Раздел «Ландшафт» (Landscape) ... 42
3.1. Навигация в разделе «Ландшафт» ... 43
3.2. Хост. Вкладка «Обзор» ... 45
4. Раздел «Ландшафт». СУБД. Вкладка «Обзор» ... 47
5. Раздел «Ландшафт». СУБД. Вкладка «Назначение ролей» ... 48
6. Раздел «Ландшафт». СУБД. Вкладка «Параметры СУБД» ... 49
6.1. Шаблоны ... 50
6.1.1. Создание шаблона ... 51
6.1.2. Импорт шаблона ... 51
6.1.3. Применение шаблона к СУБД ... 52
7. Раздел «Ландшафт». СУБД. Вкладка «Правила доступа» ... 54
8. Раздел «Ландшафт». СУБД. Вкладка «Доступные расширения» ... 57
9. Раздел «Ландшафт». СУБД. Вкладка «Роли СУБД» ... 59
9.1. Список пользователей ... 59
9.2. Создание роли ... 60

9.2.1. Вкладка «Основные параметры» (Main settings); ... 60
9.2.2. Вкладка «Атрибуты» ... 61
9.2.3. Вкладка «Роли и группы» (Roles and groups) ... 63
9.2.4. Вкладка «Привилегии» (Privileges) ... 66
9.2.5. Вкладка «SQL» ... 69
9.3. Редактирование роли ... 70
9.4. Недоступные функциональные возможности. «Работа с блокировками» ... 70
9.5. Удаление роли ... 71
9.6. Псевдороль «Public» ... 72
10. Раздел «Ландшафт». СУБД. Вкладка «Список событий» (Event List) ... 73
10.1. Выбор служебной БД ... 73
10.2. Фильтр событий ... 74
10.3. Просмотр списка событий ... 77
10.4. Выбор столбцов (Columns) ... 77
10.5. Сортировка списка событий ... 79
10.6. Полнотекстовый поиск событий ... 79
11. Раздел «Ландшафт». СУБД. Вкладка «Проблемы и решения» (Problems & Solutions) ... 81
11.1. Вкладка «Правила сканирования» ... 81
11.2. Режим сканирования ... 82
11.3. Вкладка «Задачи» ... 85
11.4. Работа нескольких пользователей с подразделом «Проблемы и решения» (Problems & Solutions) ... 89
12. Раздел «Ландшафт». СУБД. Вкладка «Активность БД» (DB Activity) ... 91
12.1. Вкладка «Сессии» (Session) ... 91
12.1.1. Завершение сессии (End session) ... 94
12.2. Вкладка «Блокировки» (Locks) ... 96
12.2.1. Завершение заблокированной сессии ... 96
12.3. Вкладка «Подключения» ... 98
13. Раздел «Ландшафт». СУБД. Вкладка «LDAP синхронизация» (LDAP Sync) ... 100
13.1. Табличная часть «Профили» (Profiles) ... 101
13.1.1. Создание профиля синхронизации с Active Directory ... 101
13.1.2. Создание профиля синхронизации с ALD Pro ... 102
13.1.3. Создание профиля синхронизации с FreeIPA ... 104
13.1.4. Создание профиля синхронизации с Samba ... 105
13.1.5. Настройка LDAPS для сервера СУБД в ОС семейства Windows и GNU/Linux ... 108
13.1.6. Редактирование и удаление профиля синхронизации ... 109
13.2. Табличная часть «Маппинг» (Mappings) ... 110
13.2.1. Создание профиля маппинга Active Directory ... 110
13.2.2. Создание профиля маппинга ALD Pro ... 112
13.2.3. Создание профиля маппинга FreeIPA ... 113

13.2.4. Создание профиля маппинга Samba ... 115
13.2.5. Редактирование и удаление профиля маппинга ... 118
13.3. Табличная часть «Журнал» (Log) ... 119
14. Раздел «Ландшафт». СУБД. Вкладка «Парольные политики» (Password policies) ... 121
14.1. Вкладка «Управление политиками» (Policy management) ... 121
14.2. Вкладка «Привязка ролей» (Role Binding) ... 122
14.3. Вкладка «Работа с блокировками» ... 123
14.3.1. Вкладка «securityprofile» ... 123
14.3.2. Вкладка «checksum» ... 124
15. Раздел «Ландшафт». БД. Вкладка «Обзор» ... 126
16. Раздел «Ландшафт». БД. Вкладка «Расширения» ... 127
16.1. Установка расширения в БД ... 127
16.1.1. Удаление расширений БД ... 128
16.2. БД. Установка расширения pg_profile ... 129
16.3. БД. Установка расширения securityprofile (парольные политики) ... 133
16.4. БД. Установка расширения ja_csum (контроль целостности) ... 135
17. Раздел «Ландшафт». БД. Вкладка «Матрица доступа» (Access matrix) ... 137
17.1. Выбор субъектов ... 138
17.2. Фильтр «Матрицы доступа» ... 139
18. Раздел «Ландшафт». БД. Вкладка «Анализ рисков» (User Risk) ... 142
18.1. Выбор схемы данных (Schema) ... 142
18.2. Отображение матрицы ... 142
18.3. Диаграмма ... 144
19. Раздел «Ландшафт». Вкладка «Кластеры jaDog» ... 145
19.1. Навигация в разделе ... 145
19.1.1. Вкладка «Обзор» параметров узла ... 147
19.1.2. Вкладка «Структура» ... 147
19.1.3. Вкладка «Репликация» ... 148
19.1.4. Вкладка «Обзор» кластера ... 148
19.1.5. Вкладка «Список узлов» ... 149
19.1.6. Вкладка «Параметры» ... 151
19.2. Подключение к существующему кластеру ... 152
19.3. Создание кластера ... 153
19.4. Подключение узла кластера ... 154
19.4.1. Каскадная репликация ... 155
19.5. Активация/деактивация PublicIP кластера ... 155
19.6. Назначение узлу роли Мастер ... 156
19.7. Удаление узла ... 157
19.8. Дата-центр ... 157

19.8.1. Подготовительные действия для создания кластера ... 159
19.8.2. Создание/удаление Дата-центров ... 161
19.8.3. Присоединение узлов кластера к Дата-центру ... 162
19.9. Отключение кластера от JDS ... 164
20. Раздел «Мониторинг» (Monitoring) ... 165
20.1. Библиотека виджетов ... 166
20.2. Добавление панели виджетов ... 169
20.3. Панель виджетов для кластера ja_Hipe_Cluster ... 170
20.4. Уведомления. Информирование о заданном значении показателя ... 171
21. Раздел «Анализ запросов» (Query analysis) ... 173
21.1. Вкладка «Запросы» ... 173
21.2. Вкладка «Мегазапросы» ... 178
21.3. Вкладка «Блокировки» ... 180
21.4. Вкладка «Ошибки» ... 182
21.4.1. Вкладка «по хостам» ... 183
21.4.2. Вкладка «по ошибкам» ... 185
21.5. Вкладка «Статистика» ... 186
21.6. Вкладка «Настройки» ... 187
21.7. Форматирование запроса ... 187
21.8. Добавление плана запроса ... 188
21.8.1. Форматированное текстовое представление плана запроса ... 190
21.8.2. Сравнительные диаграммы плана запроса ... 192
21.8.3. Функциональная диаграмма плана запроса ... 194
21.8.4. Модель плана запроса ... 195
21.8.5. Диаграмма отношений таблиц ... 195
21.8.6. Автоматические рекомендации по повышению качества запросов ... 196
22. Подраздел «Подключения JDS» (JDS connections) ... 198
23. Раздел «Резервное копирование» (Backup) ... 200
23.1. Настройки для ProBackUp ... 200
23.2. Вкладка «Хранилища» ... 201
23.3. Вкладка «Резервные копии» ... 202
23.4. Восстановление резервной копии ... 204
24. Раздел «Снимки и отчеты» (Snapshots & Reports) ... 205
24.1. Вкладка «Снимки» (Snapshots) ... 205
24.2. Вкладка «Baseline» ... 207
24.3. Вкладка «Отчеты» (Reports) ... 207
25. Раздел «Уведомления» (Notifications) ... 210
25.1. Подраздел «Настройки» (Settings) ... 210
25.1.1. Сервисы Email (Email services) ... 210

25.1.2. Сервисы Zulip (Zulip services) ... 212
25.1.3. Настройки обработки (Processing settings) ... 216
25.2. Подраздел «Подписки» (Subscriptions) ... 217
25.2.1. Ошибки БД ... 221
25.2.2. События учетных записей ... 223
25.2.3. Произвольный текст ... 225
25.2.4. Канал событий программного компонента JDS ... 225
25.3. Подраздел «Сообщения» (Messages) ... 226
25.3.1. Очередь (queue) ... 226
25.3.2. Обработчики (Handlers) ... 229
25.4. Журнал сообщений (Message log) ... 229
26. Журналы событий JDS ... 231
27. Сообщения об ошибках ... 233
27.1. Ошибка при проверке подключения к цели: 28P01 ... 233
27.2. Ошибка при проверке подключения к цели ... 233
27.3. Ошибка настройке конфигурационного файла: 28000 ... 233
27.4. Ошибка при получении списка записей журнала ldapsync ... 233
27.5. Ошибка при получении списка профилей ldapsync ... 234
27.6. Ошибка при создании профиля ldapsync ... 234
27.7. Ошибка при создании/обновления маппинга ldapsync ... 234
27.8. Ошибка при создании одноименного профиля ldapsync ... 234
27.9. Ошибка выполнения синхронизации ... 235
27.10. Сообщение «Синхронизация частично выполнена» ... 235
27.11. Ошибка при добавлении в кластер Master узла ... 236
27.12. Ошибка при создании канала событий ... 236
27.13. Дублирование сообщений при рассылке уведомлений ... 236
27.14. Резервное копирование ... 237
Приложение 1 ... 238
Перечень «Классов событий» используемых в подразделе «Подписки» ... 238
Термины и определения ... 247
Перечень сокращений ... 249

1. НАЗНАЧЕНИЕ КОМПОНЕНТА

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

Разделы «Матрица доступа» и «Анализ рисков» используются для:

— проведения оперативного контроля назначенных прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

— расследования инцидентов безопасности;

— формирования аттестационной документации для АРМ и проведения ЕТК, в частности для документа – разрешительная система доступа;

— сертификационной документации Системы менеджмента информационной безопасности (далее – СМИБ) (ISO/IEC 27001);

— прохождения ежегодного аудита органом по сертификации СМИБ.

Конфигурирования и управления СУБД и кластером.

Раздел 19 «Ландшафт» позволяет управлять кластером серверов СУБД. Раздел представляет собой графическое отображение управления компонентом «jaDog».

Раздел 10 «Список событий (Event List)» предназначен для просмотра событий безопасности в выбранной инсталляции (Target). Разработан с учетом требований ГОСТ Р 59548 – 2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

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.

Раздел 24 «Снимки и отчеты (Snapshots & Reports)» предназначен для создания снимков состояния БД (Snapshots) и получения отчетов. Формирование статической информации выполняется компонентом «pg_Profile».

Раздел 10 «Проблемы и решения (Problems & Solutions)» представляет собой интеллектуальный инструмент, который позволяет определять ряд проблем, существующих в целевой СУБД.

Раздел 21 «Анализ запросов» предназначен для визуализации плана запроса средствами Pg-explain;

Раздел 12 «Активность БД» предназначен для мониторинга активности СУБД;

Раздел 21 «Подключения JDS» предназначен для отображения количество подключений к компоненту.

Раздел 13 «LDAP синхронизация (LDAP Sync)» предназначен для графического отображения операций по синхронизации учетных записей со службами каталогов и учетных записей целевой СУБД. Для выполнения синхронизации требуется, чтобы расширение было установлено на целевой СУБД.

Раздел 23 «Уведомления» (Notifications)» предназначен для:

— настройки сервисов отправки сообщений (Zulip) и писем (Email);

— настройки периодичности отправки сообщений и писем;

— формированию подписок на события безопасности пользователей JDS;

— отправки сообщений и писем;

— отправки писем с вложениями пользователей JDS подписанным на события безопасности.

Раздел 18 «Ландшафт» предназначен для управления СУБД.

Раздел 9 «Роли БД» предназначен для администрирования ролей целевой СУБД.

Раздел 23 предназначен для управления:

— парольными политиками на целевой СУБД;

— блокированием/разблокированием ролей.

Раздел 23 предназначен для управления резервными копиями

1.1. Структура документации компонента

Документация компонента имеет распределенную структуру.

Установка компонента описана в документе «Руководстве по установке».

Подготовка хостов и развертывание СУБД «Jatoba», настройка SSH и SSL соединений описана в документе «Руководство по безопасности».

Функциональные возможности компонента разделов компонента описаны в настоящем документе.

1.2. Функциональны возможности

Компонент пользовательского веб-интерфейса обладает следующими функциональными возможностями:

— просмотр событий безопасности;

— управление кластером СУБД;

— формирование матрицы привилегий пользователей;

— формирование матрицы системных привилегий пользователей;

— формирование отчетов о СУБД;

— синхронизация учетных записей пользователей;

— управление ролями в целевой СУБД;

— управление парольными политиками в целевой СУБД.

Клиентское приложение выполнено в форме веб-приложения и работает по клиент-серверной технологии. Возможна клиент-серверная и локальная установка.

При клиент-серверной установке компонент будет использовать СУБД как служебную со служебной БД, а остальные СУБД будут для него в качестве целевых СУБД.

Схема работы компонента при клиент-серверном варианте представлена на рисунке 1.1.

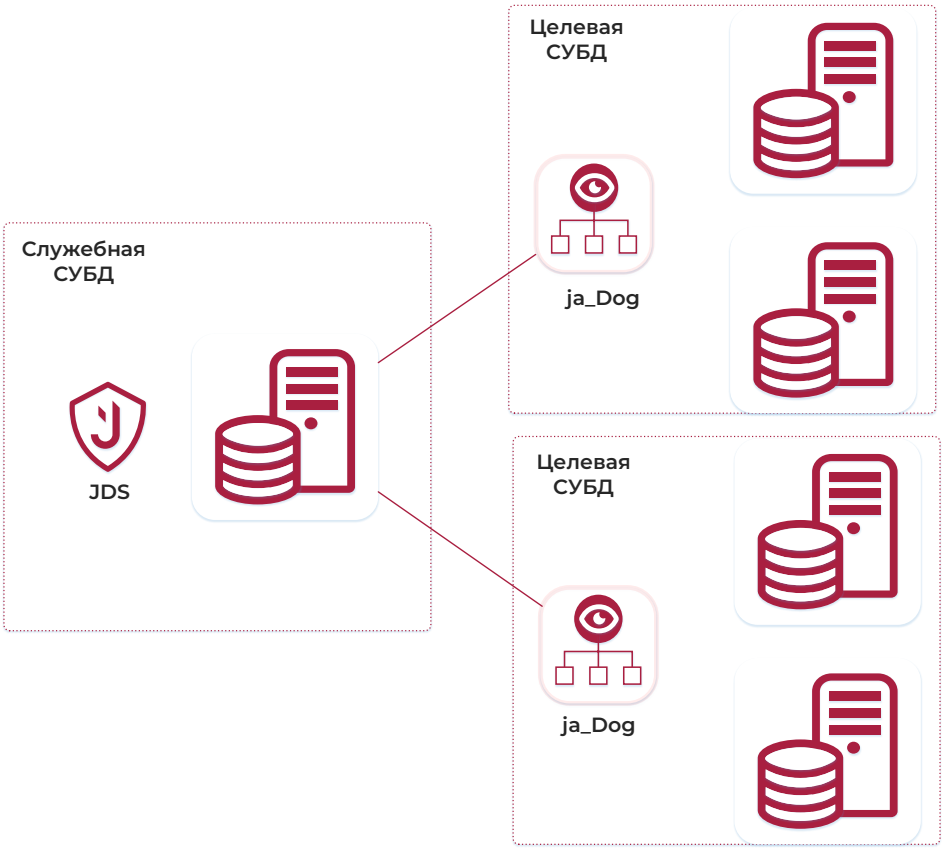

Рисунок 1.1 – Схема работы компонента при клиент-серверном варианте

При локальной установке на сервере СУБД станет для компонента основной.

В каждом из вариантов использования компонент JDS использует служебную БД «jdsdb».

Схема работы компонента при локальной установке представлена на рисунке 1.2.

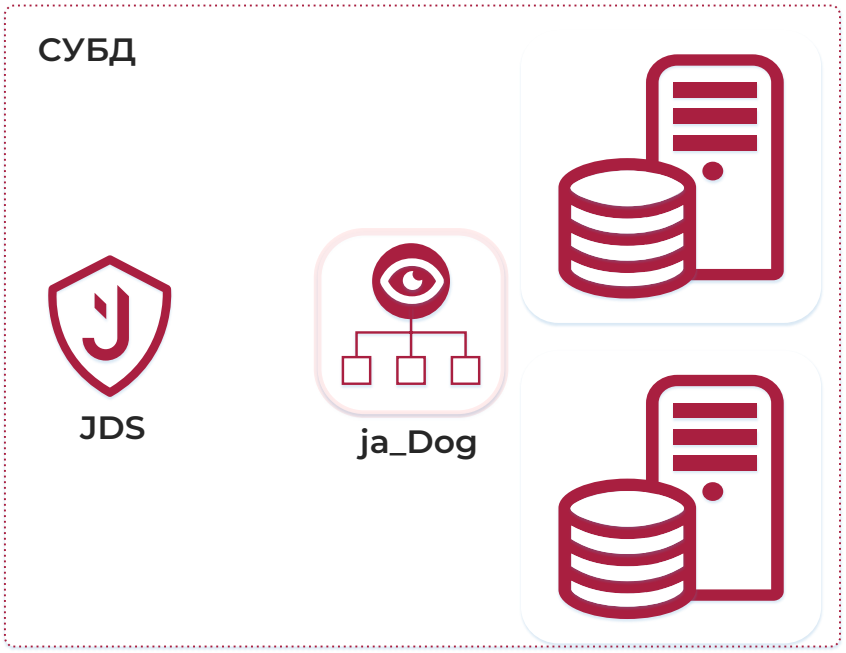

Рисунок 1.2 – Схема работы компонента при локальной установке

Функциональная возможность по сбору событий безопасности с компонентом «ja_Log» и просмотру в разделе JDS «Event List» подразумевает хранение их в служебной БД «ja_log». В клиент-серверной установке выбирается менее нагруженная СУБД с достаточным размером дискового пространства. При локальной установке должна учитываться дополнительная нагрузка на СУБД при сборе событий безопасности и размер свободного дискового пространства.

Использование компонента JDS в локальной установке допустимо, но не является желательной.

Рекомендуется использовать распределенную структура, когда у компонента JDS есть своя служебная СУБД «Jatoba», т.е. клиент-серверный вариант, как описано выше.

1.3. Требования к среде функционирования

Компонент JDS в составе СУБД «Jatoba» поставляется в составе сертифицированной и коммерческой версии.

Сертифицированная версия СУБД «Jatoba» может использоваться в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в

информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса, для которых должна использоваться сертифицированная ОС.

Компонент JDS функционирует под управлением ОС, указанных в таблице 1.1.

Таблица 1.1 – 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 1.7 Special Edition Смоленск (x86-64)	X	X	20.10.2	2557	30.01.2012
7	Astra Linux 1.8 (x86-64)	X	X	—	—	—
8	Astra Linux 2.12 Common Edition Орел (x86-64)	X	X	—	—	—
9	Debian 11	X	X	24.0.2	—	—
10	Debian 12	X	X	24.0.2	—	—
11	Альт 8 СП	X	X	20.10.11	3866	10.08.2018
12	Альт 10 СП	X	X	20.10.11	3866	10.08.2018
13	Альт 9.1 Server	X	X	—	—	—
14	Альт 10 Server	X	X	23.0.1	—	—
15	Ubuntu 20.04	X	X	24.0.2	—	—
16	Ubuntu 22.04	X	X	24.0.2	—	—
17	Ubuntu 24.04	X	X	24.0.2	—	—
18	ОСНОВА2	X	X	25.05	4381	31.03.2021
19	РЕД ОС 7.3 Муром	X	X	20.10.1	4060	12.01.2019
20	РЕД ОС 8	X	X	—	—	—
21	РОСА 12.4	X	X	—	—	—
22	Oracle Linux 8.4	X	X	—	—	—

Компонент JDS СУБД «Jatoba» устанавливается на ЭВМ с процессорами, имеющими архитектуру x86, x86-64 и AMD64, удовлетворяющие следующим аппаратным требованиям, указанным в таблице 1.2.

Таблица 1.2 – Аппаратные требования к ЭВМ, на которых фукционируют клиентская и серверная части СУБД

Параметр	Характеристика	Сертифицированная ОС
Требования к аппаратному обеспечению сервера JDS		
ОЗУ	Не менее 2 Гб	

Параметр	Характеристика	Сертифицированная ОС
Свободный объем жесткого диска	Минимальный объем от 40 Гб Рекомендуемый объем от 100 Гб	
Устройства видео вывода	Монитор и видеоадаптер с поддержкой HD и Full HD	
Тип процессора и минимальная тактовая частота процессора	64-разрядный процессор Intel или AMD 3 ГГц или больше	
Минимальное количество ядер	4	
Устройства ввода-вывода	Стандартные 105-клавишная клавиатура и манипулятор «мышь» с USB, либо PS/2 интерфейсами	
Адаптер Ethernet	100 Мбит/с	
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 браузер	• Google Chrome;	X
	• Яндекс.Браузер;	X
	• Chromium;	X
	• Opera;	X
	• Mozilla Firefox;	X
	• Microsoft Edge	—

При использовании функциональной возможности по централизованному сбору событий безопасности с целевых СУБД в служебную СУБД JDS рекомендуется использовать дополнительное дисковое пространство.

1.4. Компоненты, используемые для работы JDS

Корректная работа компонента JDS гарантируется с компонентами, входящими в поставку Изделия, и версии которых не ниже приведенных таблице 1.3.

Таблица 1.3 – Версии компонент совместимых с JDS

Разделы JDS	Используемые компоненты	Версия ядра/компонента
Мониторинг	node_exporter	1.8.0-2159
	postgres_exporter	0.18.1
	sql_exporter	0.18.6
	Prometheus	3.5.0
	alertmanager	0.27.0-3083
Анализ рисков (User Risk)	—	—
Кластеры (Clusters)	ja_Dog	4.1
Аудит и отчетность		
События безопасности (Event List)	ja_Log	2.1
Матрица доступа (Access Matrix)	—	X
Производительность		
Снимки и отчеты (Snapshots & Reports)	pg_Profile	4.2
Проблемы и решения (Problems & Solutions)	—	X
Анализ запросов	pg-explain	1.6.2
	pg-explain-db	1.6.0
	pg-monitor	1.6.5
	pg-monitor-collector	1.6.5
	pg-monitor-dispatcher	1.6.5
Активность БД	—	X
Подключения JDS	—	X
LDAP синхронизация (LDAP Sync)	ja_Sync_Ldap	1.3.2
	JDV	1.5.0
	securityprofile	2.4
Ландшафт	—	X
Роли БД	securityprofile	2.4
	JDV	1.5.0
Уведомления (Notifications)	ja_Log	1.1
Парольные политики	securityprofile	2.4
	ja_CSum	1.1
Резервное копирование	pg_ProBackup	2.5.15

Сопоставление разделов JDS и компонентов целевой СУБД, обеспечивающих их функционирование, представлено на рисунке 1.3.

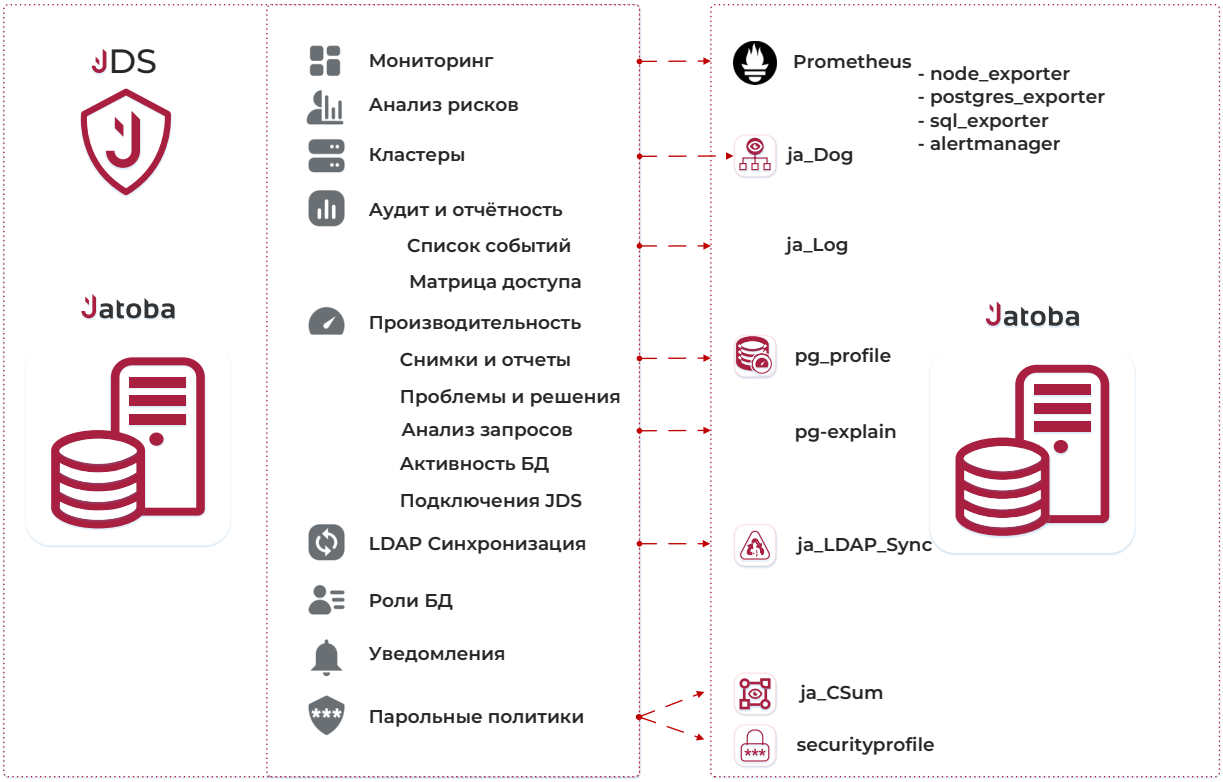

Рисунок 1.3 – Компоненты целевой СУБД, требуемые для работы разделов JDS

1.5. Разделы JDS совместимые с СУБД PostgreSQL

Данный пункт не содержит в себе конкретных инструкций по развертыванию сторонних компонент совместимых с JDS

Функциональные возможности «Jatoba data safe» позволяют проводить мониторинг и администрирование инсталляции СУБД под управлением GNU/Linux:

— СУБД «Jatoba»;

— СУБД PostgreSQL.

В качестве служебной СУБД компонент «Jatoba data safe» может использовать любую из вышеперечисленных СУБД. Для установки должен использоваться инсталляционный скрипт install.sh, как описано в документе «Руководство по установке». Скрипт обнаружит подходящую СУБД, создаст служебную БД и пользователя.

Доступность разделов JDS при мониторинге СУБД PostgreSQL и используемые компоненты приведены в таблице 1.4.

Таблица 1.4 – Доступные разделы JDS при мониторинге СУБД PostgreSQL и используемые при этом компоненты

Разделы JDS	**Доступность раздела при мониторинге PostgreSQL**	**JDS 2.10**	**Используемые компоненты PostgreSQL**	**Используемые компоненты Jatoba**
Мониторинг	X	X	node_exporter	Jatoba<ver>-node-exporter
			postgres_exporter	jatoba<ver>-postgres-exporter
			sql_exporter	jatoba<ver>-sql-exporter
			prometheus	jatoba<ver>-prometheus
			alertmanager	jatoba<ver>-alertmanager
Анализ рисков (User Risk)	X	X	Не требует установки компонент	Не требует установки компонент
Кластеры (Clusters)	—	X	—	Не применим jatoba<ver>-jadog
Аудит и отчетность				
События безопасности (Event List)	—	X	—	Не применим jatoba<ver>-ja-log
Матрица доступа (Access Matrix)	X	X	Не требует установки компонент	Не требует установки компонент
Производительность				
Снимки и отчеты (Snapshots & Reports)	X	X	pg_Profile	Не применим jatoba<ver>-pg-profile
Проблемы и решения (Problems & Solutions)	X	X	Не требует установки компонент	Не требует установки компонент
Анализ запросов	X	X	auto_explain	auto_explain,
			pgaudit	Не применим jatoba<ver>-pgaudit
			pg-repack	Не применим jatoba<ver>-pg-repack
			pg-explain	Не применим pg-explain
			pg-explain-db	Не применим pg-explain-db
			pg-monitor	Не применим pg-monitor
			pg-monitor-collector	Не применим pg-monitor-collector
			pg-monitor-dispatcher	Не применим pg-monitor-dispatcher
Активность БД	X	X	Не требует установки компонент	Не требует установки компонент
Подключения JDS	X	X	Не требует установки компонент	Не требует установки компонент
LDAP синхронизация	—	X	—	Не применим jatoba<ver>-ja-sync-ldap

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

Разделы JDS	Доступность раздела при мониторинге PostgreSQL	JDS 2.10	Используемые компоненты PostgreSQL	Используемые компоненты Jatoba
(LDAP Sync)				
Роли БД	X	X	Не требует установки компонент	Не требует установки компонент
Уведомления (Notifications)	—	X	—	Набор компонентов не применим
Парольные политики	—	X	—	Не применим jatoba<ver>-securityprofile

Примечание:

X – Знак обозначает доступность раздел компонента JDS.

— – Знак обозначает недоступность раздела компонента JDS или отсутствие пакета (компонента) для СУБД PostgreSQL.

Пакеты компонентов могут быть использованы, как из репозитория СУБД «Jatoba», так и из репозитория сторонних разработчиков. Использование репозитория СУБД «Jatoba» полностью не представляется возможным, т.к. компоненты разрабатывались специально для нее.

Доступность разделов, приведенных в таблице 1.4, схематично отражена на рисунке 1.4.

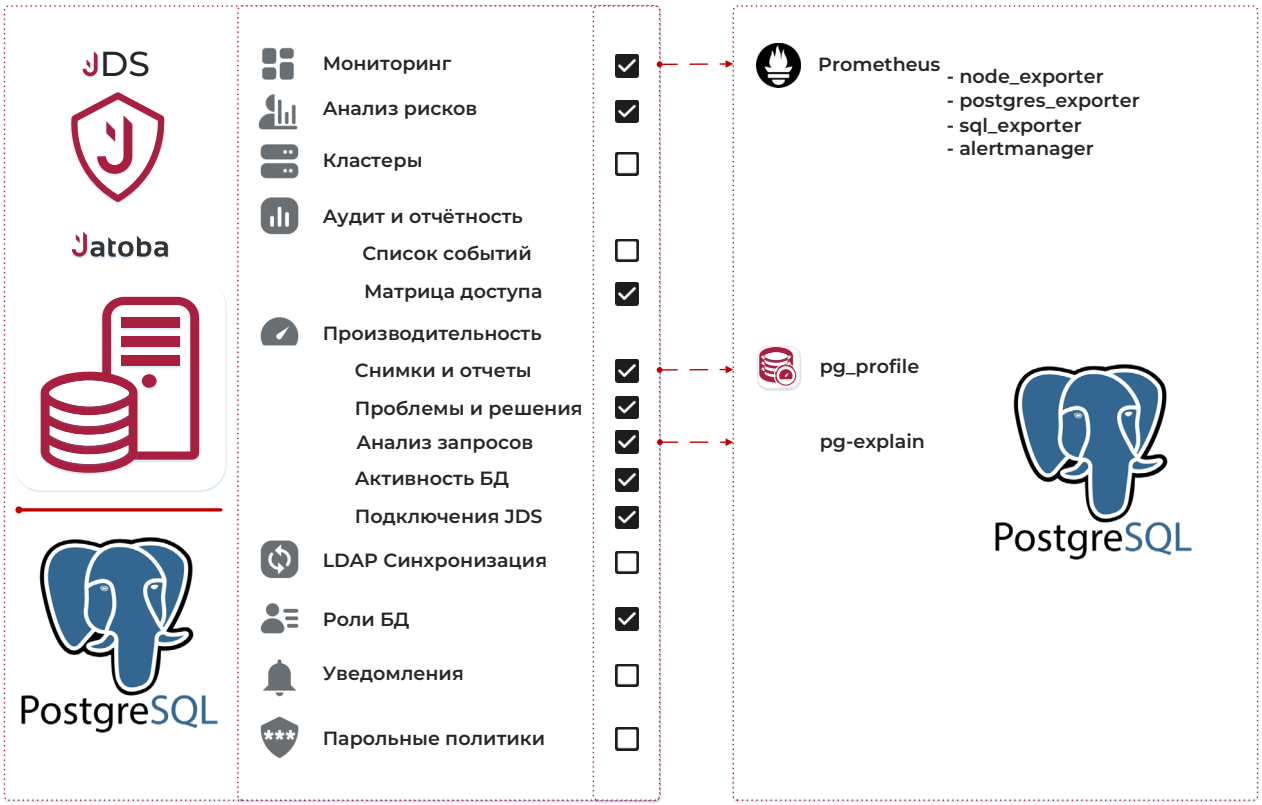

Рисунок 1.4 – Перечень разделов JDS, доступных для работы с СУБД PostgreSQL

Разделы «Анализ рисков», «Матрица доступа», «Активность БД», «Подключения JDS» и «Роли БД» используют SQL-запросы к БД и поэтому не требуют установки дополнительных компонент.

Как было сказано выше, для раздела «Мониторинг» могут использоваться компоненты как из репозитория СУБД «Jatoba», так и из репозитория сторонних разработчиков. Функциональные возможности раздела описаны в разделе 3 настоящего документа. Установка и настройка компонент описана в документе «Руководство по настройке. Часть 28. Поддержка мониторинга СУБД».

Раздел «Анализ запросов» будет доступен при использовании компонент сторонних разработчиков.

2. УСТАНОВКА И НАСТРОЙКА

Установка компонента «Jatoba Data Safe» полностью описана в документе «Защищенная система управления базами данных «Jatoba». Руководство по установке» в одноименном разделе.

Установка компонента происходит в два этапа:

1) создание служебной БД на базе СУБД (БД) «Jatoba»;

2) установка компонента JDS (см. документ «Руководстве по установке»).

СУБД «Jatoba» должна быть установлена в первую очередь.

Для служебной БД JDS обязательно должен быть установлен параметр:

```
standard_conforming_strings=on
```

Параметр устанавливается автоматически при установке.

Служебная БД будет хранить список целей (target), учетные записи пользователей, технических учетных записей и обеспечивать меры безопасности.

Установка и настройка служебной СУБД описана в документах:

- «Защищенная система управления базами данных «Jatoba». Руководство по установке. 643.72410666.00067-07 95 01»;
- «Защищенная система управления базами данных «Jatoba». Руководство администратора. 643.72410666.00067-07 97 01».

В качестве метода аутентификации должен использоваться метод «password».

2.1. Аутентификация пользователей JDS

Реализована двухкомпонентная ролевая модель.

Первым компонентом выступает ролевая модель JDS, в которую включена доступность разделов.

Вторым компонентом ролевой модели является набор ролей в целевых СУБД, которым предоставлены необходимые права и привилегии при инициализации компонент и расширений СУБД.

При использовании ролевой модели пользователь JDS не будет знать учетную запись для доступа к инсталляции СУБД, что обеспечивает безопасный доступ к конфиденциальным данным.

Для безотказной работы JDS на стороне СУБД должны быть сформированы и поддерживаться в актуальном состоянии ассоциированные роли. Поскольку при настройке компонента:

— будет создана УЗ компонента;

— УЗ компонента связана с доступными целевыми СУБД (Tagret);

— УЗ компонента ассоциируется с ролью в целевой СУБД (Tagret).

Каждая инсталляция СУБД является целью «Target».

Первоначально JDS будет устанавливать соединение с СУБД и БД по умолчанию, а при выборе Target JDS переустановит соединение.

2.1.1. Ролевая модель JDS

Компонент JDS для доступа разделам использует встроенную ролевую модель. В ролевой модели предустановлены:

— Администратор СУБД - обеспечивающий эффективное функционирование, безопасность, резервное копирование и оптимизации работы СУБД;

— Аудитор - выполняющий внутренний или внешний комплексный аудит систем ИБ, в том числе СУБД;

— Администратор ИБ - обеспечивающий защиту информации в автоматизированных ИС, контроль доступа, мониторинг и расследование инцидентов.

— Разработчик БД – выполняющий разработку программного кода для манипулирования данными в БД, оптимизации работы БД в автоматизированных ИС.

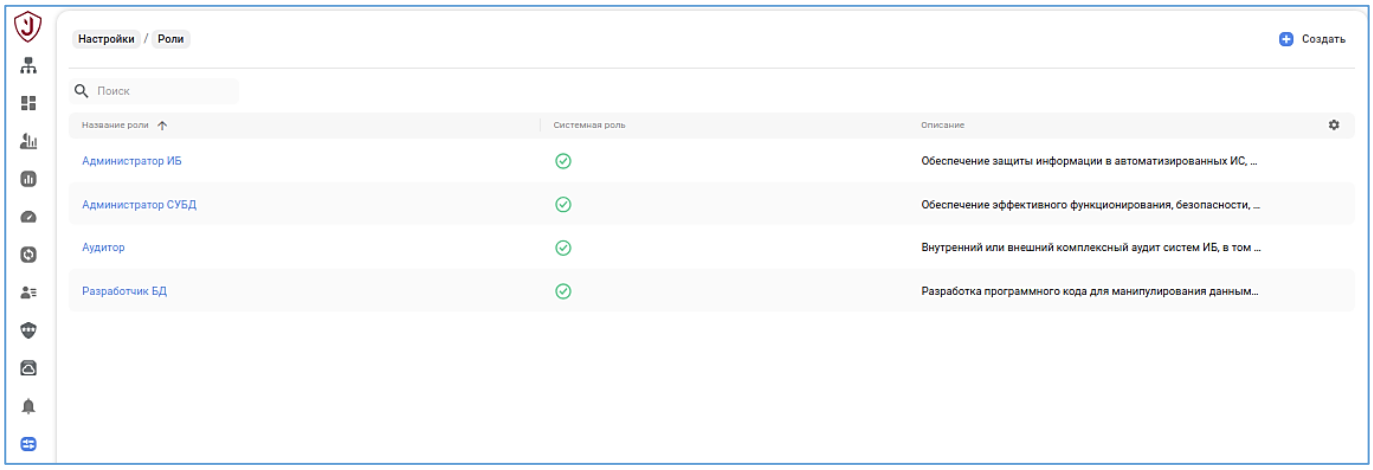

Рисунок 2.1 – Роли JDS

Для каждой роли назначены не изменяемые права доступа к разделам компонента описанные в таблице 2.1.

Таблица 2.1 – Назначенные права

Раздел	**Подраздел**	**Роль**			
		Администратор СУБД	**Аудитор**	**Администратор ИБ**	**Разработчик БД**
Меню JDS	Ландшафт (СУБД)	Управление	Просмотр	Просмотр	Просмотр
	Ландшафт (Кластеры jaDog)	Управление	Нет доступа	Нет доступа	Нет доступа
	Мониторинг	Управление	Управление	Управление	Управление
	Анализ запросов	Управление	Нет доступа	Нет доступа	Управление
	Подключения JDS	Управление	Нет доступа	Управление	Нет доступа
	Резервное копирование	Управление	Просмотр	Просмотр	Нет доступа
	Снимки и отчеты	Управление	Нет доступа	Управление	Управление
	Уведомления	Управление	Нет доступа	Управление	Нет доступа
	Настройки	Управление	Нет доступа	Нет доступа	Нет доступа
Меню СУБД	Обзор	Управление	Просмотр	Просмотр	Просмотр
	Назначение ролей	Управление	Нет доступа	Нет доступа	Нет доступа
	Параметры СУБД	Управление	Просмотр	Просмотр	Нет доступа
	Правила доступа	Управление	Просмотр	Просмотр	Нет доступа
	Доступные расширения	Управление	Нет доступа	Нет доступа	Нет доступа
	Настройки для probackup	Управление	Нет доступа	Нет доступа	Нет доступа
	Роли СУБД	Управление	Нет доступа	Управление	Нет доступа
	Список событий	Управление	Управление	Управление	Нет доступа
	Проблемы и решения	Управление	Нет доступа	Нет доступа	Нет доступа
	Активность БД	Управление	Нет доступа	Управление	Нет доступа
	LDAP синхронизация	Управление	Нет доступа	Нет доступа	Нет доступа
	Парольные политики	Управление	Просмотр	Управление	Нет доступа
Меню БД	Обзор	Управление	Просмотр	Просмотр	Просмотр
	Расширения	Управление	Нет доступа	Нет доступа	Нет доступа
	Анализ рисков	Управление	Управление	Управление	Нет доступа
	Матрица доступа	Управление	Управление	Управление	Нет доступа

Предустановленные роли имеют атрибут «системные».

Дополнительно возможно создать специализированные роли, для которых назначить особый набор прав доступа к каждому из подразделов. Набор прав варьируется в зависимости от функциональной возможности их назначения. Если такая возможность отсутствует, то название во вкладке помечено серым цветом.

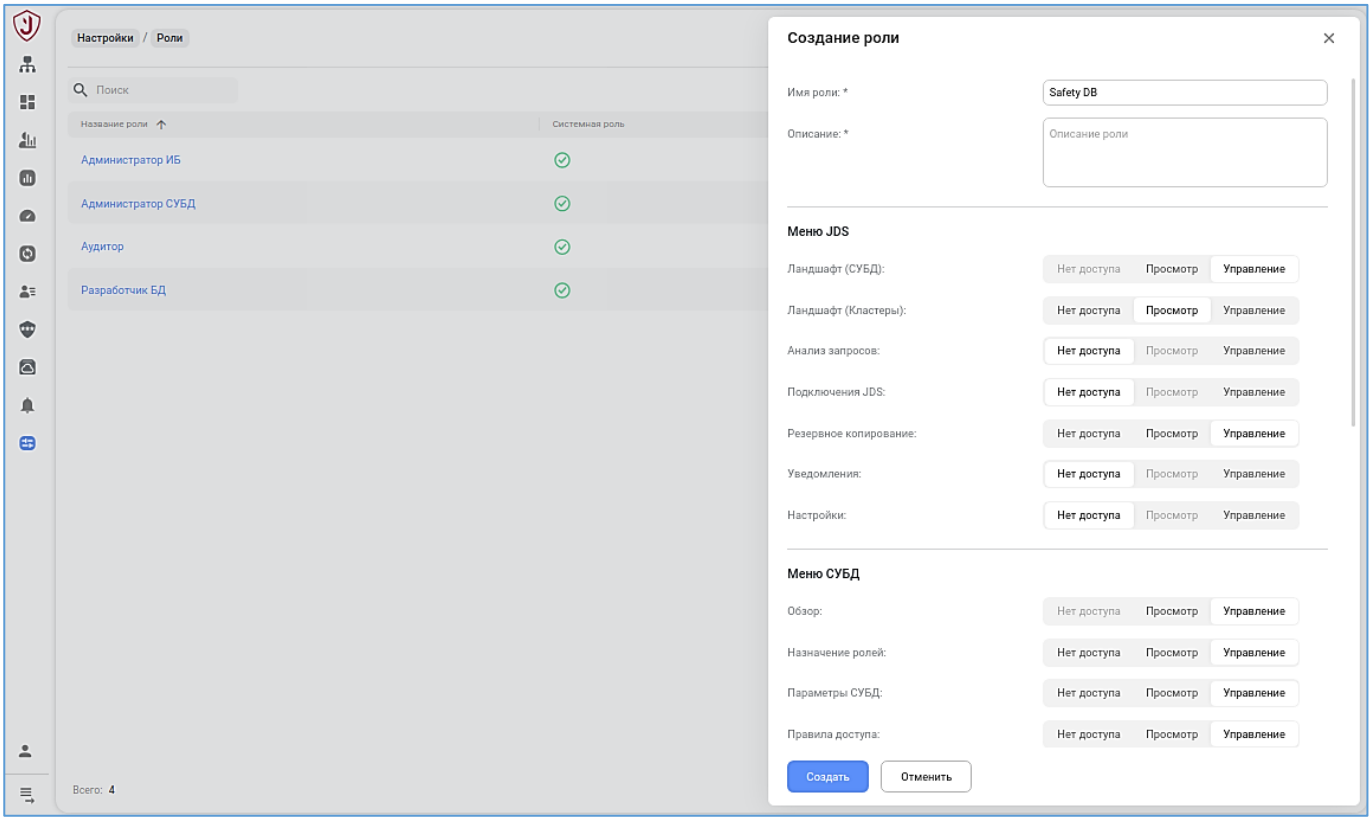

Рисунок 2.2 – Создание специализированной роли

Назначенные права доступа для роли возможно:

- просмотреть при нажатии на гиперссылку роли в модальном окне
- изменить через контекстное меню в строке роли.

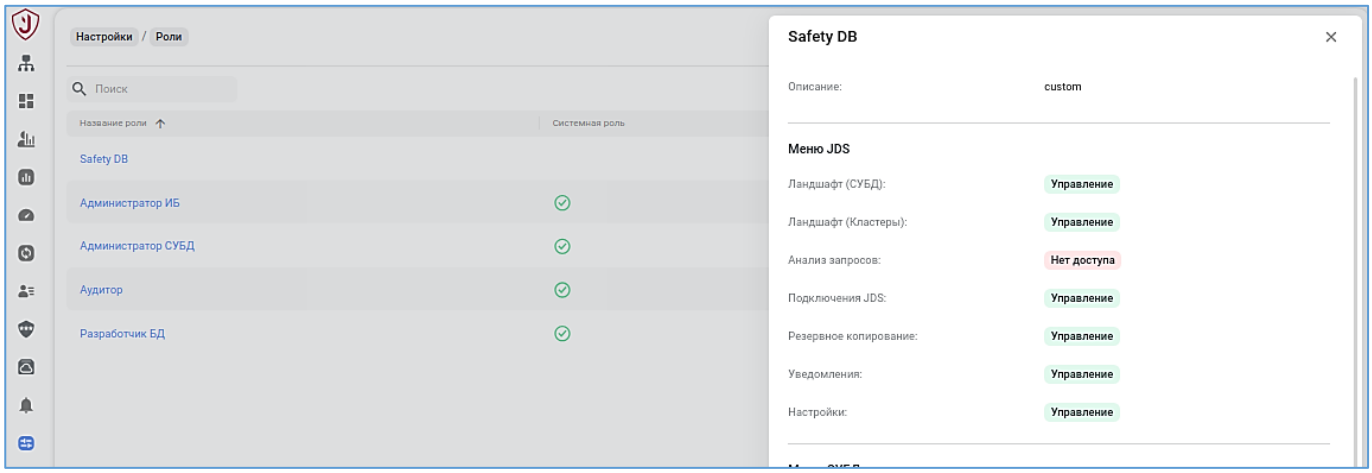

Рисунок 2.3 – Окно просмотра назначенных прав доступа

2.1.2. Модель ролевой консолидации JDS и целевой СУБД

В модели ролевой консолидации пользователь JDS получив доступ к разделам дальнейшие действия в целевой СУБД выполняет от имени и с правами привилегированного пользователя.

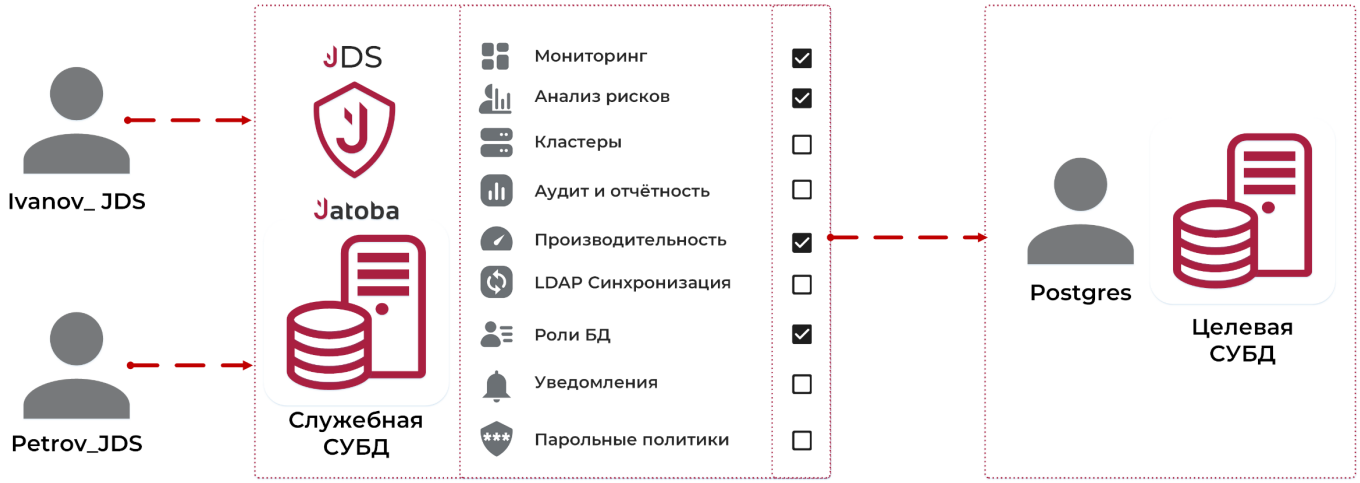

Рисунок 2.4 - Модель ролевой консолидации

При этом действия каждого пользователя регистрируются в журнале событий компонента.

2.1.3. Создание пользователей JDS

Создание пользователей возможно от имени и с правами администратора компонента JDS и доступно на вкладке «Пользователи» раздела «Настройки». Если подключения к целевым СУБД «Target» были созданы ранее, то по умолчанию они будут доступны пользователю с ролью «Администратор» и находится в списке.

Вызов окна создания пользователей компонента JDS доступно через пиктограмму «Add», как представлено на рисунке 2.5.

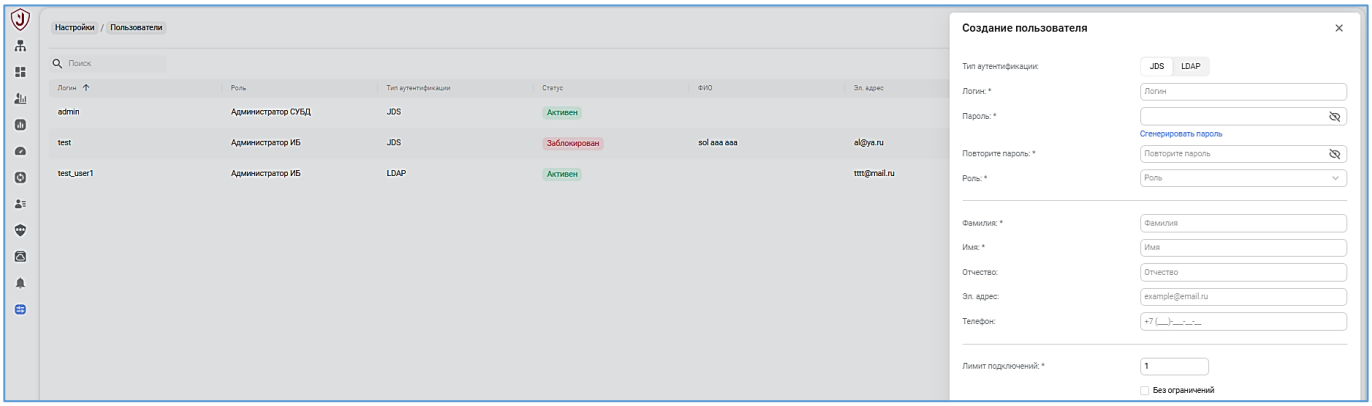

Рисунок 2.5 – Вкладка «Пользователи» («Users»)

В открывшимся окне потребуется установить параметры, приведенные в таблице 2.2

Таблица 2.2 – Параметры создания пользователя

№	Параметр	Параметр (ENG)	Обязательность параметра	Тип поля
1	Логин	Username	Обязательный	Текстовое
2	Пароль	Password	Обязательный	Текстовое
3	Повторить пароль	Repeat password	Обязательный	Текстовое
4	Роль	Role	Обязательный	Выпадающий список
5	Фамилия	Last name	Обязательный	Текстовое
6	Имя	First name	Обязательный	Текстовое
7	Отчество	Middle name	Необязательный	Текстовое
8	Эл. адрес	E-mail	Необязательный	Текстовое
9	Телефон	Phone	Необязательный	Текстовое
10	Лимит подключений	Connection limit	Обязательный	Текстовое

При успешном создании пользователя, его учетная запись появится в списке пользователей JDS.

Далее станут доступны операции по корректировке учетной записи пользователя через контекстное меню:

— Сменить пароль (Change password);

— Редактировать;

— Удалить (Delete).

2.1.4. Подключения LDAP

JDS поддерживается подключение пользователя компонента из активных каталогов, таких как: Active Directory, FreeIPA, ALD Pro и Samba используя отдельную группу пользователей LDAP.

Во избежание проблем с подключением, рекомендуется в дереве каталогов LDAP проводить преднастройку - создание отдельной группы пользователей LDAP, для упрощения подключения и добавления пользователей, например ограничивать базы поиска до "ou=users, dc=da, dc=lan" (ActiveDirectory/SAMBA) или до определенной группы (cn=my_group, dc=da, dc=lan) для FreeIPA и ALDPro.
Примеры создания групп пользователей приведены в документе «Руководство по настройке. Часть 8. Синхронизация учетных записей служб каталогов и СУБД. Компонент «ja_Sync_LDAP».

В рассматриваемом примере будет использоваться база поиска до "ou=users, dc=da, dc=lan".

Перед настройкой подключения, если требуется подключение по доменному имени, на хосте с JDS пропивается подключение к активному каталогу командой:

```
nano /etc/hosts
```

Внести IP-адрес и имя активного каталога.

Например

```
10.116.101.114 dc.domain.test
```

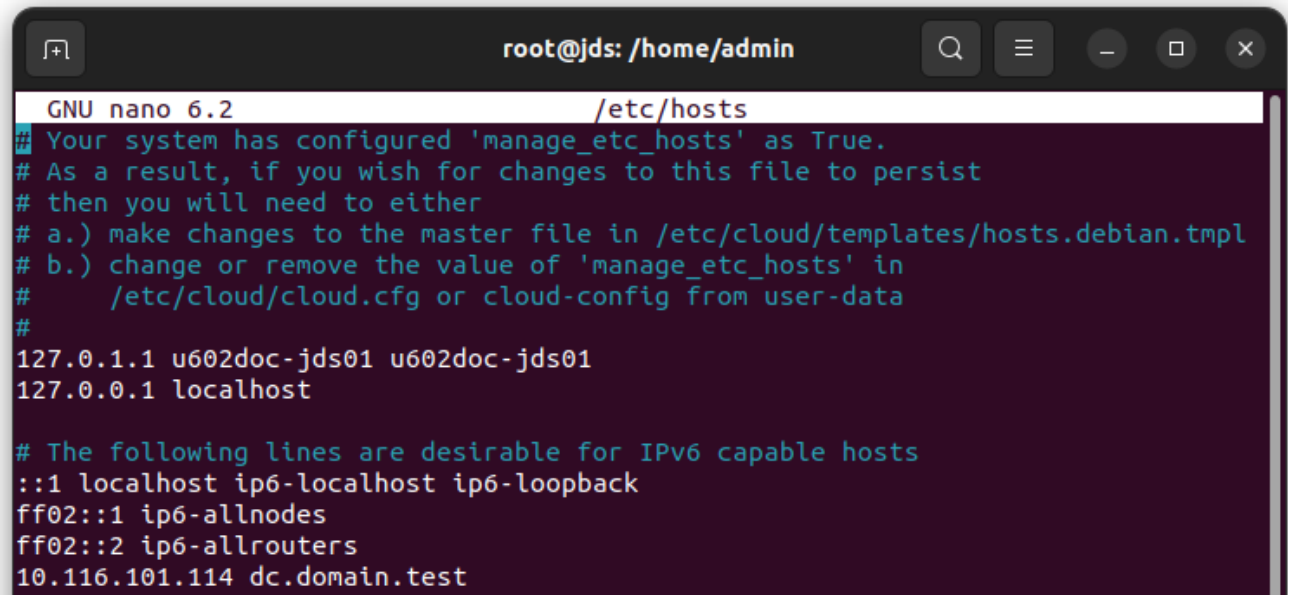

Рисунок 2.6 – Редактирование конфигурационного файла подключений

Вкладка «Подключения LDAP» находится в разделе «Настройки».

Создание подключения к активному каталогу выполняется нажатием кнопки «Добавить подключение», которое вызовет окно «Создание подключения».

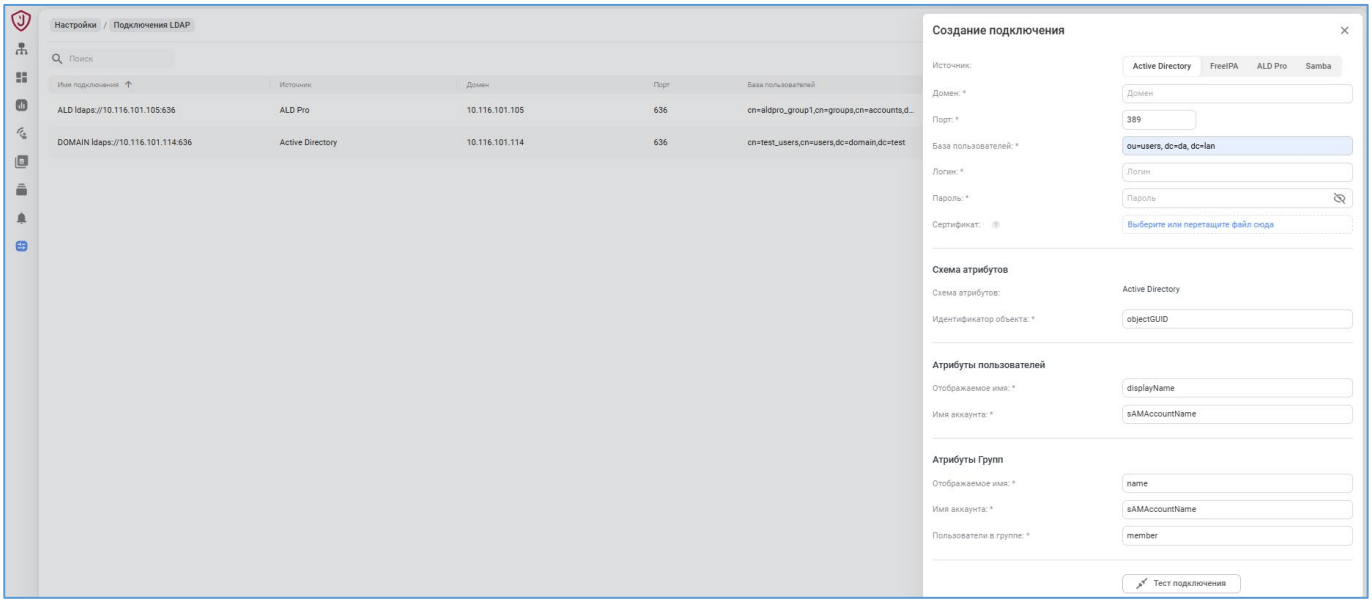

Рисунок 2.7 - Окно «Новое подключение»

Устанавливаются следующие параметры:

— Источник: тип ОС активного каталога Active Directory, FreeIPA, ALD Pro или Samba

— Домен: * - IP-адрес или DNS имя хоста активного каталога;

— Порт: * - порт подключения;

— База пользователей: * - база поиска активного каталога, в которой может использоваться организационная группа (ou) и/или группа (cn);

— Логин: * - имя пользователя, имеющего административные привилегии;

— Пароль: * - пароль пользователя;

— Сертификат: - сертификат в формате *.pfx.

Схема атрибутов

— Схема атрибутов: - схема устройства каталога LDAP того или иного типа. Устанавливается автоматически в зависимости от выбранного типа активного каталога

— Идентификатор объекта: * - атрибут, значение которого является уникальным идентификатором объекта в дереве структуры каталогов LDAP.

Атрибуты пользователей

— Отображаемое имя: * - атрибут, значение которого используется для отображения записи пользователя в дереве структуры каталогов LDAP.

— Имя аккаунта: * - атрибут, значение которого содержит имя пользователя, под которым он входит в систему и проходит аутентификацию.

Атрибуты Групп

— Отображаемое имя: * - атрибут группы, значение которого используется для отображения записи группы в дереве структуры каталогов LDAP;

— Имя аккаунта: *- атрибут группы, значение которого содержит имя, под которым она зарегистрирована в дереве каталогов LDAP.;

— Пользователи в группе: * - атрибут группы, значение которого содержит информацию о пользователях, состоящих в этой группе.

Созданное подключение отразится в общем списке подключений.

2.1.4.1 Создание пользователя JDS с LDAP аутентификацией

Пользователь JDS с LDAP аутентификацией создаётся во вкладке «Пользователи» раздела «Настройки». В окне «Создание пользователя» выбирается Вкладка «LDAP» и из выпадающих списков устанавливаются параметры:

— Домен-сервер: * - сервер активного каталога;

— Пользователь * - пользователь активного каталога;

— Роль: * - назначаемая роль пользователю в JDS;

Дополнительно устанавливается «Лимит подключений».

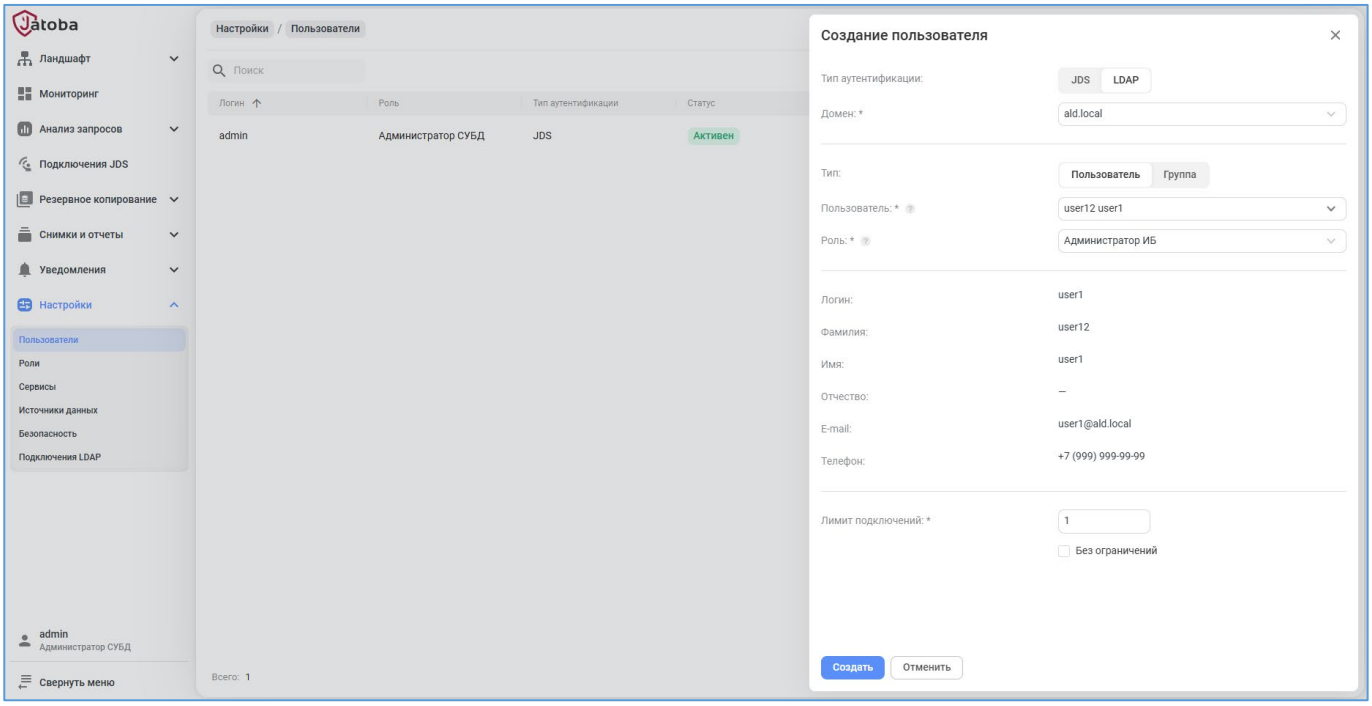

Рисунок 2.8 – Окно создание пользователя JDS с LDAP аутентификацией

Остальные данные пользователя будут загружены автоматически.

2.1.4.2 Создание пользователей JDS из группы с LDAP аутентификацией

Пользователей JDS из группы активного каталога с LDAP аутентификацией создаётся во вкладке «Пользователи» раздела «Настройки».

В окне «Создание пользователя» выбирается вкладка «LDAP» и «Группа». Из выпадающих списков устанавливаются параметры:

— Домен-сервер: * - сервер активного каталога;

— Группа * - группа активного каталога;

— Роль: * - назначаемая роль группе пользователей в JDS;

Автоматически загрузятся данные о группе, количестве пользователей и выведет список пользователей.

Выбор пользователей из группы недоступен.

Дополнительно устанавливается «Лимит подключений».

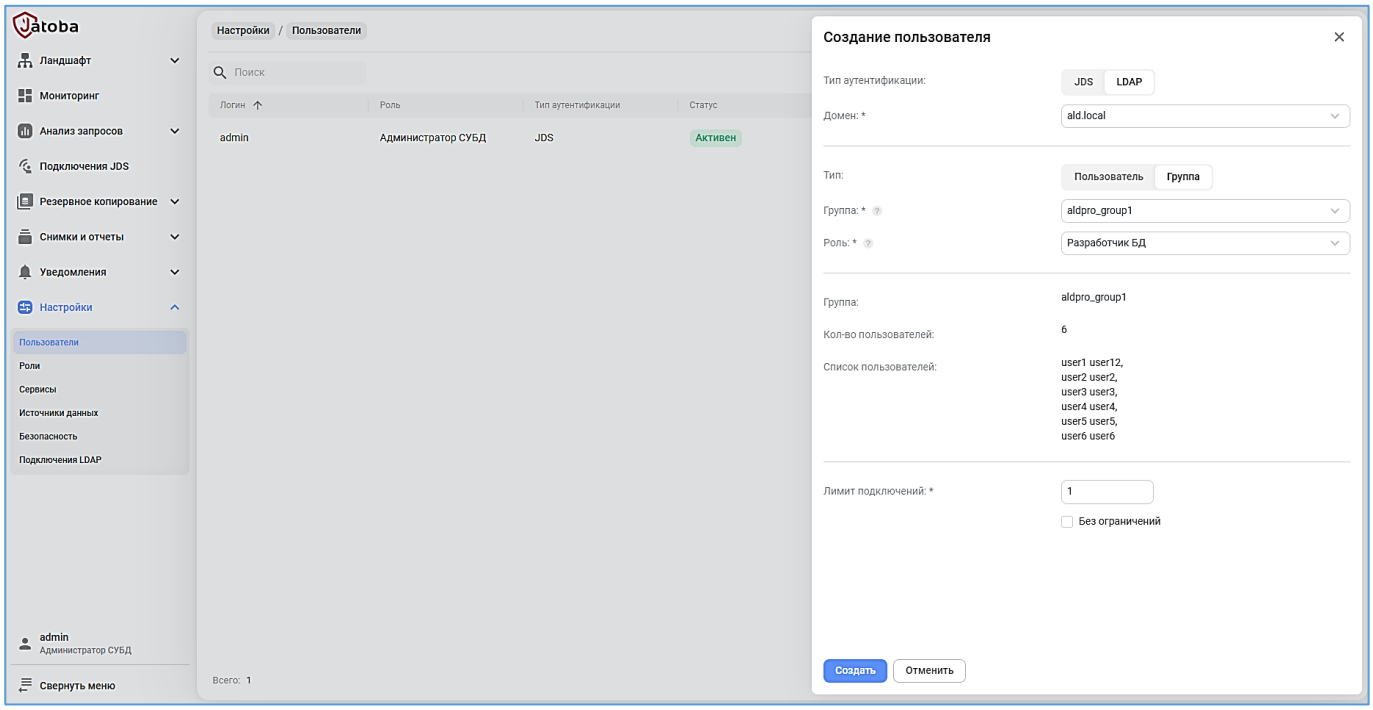

Рисунок 2.9 – Создание группы пользователей с LDAP аутентификацией

После нажатия кнопки «Создать» выполнится синхронизация с группой активного каталога.

В последствии если один или несколько пользователей будут удалены из пользователей JDS, то при повторном создании пользователей JDS из той же группы будут выбраны для синхронизации отсутствующие в списке пользователей JDS пользователи активного каталога.

2.1.4.3 LDAP аутентификация пользователей JDS

На стартовой странице JDS для LDAP аутентификации пользователи должны выбрать вкладку «LDAP», сервер LDAP, ввести логин (имя пользователя) и пароль активного каталога.

Рисунок 2.10 – LDAP аутентификация

2.1.4.4 Обновление настроек LDAP аутентификации пользователей JDS с версии 2.9 на 2.10 JDS

В связи с расширением функциональности подключения и чтения LDAP каталогов в части работ с группами пользователей, при переходе с JDS версии 2.9 на 2.10 и выше, необходимо обеспечить обновление параметров подключения к LDAP серверам по набору параметров по умолчанию, а именно по схеме атрибутов "Active Directory".

Если подключение к LDAP серверу в версии JDS 2.9 было сделано к типу каталогов Active Directory (Microsoft), при миграции данных на версию JDS 2.10 и выше, никаких дополнительных действий по настройке подключения не требуется. В ином случае, администратору необходимо авторизоваться под локальной учетной записью JDS и в форме редактирования подключения указать нужный тип LDAP каталога - FreeIPA, ALDPro или Samba.

2.2. Вкладка «Безопасность». Парольная политика JDS

Парольная политика компонента JDS основана на требованиях, установленных Приказом ФСТЭК России от 11.02.2013 N 17, к мерам безопасности:

— ИАФ.4 «Идентификация и аутентификация пользователей, являющихся работниками оператора» и усилениям к мере ИАФ.4 (1г, 2);

— (УПД.6) «Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)»;

— Усиление УПД.1(3б) «автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования»:

б) более 45 дней.

Настройка парольной политики компонента доступна администратору компонента во вкладке «Безопасность» раздела «Настройки».

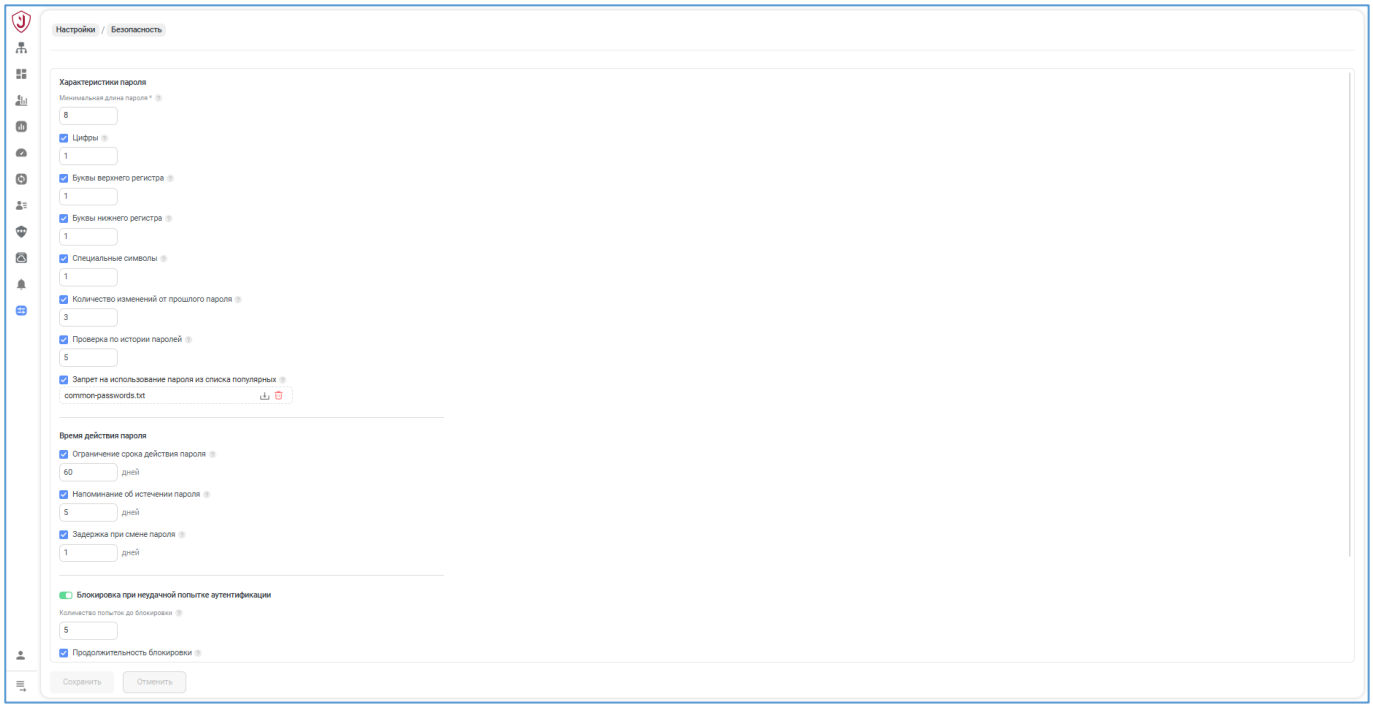

Рисунок 2.11 - Вкладка «Безопасность»

По умолчанию устанавливаются парольные политики, приведенные в таблице 2.3.

Таблица 2.3 – Парольные политики для пользователей JDS

№	Параметр	Описание параметра	Мин-е знач-е	Мак-е знач-е	Значение по умолчанию
1	Минимальная длина пароля	Минимальная допустимая длина пароля	6	255	8
2	Цифры	Обязательное использование цифр в пароле, в количестве не менее	1	255	1

№	Параметр	Описание параметра	Мин-е знач-е	Мак-е знач-е	Значение по умолчанию
3	Буквы нижнего регистра	Обязательное использование символов нижнего регистра в пароле, в количестве не менее	1	255	1
4	Буквы верхнего регистра	Обязательное использование символов верхнего регистра в пароле, в количестве не менее	1	255	1
5	Специальные символы	Обязательное использование специальных символов в пароле из набора \!"#$%&()*+,-./:;<=>?@[]^_'{|}~, в количестве не менее	1	255	1
6	Количество изменений от прошлого пароля	Минимальное количество изменений в новом пароле по сравнению со старым	1	255	3
7	Проверка по истории паролей	Количество последних использованных паролей, с которыми не должен совпадать задаваемый пароль	1	30	5
8	Запрет на использование пароля из списка популярных	Пароль не должен совпадать ни с одним из списка популярных паролей	0	1	1
9	Ограничение срока действия пароля	По истечении срока действия пароль должен быть сменен, дней	1	int_max	60
10	Напоминание об истечении пароля	При входе в систему напоминать пользователю о скором истечении срока действия пароля	1	int_max	5
11	Задержка при смене пароля	Минимальный срок действия пароля, срок до истечения которого пароль нельзя сменить, дней	1	int_max	1
12	Количество попыток до блокировки	После указанного количества неправильно введенного пароля учетная запись временно блокируется	1	int_max	5
13	Продолжительность блокировки	Продолжительность блокировки учетной записи	1	int_max	15
14	Блокировка учетной записи при отсутствии активности	Блокировать неиспользуемую учетную запись по истечении указанного периода	1	int_max	45

№	Параметр	Описание параметра	Мин-е знач-е	Мак-е знач-е	Значение по умолчанию
15	Блокировка администратора при длительном отсутствии	Применять правила блокировки неиспользуемых учетных записей для учетной записи по умолчанию «admin»	0	1	0

Внесённые изменения вступают в силу сразу после сохранения.

2.2.1. Смена пароля пользователя JDS администратором

Согласно установленной ролевой модели, встроенной учетной записи «admin» и пользователям с ролью «Администратор СУБД» доступна функциональная возможность смены пароля всем категориям пользователей JDS без ввода текущего пароля.

Смена пароля выполняется через контекстное меню в строке пользователя.

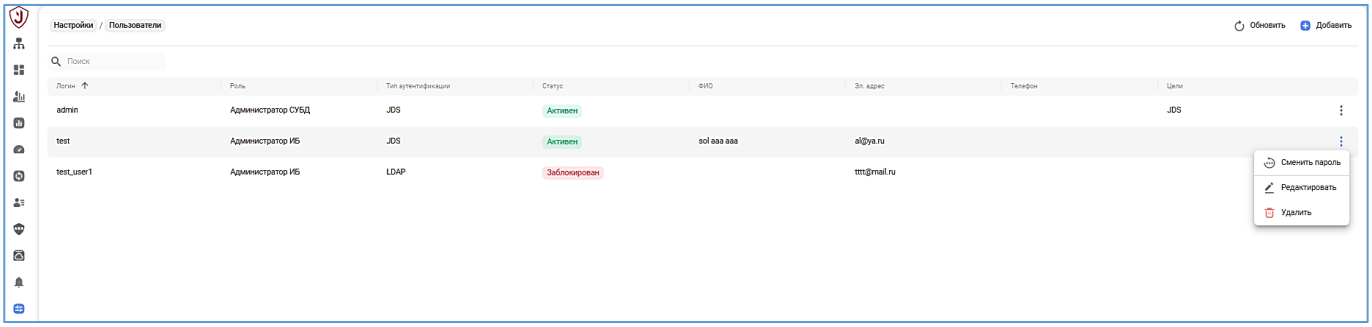

Рисунок 2.12 – Контекстное меню в строке пользователя JDS

При выборе опции «Сменить пароль» откроется окно «Смена пароля». Установите или сгенерируйте новый пароль и подтвердите его.

При вводе пароля будет отражаться подсказка по установленным требованиям к парольной политике, которые устанавливаются во вкладке «Безопасность».

Вводимая аутентификационная информация будет скрыта, что соответствует мере защиты информации (ИАФ.5) «Защита обратной связи при вводе аутентификационной информации», установленной Приказом ФСТЭК России от 11.02.2013 N 17.

Смена пароля пользователя через служебную БД компонента JDS невозможно.

2.2.2. Смена пароля пользователем JDS

Поле первичной идентификации, при первом входе в компонент, пользователь JDS обязан сменить присвоенный ему пароль. При этом, в целях безопасности, ему не будет доступна и известна аутентификационная информация для доступа к целевой СУБД.

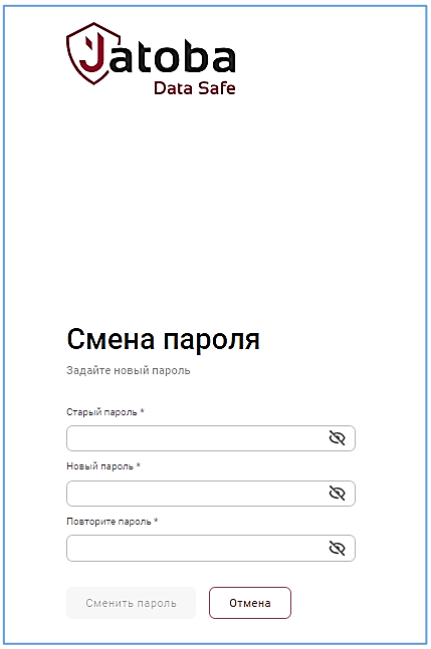

Рисунок 2.13 – Смена пользователем JDS выданного пароля при первом входе

Смена собственного пароля для всех пользователей компонента JDS доступна через пиктограмму текущего пользователя, расположенную в левом углу окна.

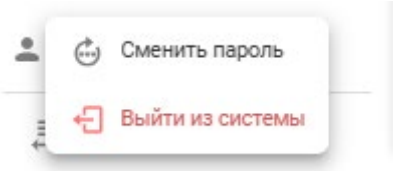

Рисунок 2.14 – Пиктограмма текущего пользователя

При истечении срока действия пароля пользователь будет периодически получать сообщение о смене пароля.

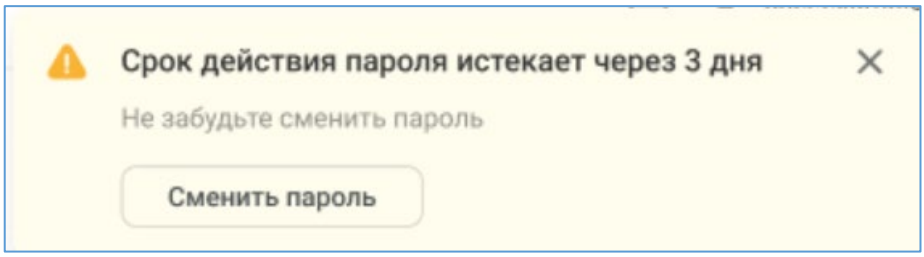

Рисунок 2.15 – Сообщение о смене пароля

2.2.3. Блокирование пользователя JDS администратором

Пользователь JDS, как с парольной, так и с LDAP аутентификацией, может быть заблокирован администратором принудительно. Такая блокировка выполняется в карточке пользователя через операцию «Редактировать» во вкладке «Пользователи» раздела «Настройки».

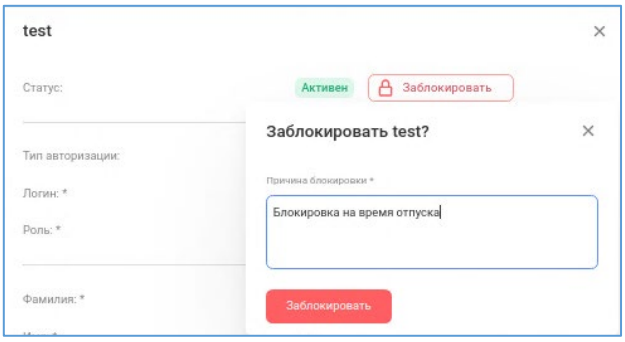

Рисунок 2.16 – Принудительное блокирование пользователя JDS

Ввод комментария является обязательным. Далее она будет отражаться в карточке пользователя.

2.2.4. Разблокирование пользователя JDS

Пользователь JDS может быть заблокирован:

— компонентом в следствии нарушения парольных политик;

— администратором компонента;

— администратором домена.

Статус пользователя отображается в одноименном столбце во вкладке «Пользователи» раздела «Настройки».

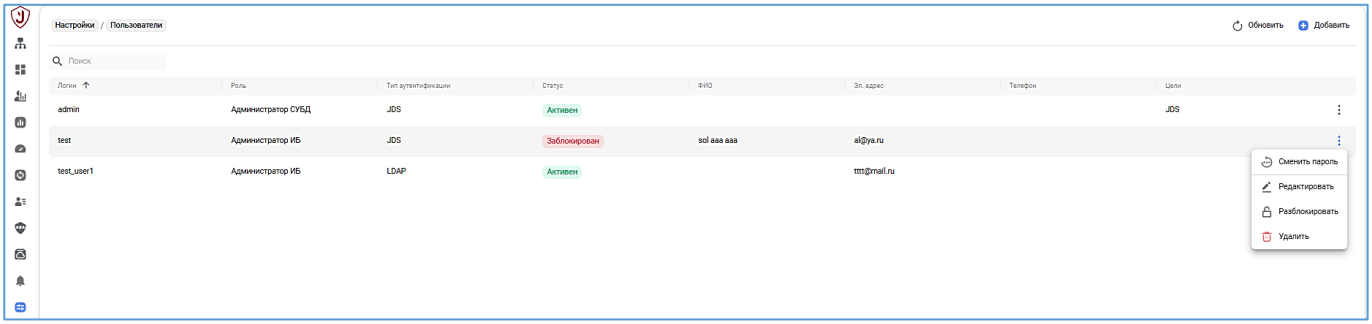

Рисунок 2.17 – Разблокировка пользователя JDS

Разблокирование пользователя JDS выполняется администратором компонента через контекстное меню.

Разблокировка LDAP - пользователя JDS недоступна, если он был заблокирован администратором домена.

2.3. Вкладка «Источники данных»

Вкладка «Источники данных» в разделе «Настройки» используется для раздела «Мониторинг», описанного в п. 3 настоящего документа.

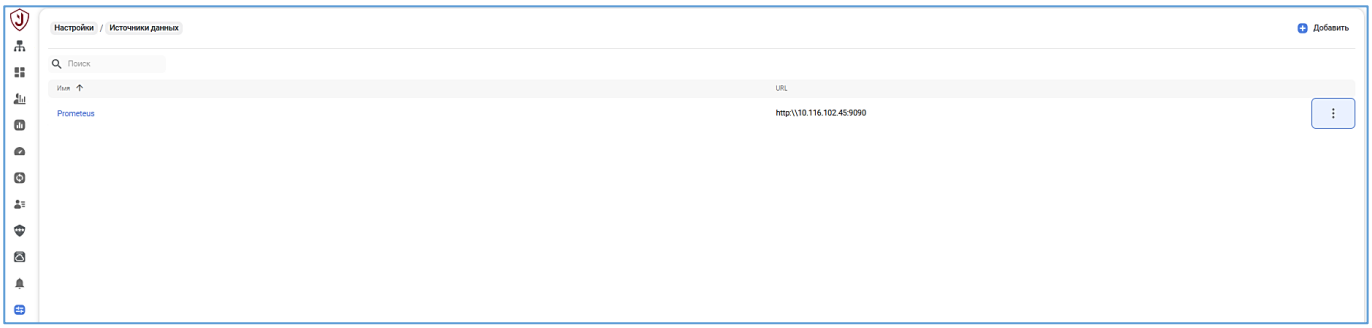

Рисунок 2.18 – Вкладка «Источники данных»

В качестве источника данных используется система «PROMETHEUS», для подключения к которой потребуется указать имя подключения и URL с используемым портом.

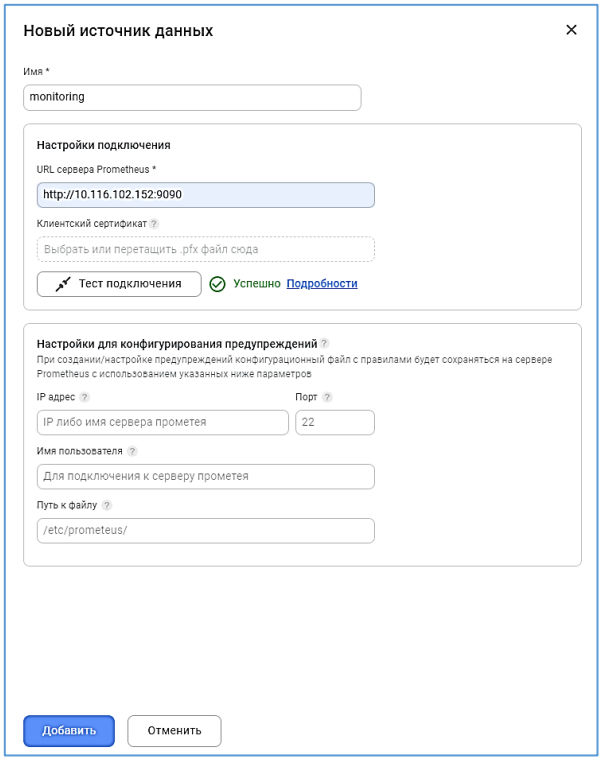

Рисунок 2.19 – Окно добавления нового источника данных

Установив параметры подключения, требуется проверить доступность источника. Нажатие на кнопку «Тест подключения» проверить доступность источника и сформирует дополнительную информацию по источнику, доступную по гиперссылке «Подробности».

При тестировании соединения в момент создания нового подключения к системе «PROMETHEUS» предоставляется подробная информация о настроенных экспортерах, а также адреса серверов СУБД, наблюдаемых соответствующими экспортерами.

Таким образом предоставляется информация о подключении требуемого инстанса системы «PROMETHEUS», правильно ли настроена система и подключены ли к ней желаемые базы.

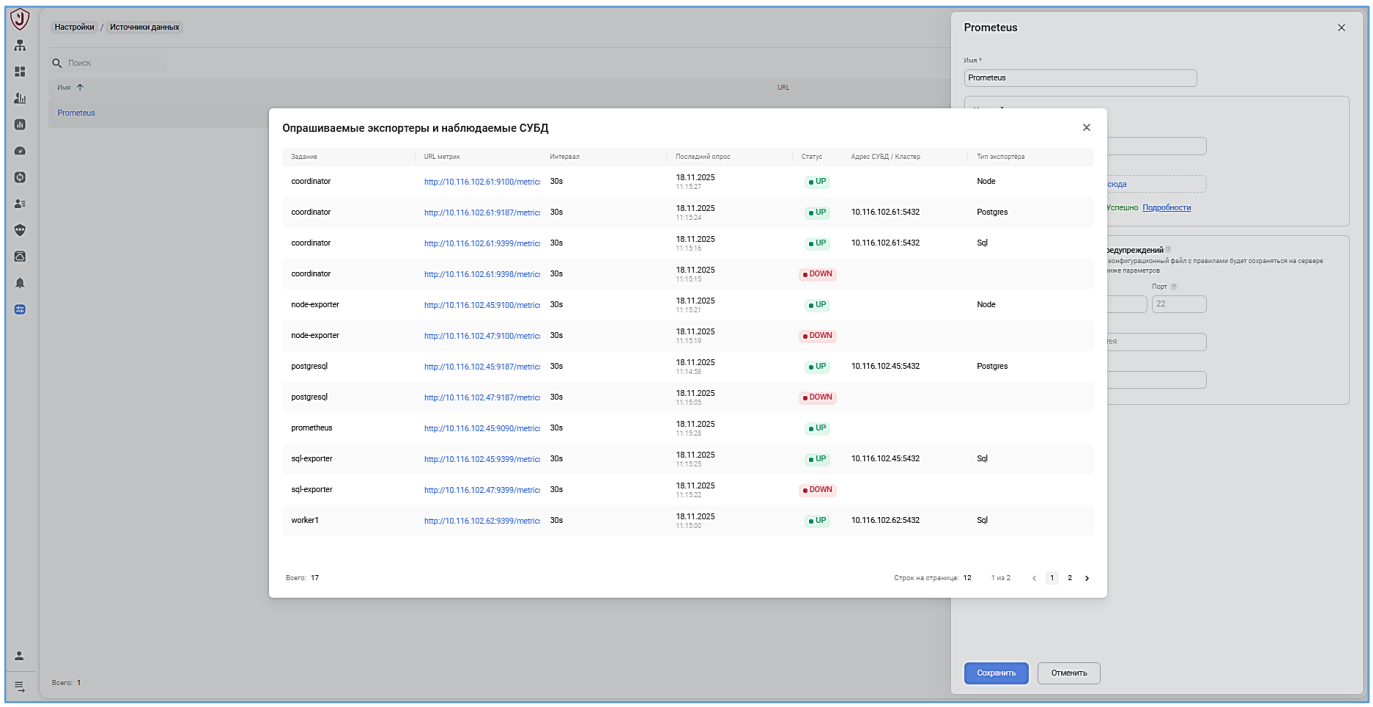

Рисунок 2.20 – Окно «Опрашиваемые экспортеры и наблюдаемые СУБД»

Перечень полей окна «Опрашиваемые экспортеры и наблюдаемые СУБД» приведен в таблице 2.4.

Таблица 2.4 - Перечень полей

Столбец	Примечание
Задание	
URL метрик	Активная ссылка, открывается в новой вкладке браузера
Интервал	Интервал опроса
Последний опрос	Временная метка последнего опроса
* всплывающая подсказка	Отображать длительность опроса в формате: "Длительность: 99.9 с"/"Duration: 99.9 s"
Статус	Статус экспортера: – UP - последний опрос экспортёра вернул метрики, экспортёр работоспособен; – DOWN - последний опрос экспортёра вернул ошибку
* всплывающая подсказка	В случае статуса DOWN отображать информацию об ошибке

Адрес СУБД	Адрес СУБД получаемый из метрик Prom-QL запросом: – pg_static (для postgres_exporter); – pg_server (для sql_exporter).
Тип экспортера	Тип экспортёра определяемый сочетанием названия метрики и содержимым метки **instance**: – pg_static для postgres_exporter; – pg_server для sql_exporter; – node_os_info для node_exporter; – windows_os_info для windows_exporter;

2.3.1. Информирование о неполном перечне наблюдаемых СУБД

После настройки источника данных компонент определит полный перечень возможных для мониторинга объектов.

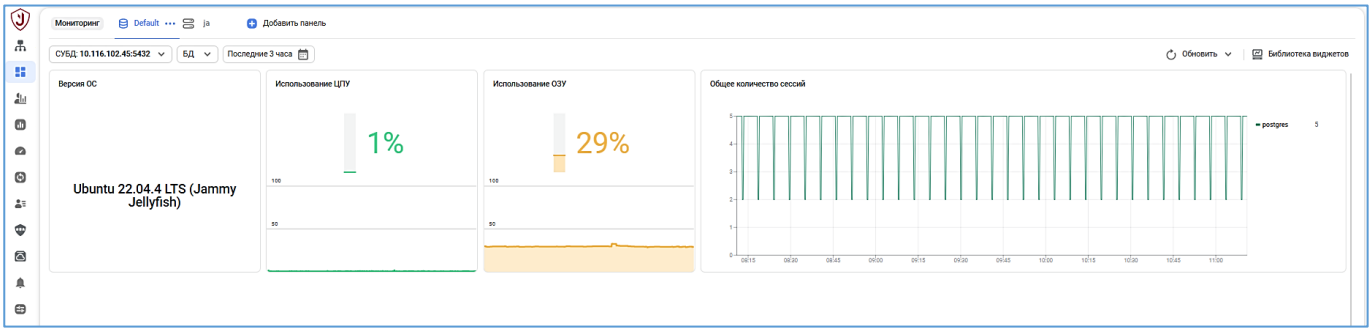

Рисунок 2.21 – Поле «Источник данных»

В поле выбора «Истопника данных» (СУБД) появится предупредительный знак, если в область мониторинга были не включены все инстансы системе «PROMETHEUS».

Наведение курсора на предупредительный знак, появится всплывающая подсказка.

Перейдя по гиперссылке «Вкладка «Источники данных» откроется одноименный раздел компонента, где выбрав любое из подключений и протестировав его в окне «Опрашиваемые экспортеры и наблюдаемые СУБД» будет выведен полный список (см. Рисунок 2.20).

2.4. Установка прав доступа к конфигурационным файлам

2.4.1. Установка прав доступа к конфигурационному файлу appsettings.json

Установка прав доступа к конфигурационному файлу appsettings.json выполняется администратором ИС.

Для администраторов ОС устанавливаются полные права, а для пользователей ОС устанавливаются права на чтение и выполнение.

Файл расположен по пути в:

— ОС семейства Windows

```
C:\Programm Files\GIS\JDS\appsettings.json
```

— В GNU Linux

```
/opt/jds/appsettings.json
```

2.4.2. Установка параметров в конфигурационного файле appsettings.json JDS

Описание раздела актуально для версии компонента JDS 2.3 и выше

В конфигурационного файле appsettings.json устанавливаются основные параметры работы компонента.

Remove expired refresh tokens

Проверка актуальности токенов, выдаваемых пользователям компонента, выполняется пакетным сценарием «Remove expired refresh tokens».

«Remove expired refresh tokens» по установленному интервалу времени, управляемого программным планировщиком Quartz.AspNetCore, в служебной БД JDS выполняет периодическую проверку таблицы «refreshtokens» для удаления записей.

Записи удаляются, если значение «refreshtokens.ExpireAT» меньше времени начала выполнения проверки.

По умолчанию установлены параметры:

```
"AccessTokenExpiration": 480, "RefreshTokenExpiration": 960
```

При необходимости измените параметры жизни «AccessTokenExpiration» и «RefreshTokenExpiration». Истечение срока действия «RefreshTokenExpiration» должно превышать «AccessTokenExpiration».

Таблица 2.5 – Параметры пакетного сценария «Remove expired refresh tokens»

Параметр	Значение	Единица измерения	Описание
JobKey	Remove expired refresh tokens		Наименование пакетного сценария
Active	True		Параметр определяющий статус выполнения Job.

Параметр	Значение	Единица измерения	Описание
			Допускаются значения: – True – включен; – False – отключен.
Interval	10080	Минуты	Периодичность запуска. Значение по умолчанию - 7 дней.

3. РАЗДЕЛ «ЛАНДШАФТ» (LANDSCAPE)

Подготовка хостов и развертывание СУБД «Jatoba», настройка SSH и SSL соединений, подключение хостов и СУБД к разделу «Ландшафт», описана в документе «Руководство по безопасности».

Раздел «Ландшафт» предназначен для:

— получения общей информации о хосте СУБД;

— получения общей информации о СУБД;

— управления конфигурационными файлами СУБД;

— установки и управления расширениями СУБД.

Доступен раздел в компоненте, только для пользователя с ролью «Администратор СУБД».

Добавление элементов во вкладку «Обзор» имеет иерархическую структуру и требует аутентификационную информацию для SQL, SSL и SSH соединения.

Не рекомендуется добавлять в раздел «Ландшафт» служебную СУБД «Jatoba» используемую компонентом JDS, а также проводить операции со служебной БД.

Управление хостом, в том числе и конфигурационными файлами требуют настройки SSH – соединения.

Таблица 3.1 – Требуемые параметры для подключения целевой СУБД

Уровень иерархии	Параметр	Значение
Группа		Произвольное
	Имя	Произвольное
	Описание	Произвольное
Хост		
	IP-адрес или FQDN-имя	
	Имя учётной записи	jdscontrol
	Порт для управления по SSH	22
СУБД		
	Имя сервиса *	
	Порт *	5432
	Путь к папке данных *	

Уровень иерархии	Параметр	Значение
	Путь к папке для резервного копирования *	
	Сертификат УЦ	
	Имя учётной записи администратора СУБД *	postgres
	Имя служебной БД *	postgres
	Режим шифрования	Disable/ Allow/ Prefer/ Require/ VerityCA/ VerityFull
	Способ аутентификации	Пароль/ SSL-сертификат
	Логин пользователя базы данных *	
	Пароль *	
Кластеры	Название	Имя кластера
	Адрес	Публичный IP-адрес
	Порт REST API	54443 (Custom)
	Сертификат пользователя	Контейнер pfx

Доступны операции:

— Создать группу с заданным наименованием;

— Изменить наименование группы;

— Расформировать группу;

После удаления группы все хосты, которые находились в ней, перемещаются в корень дерева «Ландшафта».

— Добавить хост в группу;

Если в группу добавляется хост, который уже находится в другой группе, то хост переносится из исходной группы в новую;

— Удалить хост из группы;

При удалении Хоста из Группы он перемещается в корень дерева Ландшафта.

3.1. Навигация в разделе «Ландшафт»

Навигация в разделе организована по принципу «хлебные крошки» (breadcrumbs).

В виде иерархической цепочки от имени раздела до уровня сущности СУБД, с возможностью перехода по уровням иерархии и выбора сущностей СУБД.

Раздел «СУБД» имеет две вкладки:

— «Список СУБД»;

— «Дерево инфраструктуры».

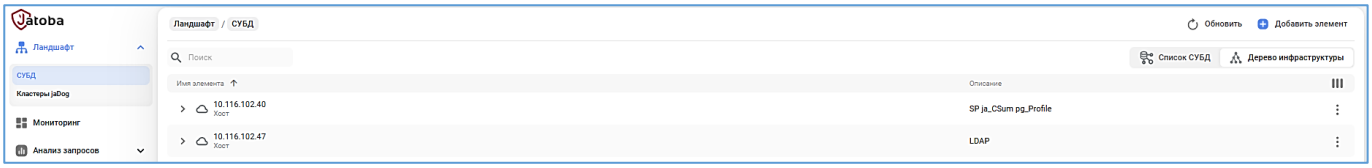

Рисунок 3.1 – Структура раздела «Ландшафт»

Список СУБД

Во вкладке «Список СУБД» выводится список подключенных к JDS СУБД.

Переход по гиперссылке СУБД выведет во вкладку «Обзор» и меню доступных действий, таких как:

— Назначение ролей;

— Параметры СУБД;

— Правила доступа;

— Доступные расширения;

— Настройка для ProBackup;

— Роли СУБД;

— Проблемы и решения;

— Активность БД;

— LDAP синхронизация;

— Парольные политики.

Отражаемый в верхней строке путь, позволяет перемещаться по разделу, в строке с именем СУБД из выпадающего списка выбрать подключенную СУБД и перейти к ней.

Дерево инфраструктуры

Во вкладке «Дерево инфраструктуры» отображается иерархическая структура хостов, СУБД и БД. В данной инфраструктуре доступны основные операции такие как:

— Добавление групп или хостов;

— Добавление СУБД;

— Редактирование параметров СУБД;

— Обновление содержания вкладки.

В левой части окна дублируются основные меню.

Во вкладке «Дерево инфраструктуры» возможно перейти до уровня БД на котором доступны

— Вкладка «Обзор» БД;

— Меню «Расширения»;

— Матрица доступа;

— Анализ рисков.

3.2. Хост. Вкладка «Обзор»

Предварительно подготовив целевой хост для управления, т.е. установив SSH-соединение, становится доступна операция добавления хоста в разделе «Ландшафт».

В результате на уровне иерархии объектов, типа «Хост», во вкладке «Обзор» отобразится состояние подключения по SSH протоколу и основная информация о хосте.

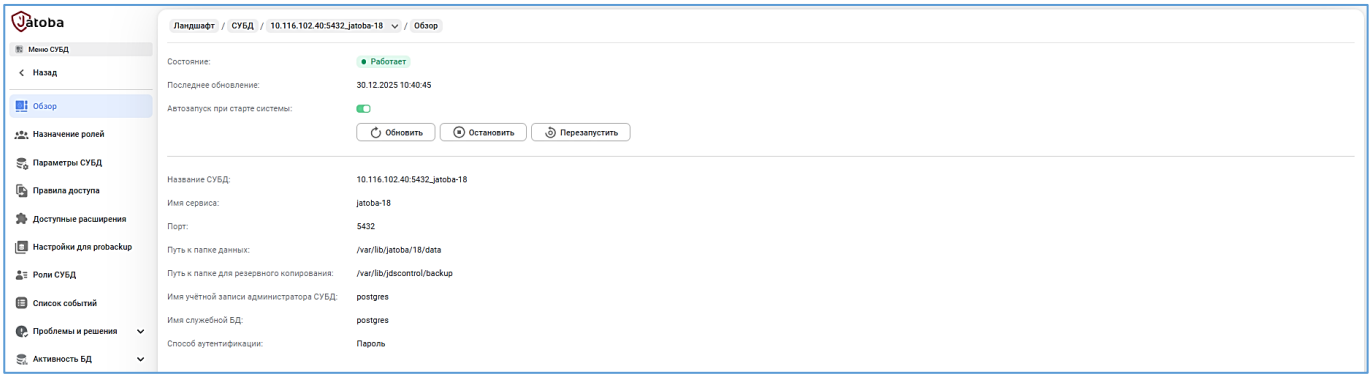

Рисунок 3.2 - Хост. Вкладка «Обзор»

Возможны 3 состояния хоста:

— "Под управлением" - успешный пробный вход на хост по протоколу SSH;

— "Ошибка аутентификации"- неуспешный пробный вход на хост по протоколу SSH;

— "Недоступен" - таймаут при попытке входа на хост по протоколу SSH.

4. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «ОБЗОР»

После подключения СУБД станет доступной и откроется вкладка «Обзор».

Во вкладке «Обзор» доступна общая информация о СУБД и управление службой СУБД на хосте:

— включение/отключение автозапуска службы в ОС;

— обновление состояния службы;

— остановка службы;

— перезапуск службы.

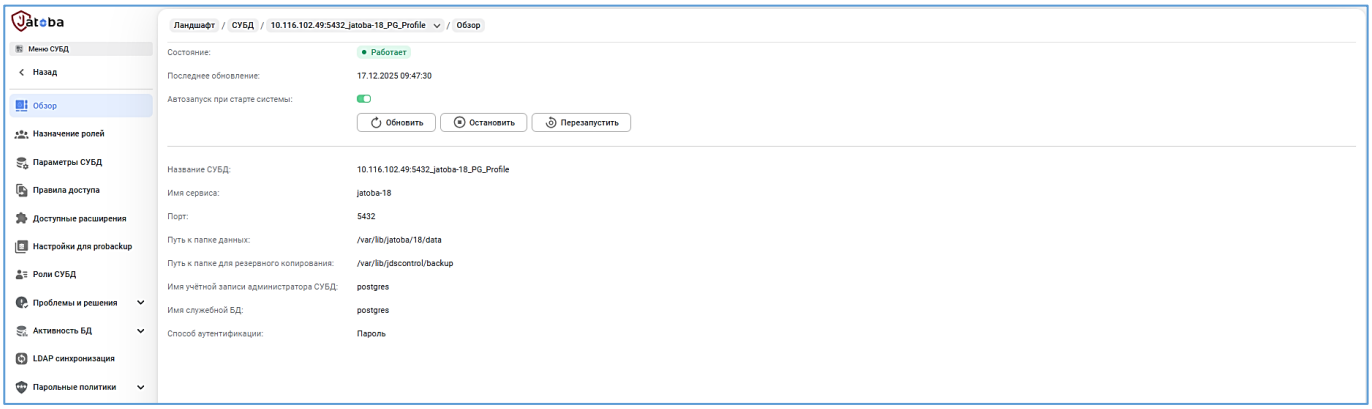

Рисунок 4.1 – Вкладка «Обзор»

5. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «НАЗНАЧЕНИЕ РОЛЕЙ»

Вкладка предназначена для тонкой автоматической настройки доступа к целевой СУБД с целью назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

Во вкладке отображаются учетные записи СУБД, которые могут использоваться для сервисов. По умолчанию используется привилегированный пользователь СУБД «postgres».

Во вкладке отображаются столбцы:

— Назначение;

— Роль;

— Способ аутентификации;

— Режим шифрования.

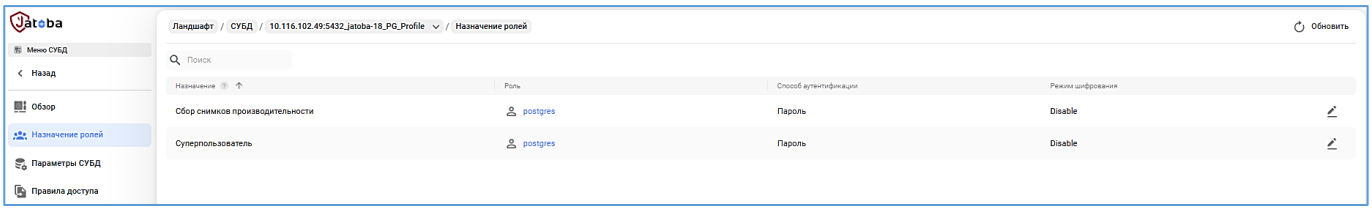

Рисунок 5.1 - Вкладка «Назначение ролей»

При нажатии на гиперссылку роли откроется одноимённое окно по имени сервиса, в котором доступно:

— смена роли;

— редактирование аутентификационной информации;

— тестирование подключения.

Смена роли автоматически вызовет скрипт назначения необходимых прав и привилегий для функционирования сервиса.

6. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «ПАРАМЕТРЫ СУБД»

Перед редактированием конфигурационных файлов СУБД «Jatoba» убедитесь, что компонент контроля целостности «ja_CSum» отключен или переведен в режим информирования (permissive). Поскольку, «ja_CSum» функционируя совместно компонентом парольных политик «SecurityProfile», пересчитав контрольные суммы конфигурационных файлов и найдя в них расхождения с эталонными значениями, передаст команду компоненту «SecurityProfile» на блокирование пользователей СУБД.

Во вкладке «Параметры СУБД» доступно изменение значений конфигурационного файла «postgresql.conf».

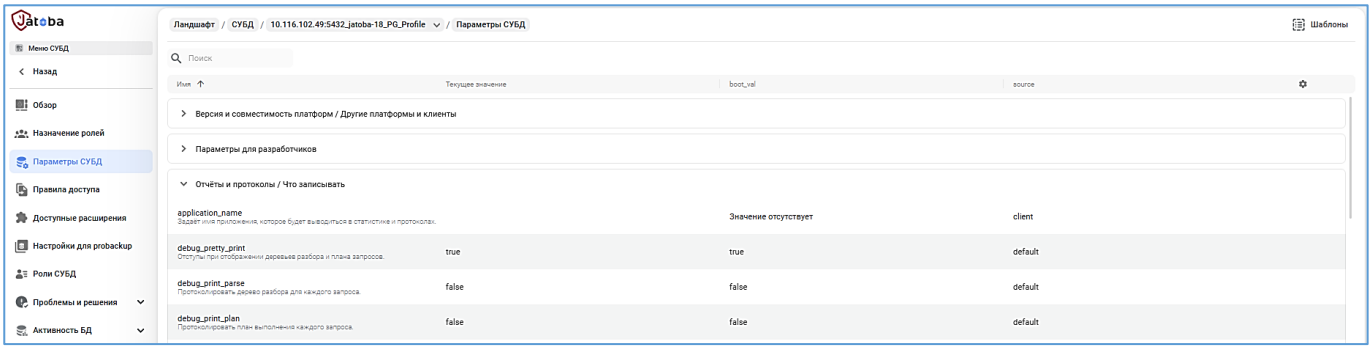

Рисунок 6.1 - Вкладка «Параметры СУБД»

Список параметров оснащен полнотекстовым поиском и сгруппирован по разделам.

Вкладка «Параметры СУБД» предоставляет набор данных:

— значение редактируемой величины;

— единица измерения текущего значения;

— тип данных текущего значения;

— величина минимального значения;

— величина максимального значения.

Изменение конкретного параметра доступно через пиктограмму в модальном окне.

Применение новых значений выполняется через:

— SQL-команду «ALTER SYSTEM»;

— Изменением конфигурационного файла, т.е. его перезаписью.

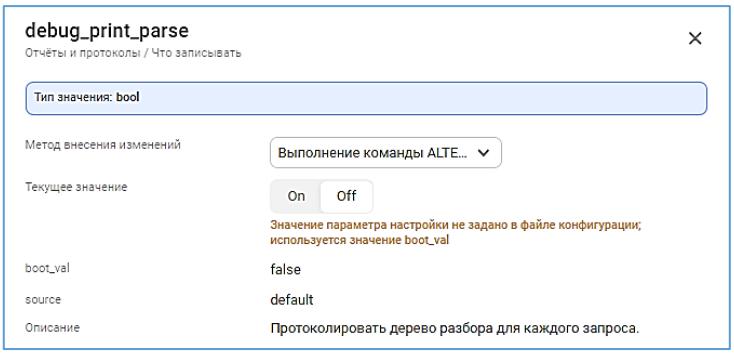

Рисунок 6.2 – Окно изменение параметра

Внесенные изменения не применяются автоматически, они отразятся в списке параметров и дополнительно будет выведено информационное сообщение в верхней строке.

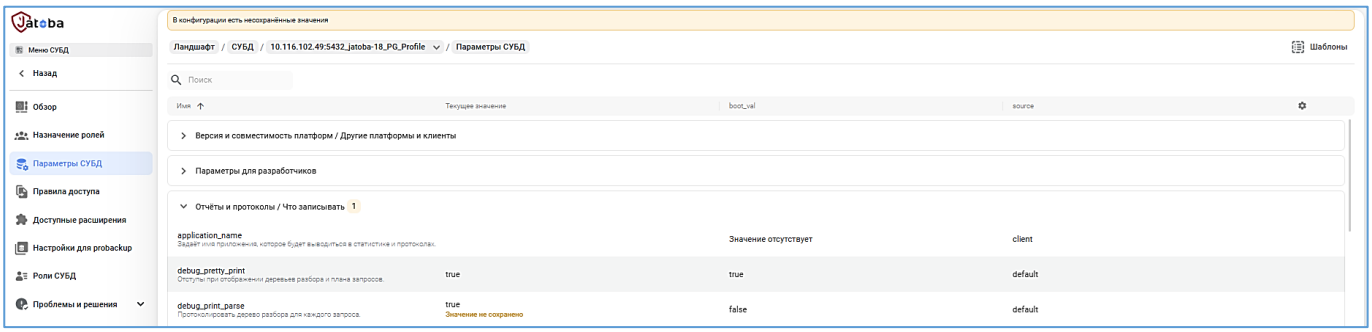

Рисунок 6.3 – Индикация о внесенных изменениях

Внесенные изменения отразятся в конфигурационного файла «postgresql.conf» отдельной строкой с комментарием о приложении внесшим изменение, дате и времени, а также о учетной записи компонента от имени и с правами которого внесены изменения.

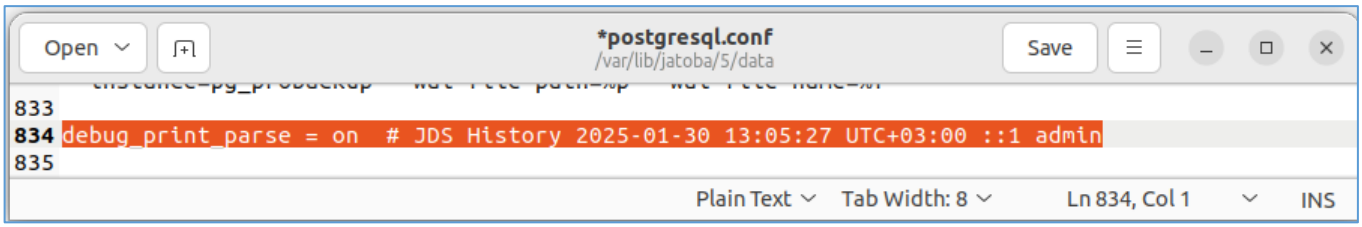

Рисунок 6.4 – Строка параметра измененная средствами компонента JDS

6.1. Шаблоны

Функциональная возможность изменения конфигурации целевых СУБД, позволяет оперативно применять, как шаблоны параметров, так и отдельные параметры, с целью:

— масштабирования типовых параметров;

— конфигурирования СУБД под определенный тип нагрузки;

— оперативного изменения набора параметров.

Имеющиеся шаблоны параметров доступны для всех СУБД, подключенных к разделу «Ландшафт».

Окно «Шаблоны параметров» вызывается кнопкой «Шаблоны», в котором доступно создание и импорт шаблона для конфигурационного файла «postgresql.conf» целевой СУБД.

6.1.1. Создание шаблона

Создание шаблона конфигурации СУБД доступно в окне «Создание шаблона» вызываемое кнопкой «Создать». В окне обязательно указывается название шаблона и дополнительно его описание.

Созданный шаблон будет пуст и иметь статус «Не соответствует». Параметр или параметры добавляются через кнопку «плюс» в строке шаблона.

Рисунок 6.5 – Добавление параметра в шаблон

После добавления параметр отразится в выпадающем списке шаблона.

Значение параметра будет автоматически проанализировано и установлен статус, как для всего шаблона, так и для параметра в частности.

6.1.2. Импорт шаблона

В качестве импорта шаблона допустимо использовать:

— имеющийся конфигурационный файл «postgresql.conf»;

— сгенерированный конфигурационный файл утилитой «ja_tune» при консольном запуске утилиты, как описано в документе «Руководство по установке»;

— любой текстовый файл в кодировке ANSI размером не более 100 кб.

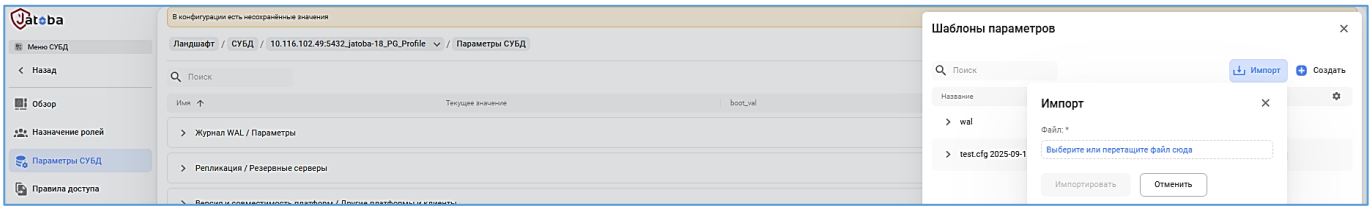

Рисунок 6.6 – Окно «Импорт»

Выбор шаблона параметров выполняется через обзор файловой системы хоста или перетаскиванием файла в окно «Импорт».

При импорте он будет проанализирован. Сравниваются «Значения текущей СУБД» и «Значения шаблона». Разница в значениях будет отмечена красным крестом. В строке шаблона будет указано количество параметров и статус проведенного анализа.

Рисунок 6.7 – Параметры импортированного шаблона конфигурации

К имени шаблона автоматически добавляется дата и время импорта.

Далее параметры могут быть изменены, удалены через кнопки в строке параметра, а также добавлены через меню в строке шаблона.

6.1.3. Применение шаблона к СУБД

Применение шаблона выполняется через опцию «Применить к текущей СУБД», в контекстном меню шаблона.

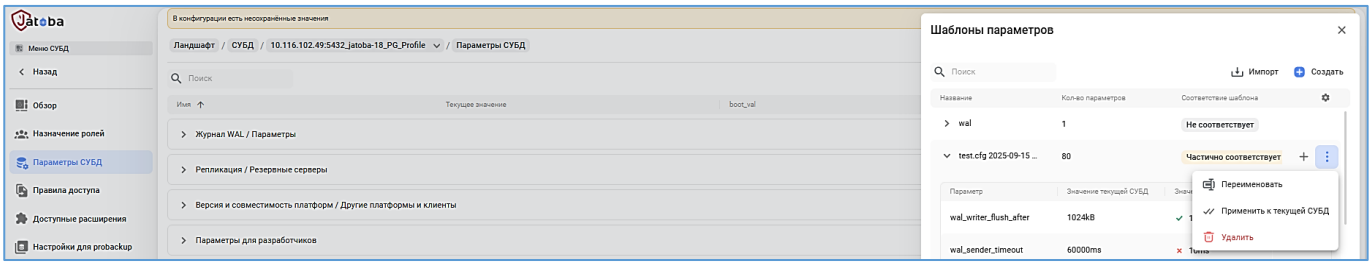

Рисунок 6.8 – Контекстное меню шаблона

Применение шаблона выполняется двумя методами:

— «По месту хранения параметра»;

— «Выполнение команды ALTER SYSTEM».

При выборе метода «ALTER SYSTEM» параметры будут дозаписаны в конфигурационный файл «postgresql.auto.conf», который имеет приоритет в выполнении.

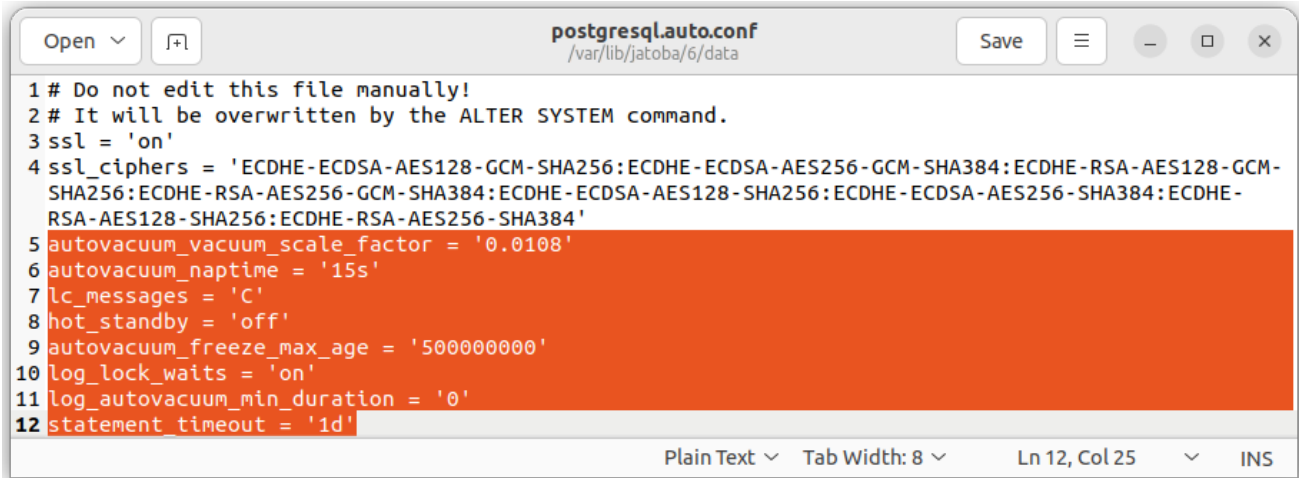

Рисунок 6.9 - Конфигурационный файл «postgresql.auto.conf» с дозаписанными параметрами

При выборе метода «По месту хранения параметра» компонент определит:

— расположение параметра, т.е. в «postgresql.conf» или в «postgresql.auto.conf»;

— попытается записать его;

— при невозможности записи параметра выведет информационное окно с описанием причин.

В случае, если компоненту не удалось применить шаблон, следует:

— устранить причину неприменимости;

— изменить метод применения.

Автоматически определится и выведется информационное сообщение о необходимости перезагрузки СУБД.

7. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «ПРАВИЛА ДОСТУПА»

Перед редактированием конфигурационных файлов СУБД «Jatoba» убедитесь, что компонент контроля целостности «ja_CSum» отключен или переведен в режим информирования (permissive). Поскольку, «ja_CSum» функционируя совместно компонентом парольных политик «SecurityProfile», пересчитав контрольные суммы конфигурационных файлов и найдя в них расхождения с эталонными значениями, передаст команду компоненту «SecurityProfile» на блокирование пользователей СУБД.

Во кладке «Правила доступа» доступно изменение значений конфигурационного файла «pg_hba.conf», в котором устанавливаются параметры аутентификации в СУБД.

Табличная часть вкладки отображает установленные параметры аутентификации.

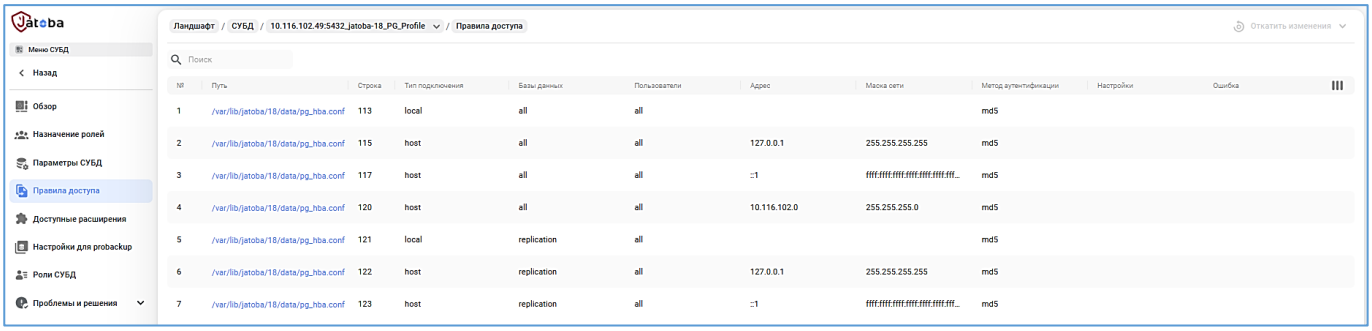

Рисунок 7.1 – Вкладка «Правила доступа»

Они целиком отражают структуру конфигурационного файла «pg_hba.conf».

Нажатие на гиперссылку в столбце «Путь» вызовет редактор, в котором доступны стандартные функции редактирования и «горячих клавиш».

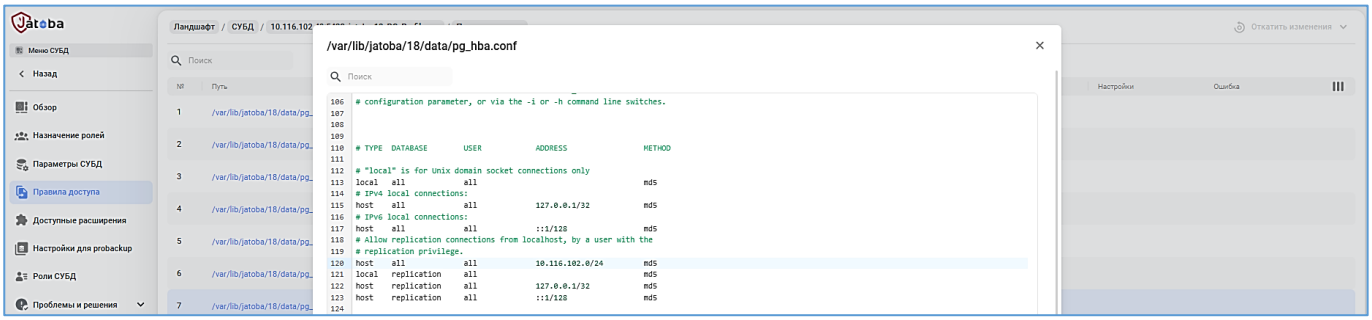

Рисунок 7.2 - Редактор конфигурационного файла «pg_hba.conf»

Внесенные изменения сохраняются по кнопке «Сохранить». При первой операции по редактированию конфигурационного файла «pg_hba.conf» сохраняться 2 резервные копии.

В первой резервной копии будет храниться исходный файл до редактирования. Во второй резервной копии будет храниться новый измененный файл.

На данном шаге сработает защитный механизм проверки файла на ошибки. Если ошибки отсутствуют, кнопка «Применить изменения» будет разблокирована, по ее нажатию производится выполнение SQL-команды:

```
SELECT pg_reload_conf();
```

Целевая СУБД применит внесенные изменения без полной перезагрузки.

Конфигурационный файл «pg_hba.conf» целевой СУБД храниться на хосте служебной СУБД JDS. Таким образом реализуется функциональная возможность управления резервными копиями конфигурационного файла.

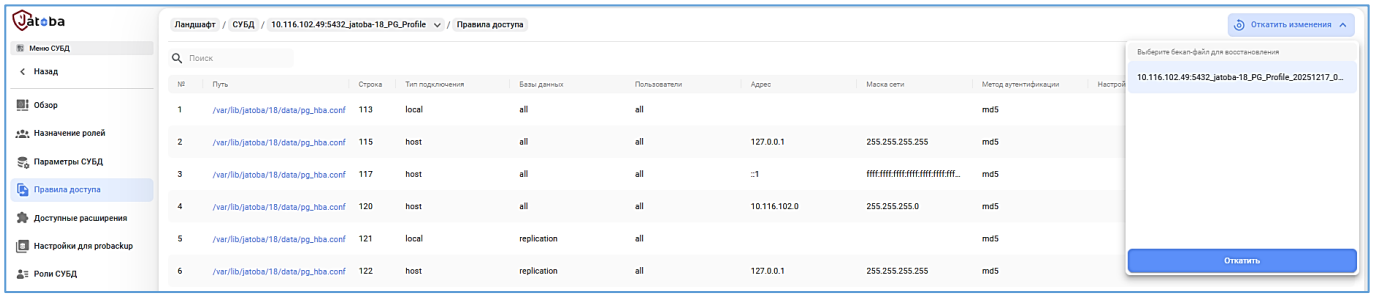

Рисунок 7.3 – Окно «Откатить изменения»

Имя файл резервной копии имеет вид <service>_ГГГГММДД_ЧЧММСС.hba.bak, где:

— <servicename> - имя сервиса СУБД на целевом хосте;

Их может быть несколько. Имя совпадает с именем сервиса, используемым в утилите systemctl:

```
systemctl status <servicename>.service
```

— ГГГГММДД - строковое представление даты создания резервной копии;

— ЧЧММСС - строковое представление времени создания резервной копии.

Имеющиеся резервные копии конфигурационного файл «pg_hba.conf» возможно восстановить (откатить). Для этого требуется:

— нажать кнопку «Откатить изменения» находящейся в правом верхнем углу окна «Правила доступа», как показано на рисунке 7.3;

— выбрать требуемую резервную копию;

— нажать кнопку «Откатить».

Изменения применяться автоматически.

Сохранение резервных копий и их восстановление выполняется от имени и с правами учетной записи ОС «jdscontrol» по протоколу SSH.

8. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «ДОСТУПНЫЕ РАСШИРЕНИЯ»

Список доступных расширений СУБД отображается во вкладке «Доступные расширения».

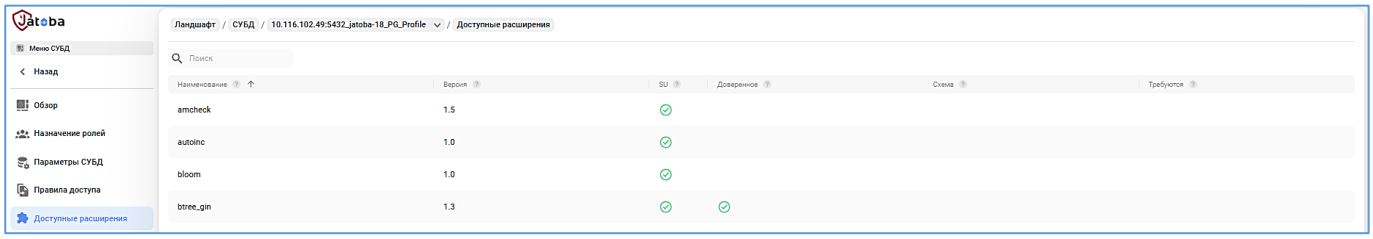

Рисунок 8.1 – Вкладка доступные расширения

Список формируется выборкой из представлений «pg_available_extension_versions» и «pg_available_extensions». Расширения идентифицируются по их наименованию в поле «pg_available_extension_versions.name».

Вкладка «Доступные расширения» предназначена для отображения списка расширений доступных на выбранной СУБД для их установки в БД.

Если в общем списке требуемое расширение не отображается и контекстный поиск в одноименном поле не дал результатов, это означает, что не установлен пакет расширения (компонента) в СУБД.

Если в общем списке требуемое расширение не отображается и контекстный поиск в одноименном поле не дал результатов, это означает, что не установлен пакет расширения (компонента) в СУБД.

Также отображается информация какие требования предъявляют расширения к своему окружению и порядку установки.

Расширения устанавливаются в разделе «Ландшафт», на уровне БД во вкладке «Расширения» (см. р. 16).

Влияние параметров прав в расширении на возможность управления пользователем этим расширением представлено в таблице 8.1

Таблица 8.1 – Влияние параметров на возможность управления расширениями

Пользователь		**Расширение**	
с правами, но без SU	с правами SU	**(SU)**	**(Доверенное)**
		Требование суперпользователя	Возможность выполнить под SU
Запрет	Выполнение под текущим суперпользователем	X	—
Выполнение под текущим пользователем	Выполнение под текущим суперпользователем	—	X
Выполнение под начальным суперпользователем	Выполнение под текущим суперпользователем	X	X
Выполнение под текущим пользователем	Выполнение под текущим суперпользователем	—	—

9. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «РОЛИ СУБД»

Раздел «Роли БД» предназначен для:

— создания ролей;

— редактирования ролей;

— назначения атрибутов и привилегий ролей.

9.1. Список пользователей

Выбор раздела «Роли БД» откроет пустое окно списка пользователей. После выбора цели и БД отразится полный список пользователей целевой СУБД.

Список пользователей состоит из столбцов:

— «Роль» (Role);

— «ID»;

— «Тип» (Type);

— «Атрибуты» (Attributes);

— «Доступные базы данных» (Available database).

В столбце «Роли» отражаются роли пользователей в алфавитном порядке и роли, включающие в себя другие роли (групповые роли). По умолчанию в начале списка находится псевдороль «public».

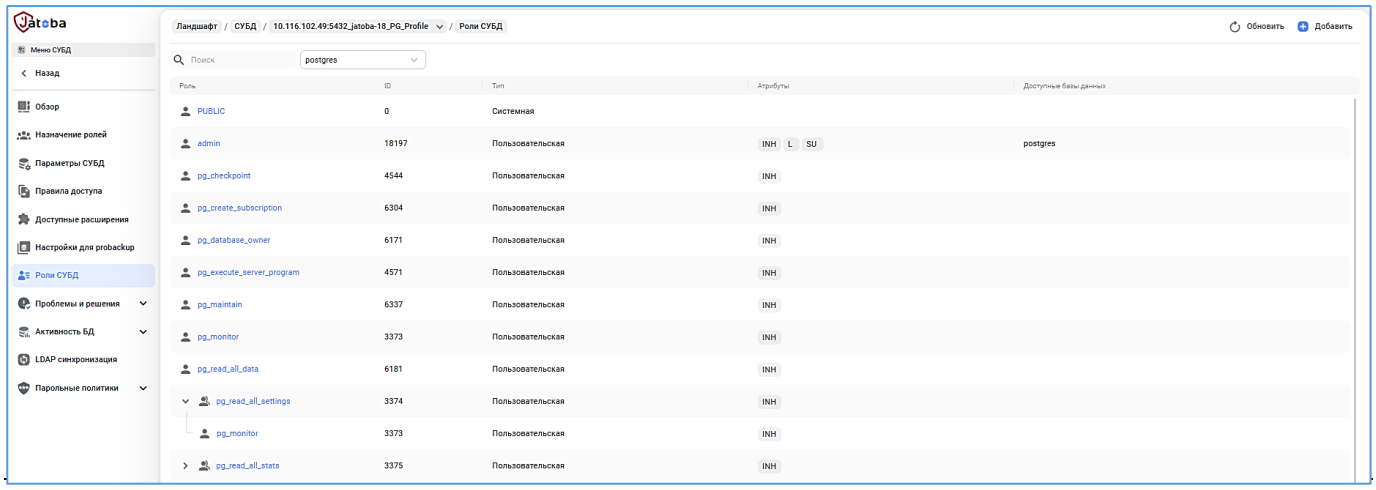

Рисунок 9.1 – Окно списка пользователей

Групповые роли отображаются с дополнительной пиктограммой и отображаются в форме иерархического списка.

В столбце «ID» отображаются автоматически присвоенные СУБД номера учетных записей.

Столбец «Type» отображает два типа учетных записей:

— пользовательская (Custom);

— системная (System).

Столбец «Attributes» отображает атрибуты присвоенные роли в форме аббревиатур, приведенных в таблице 17.1. Наведение курсора на пиктограмму аббревиатуры вызовет контекстную подсказку с полным наименованием атрибута.

Столбец «Доступные базы данных» (Available database) отображает БД доступные для подключения пользователем.

9.2. Создание роли

Окно создание роли вызывается нажатием кнопки «Добавить» (Add), расположенной в правом верхнем углу окна. Окно включает в себя 5 вкладок:

— «Основные параметры» (Main settings);

— «Атрибуты» (Attributes);

— «Роли и группы» (Roles and groups);

— «Привилегии» (Privileges);

— «SQL».

9.2.1. Вкладка «Основные параметры» (Main settings);

В вкладке «Основные параметры» выведены поля:

— «Имя» (Name);

— «Описание» (Description);

— «Пароль» (Password);

— «Подтверждение пароля» (Repeat password);

Ввод имени пользователя является обязательным.

В поле «Имя» вводится имя создаваемой роли длиной не менее двух символов. Случайно вставленные символы пробела при генерации SQL-команды будут усечены.

При вводе имени пользователя, становится доступной кнопка «Сохранить» и генерируется SQL-команда:

```
CREATE ROLE [user_name];
```

В поле «Описание» вводится описание создаваемой роли длиной до 255 символов.

Ввод описания пользователя является обязательным.

В поле «Пароль» вводится пароль для создаваемого пользователя длиной от 6 до 50 символов.

В поле «Подтверждение пароля» вводится идентичный пароль задаваемому.

Ввод пароля для роли может производится при создании роли.

При редактировании роли функциональная возможность смены пароля недоступна.

Нажатие кнопки «Сохранить» сгенерирует SQL-команду:

```
ALTER ROLE [name_role] PASSWORD [password role];
```

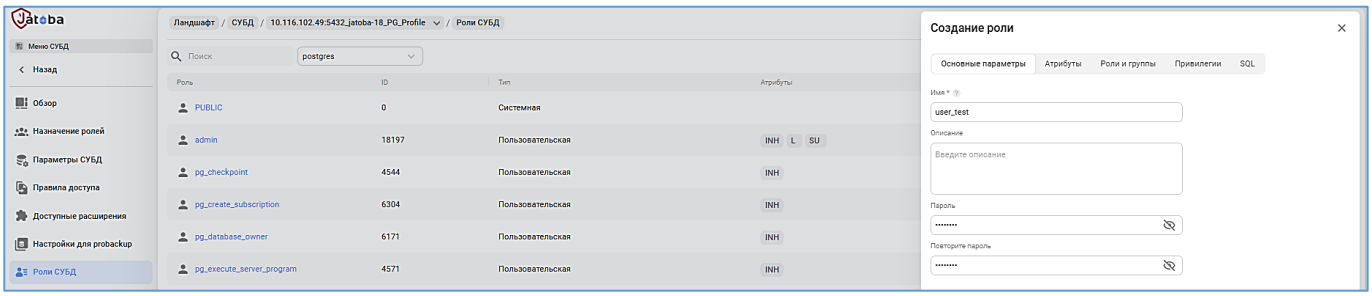

Рисунок 9.2 – Вкладка «Основные параметры» (Main settings)

9.2.2. Вкладка «Атрибуты»

На вкладке «Атрибуты» (Attributes) выведены:

— флаги:

- SUPERUSER;

- INHERIT;
- CREATEROLE;
- CREATEDB;
- LOGIN;
- REPLICATION;
- BypassRls.

— поля:

- Квота соединений (Connection limit);
- Действительна до (Valid util).

Установкой флагов назначаются атрибуты создаваемой роли.

Доступно назначение только тех атрибутов, которые назначены ассоциированной роли СУБД для пользователя JDS.

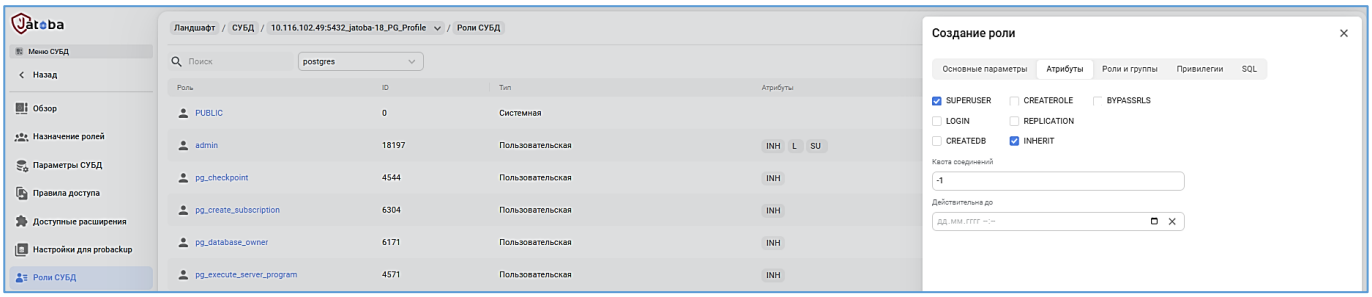

Рисунок 9.3 - Вкладка «Атрибуты» (Attributes)

В поле «Квота соединений» устанавливается значение количества соединений для роли. Доступно установить значения приведенные в таблице 9.1.

Таблица 9.1 – Допустимые значения квоты соединений

Значение	Описание
-1	нет ограничений
0	соединение запрещено
Целое положительное число	Количество соединений

Ввод значения квоты соединений для роли не является обязательным.

В поле «Действительна до» (Valid util) устанавливается дата и время действия роли, с точностью до минуты. Параметр используется для временных учетных записей.

Ввод значения доступен через окно календаря или вручную.

Ввод даты и времени действия роли не является обязательным.

9.2.3. Вкладка «Роли и группы» (Roles and groups)

В вкладке «Роли и группы» отображаются два поля:

— «Участники группы»;

— «Входит в группы».

При добавлении ролей в поле «Участники группы» роль станет «групповой» и включенные в нее роли унаследуют атрибуты и привилегии роли.

Добавление участников группы выполняется нажатием кнопки «Добавить роль», которое вызовет окно добавления ролей (см. рис. 9.4). Выбор ролей выполняется, через поле поиска или вручную установкой флагов. Нажатие кнопки «Добавить» внесет выбранные роли в поле «Участники группы».

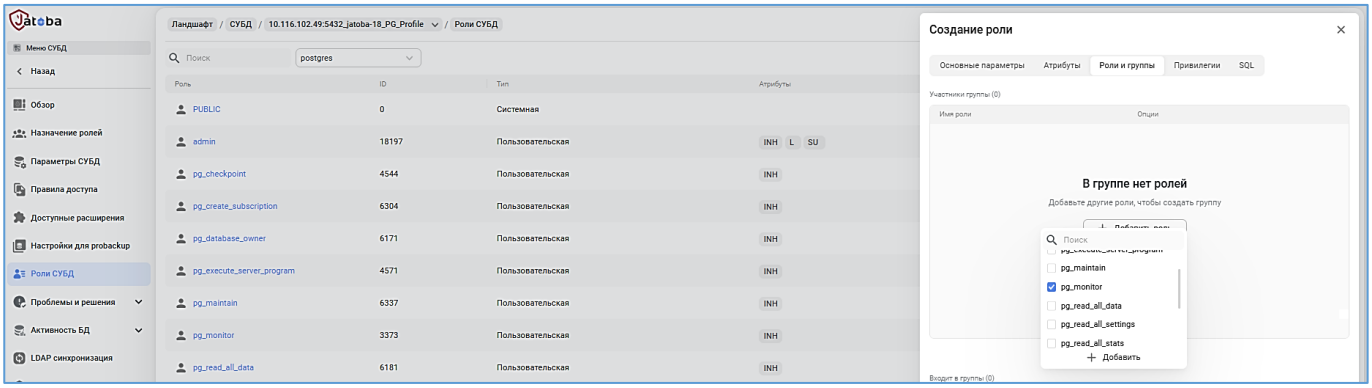

Рисунок 9.4 – Окно добавления ролей

При добавлении роли в поле «Входит в группы» она станет участником «групповой роли» и унаследует атрибуты и привилегии роли в которую она входит.

Добавление роли в группы выполняется нажатием кнопки «Добавить в группу», которое вызовет окно добавления ролей (см. рис. 9.4). Выбор ролей выполняется, через поле поиска или вручную установкой флагов. Нажатие кнопки «Добавить» внесет выбранные роли в поле «Входит в группы».

Структура ролей в СУБД имеет иерархическую структуру и не допускает «закольцованности», т.е. в случае добавление вышестоящей роли в нижестоящую по иерархии, нижестоящая роль изменит свой статус и станет вышестоящей.

Например

Созданы роли:

— role_1;

— role_2;

— role_3.

Шаг 1.

Добавим роль «role_2» в состав роли «role_1» SQL-командой:

```
GRANT "role_1" TO "role_2";
```

Рисунок 9.5 – Выполнение SQL-команды добавления роли «role_2» в состав роли «role_1»

После чего роль «role_1» станет групповой и образуется иерархия ролей. В иерархии ролей роль «role_1» займет первый уровень, а роль «role_2» займет второй уровень.

Рисунок 9.6 – Иерархия ролей при шаге 1

Шаг 2.

На втором шаге групповую роль «role_1» добавим в состав роли «role_3» SQL-командой:

```
GRANT "role_3" TO "role_1";
```

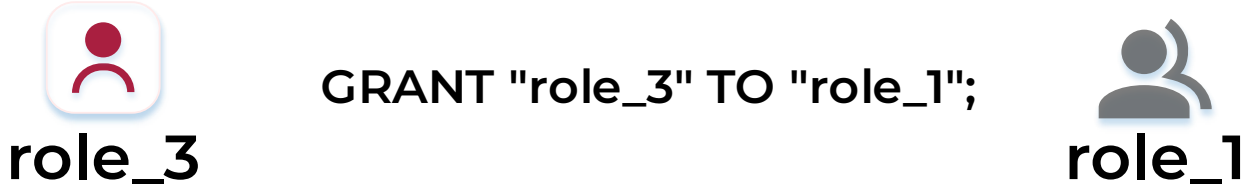

Рисунок 9.7 – Выполнение SQL-команды добавления роли «role_1» в состав роли «role_3»

После чего иерархия ролей изменится. Роль «role_3» станет групповой и займет первый уровень. На втором уровне иерархии в нее будет входить групповая роль «role_1». На третьем уровне иерархии находится простая роль «role_2», входящая в состав групповой роли «role_1», как представлено на рисунке 9.8.

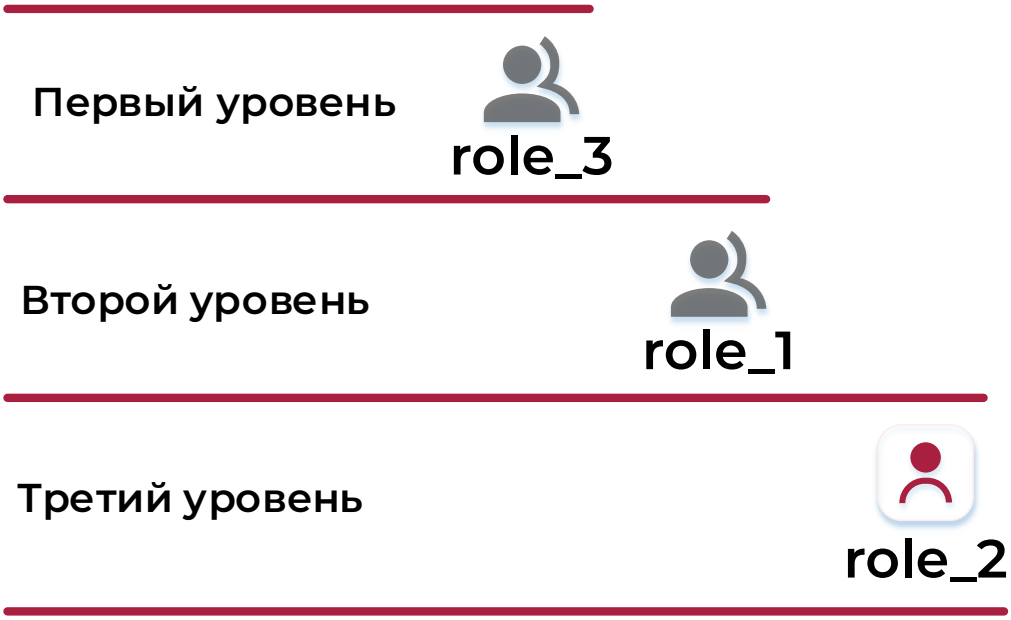

Рисунок 9.8 – Иерархия ролей при шаге 2

Шаг 3.

На третьем шаге включим в состав роли «role_2» третьего уровня, групповую роль «role_3» первого уровня SQL-командой:

```
GRANT "role_2" TO "role_3";
```

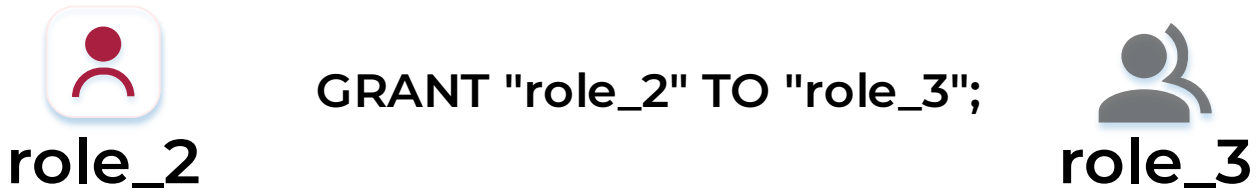

Рисунок 9.9 - Выполнение SQL-команды добавления роли «role_3» в состав роли «role_2»

Возникнет ошибка:

```
Ошибка при обновлении роли БД: Ошибка '0LP01: role "role_2" is
a member of role "role_3"' при выполнении SQL-команды 'GRANT
"role_2" TO "role_3";'!
```

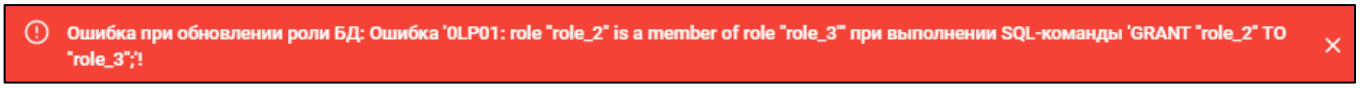

Рисунок 9.10 – Всплывающее сообщение об ошибке

Ошибка возникнет из-за нарушения иерархии ролей.

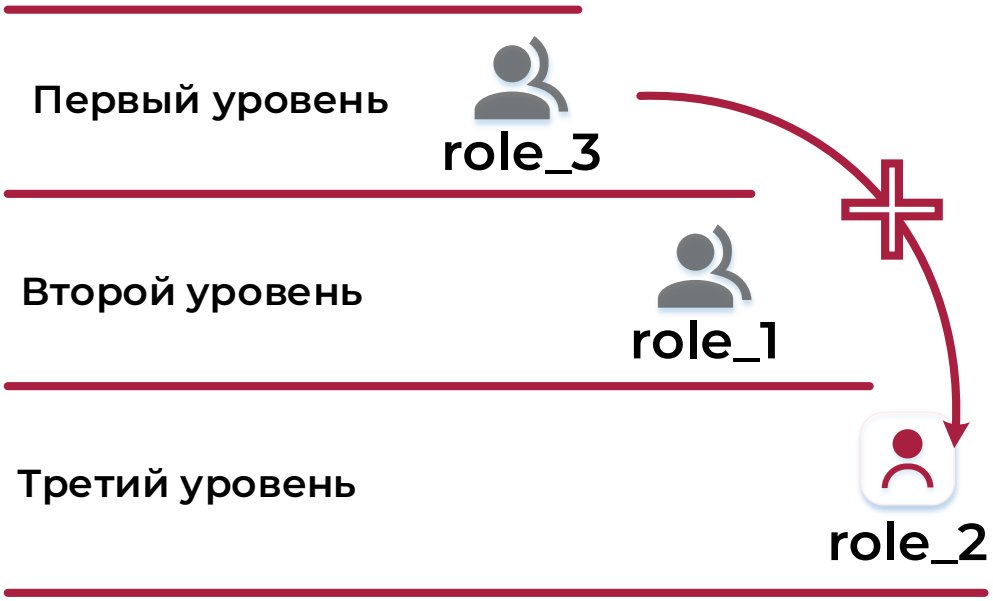

Рисунок 9.11 – Ошибка построения иерархии ролей. Закольцованность структуры

Действия по формированию групповых ролей не является обязательными.

9.2.4. Вкладка «Привилегии» (Privileges)

На вкладке привилегии назначаются привилегии и системные привилегии пользователей на объекты СУБД.

На вкладке отображается БД, к которой было произведено подключение при выборе цели в разделе «Роли БД» (DB roles). Остальные БД СУБД будут неактивны. Для работы с другими БД СУБД потребуется переподключение.

Объекты БД представлены в виде структурированного иерархического списка.

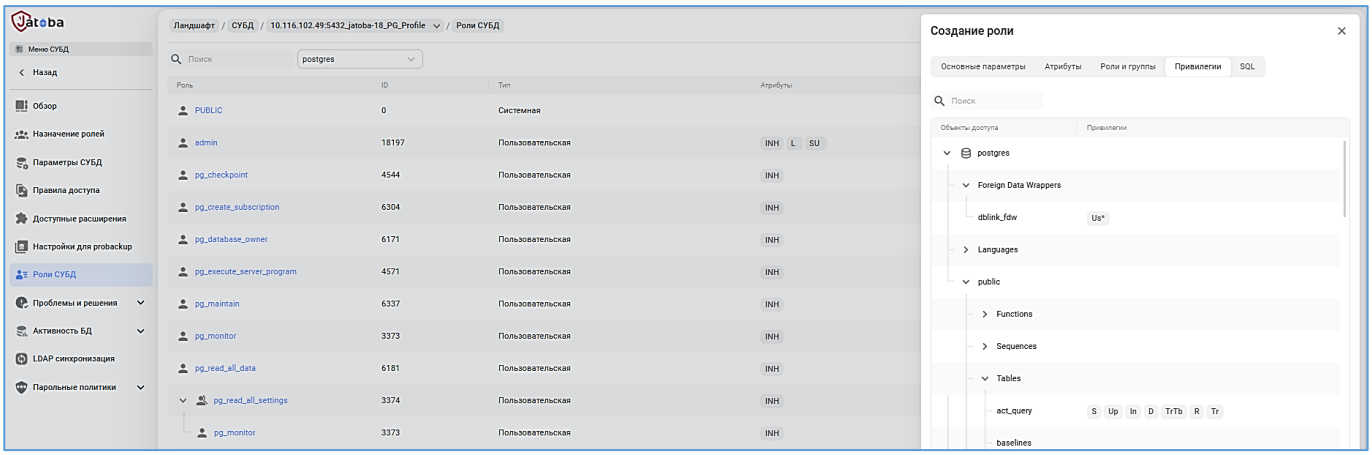

Рисунок 9.12 – Иерархический список объектов БД

Привилегии назначаются, как на типы объектов, так и на сами объекты БД.

Назначаемые привилегий представлены в таблице 9.2.

Таблица 9.2 – Назначаемые привилегии

Объекты доступа			**Привилегии пользователей**	**Сокращенные аббревиатуры в DB roles**	**Аббревиатуры в User Risk и Access Matrix**	**Наименование привилегий и системных привилегий пользователей**
БД			CONNECT	**CnDB**	**CnDB**	CONNECT DATABASE
			CREATE	**CrDB**	**CrDB**	CREATE DATABASE
			TEMPORARY	**TDB**	**TDB**	TEMPORARY DATABASE
	Схема (SCHEMA)		CREATE	**Cr**	**CrSc**	CREATE SCHEMA
			USAGE	**Us**	**USc**	USAGE SCHEMA
		Таблица	SELECT	**S**	**STb**	SELECT TABLE
			INSERT	**In**	**ITb**	INSERT TABLE
			UPDATE	**Up**	**UpTb**	UPDATE TABLE
			DELETE	**D**	**DTb**	DELETE TABLE
			REFERENCES	**R**	**RTb**	REFERENCES TABLE
			TRIGGER	**Tr**	**Tr**	-
			TRUNCATE	**TrTb**		TRUNCATE TABLE
		Представление (View)	SELECT	**S**	**S**	Select
			INSERT	**In**	**In**	Insert
			UPDATE	**Up**	**UP**	Update
			DELETE	**D**	**D**	Delete

Объекты доступа			Привилегии пользователей	Сокращенные аббревиатуры в DB roles	Аббревиатуры в User Risk и Access Matrix	Наименование привилегий и системных привилегий пользователей
			REFERENCES	**R**	**R**	-
			TRIGGER	**Tr**	**Tr**	-
		Мат.представления (Materialized View)	SELECT	**S**	**S**	Select
			INSERT	**In**	**In**	Insert
			UPDATE	**UP**	**UP**	Update
			DELETE	**D**	**D**	Delete
			REFERENCES	**R**	**R**	-
			TRIGGER	**Tr**	**Tr**	-
		Функция (FUNCTION)	EXECUTE	**E**	**EFn**	EXECUTE FUNCTION
		Последовательность (Sequence)	SELECT	**S**	**SSq**	SELECT SEQUENCE
			UPDATE	**Up**	**UpSq**	UPDATE SEQUENCE
			USAGE	**Us**	**USq**	USAGE SEQUENCE
		Типы данных (TYPE)	USAGE	**Us**	**UTy**	USAGE TYPE
	Языки (LANGUAGE)		USAGE	**Us**	**ULn**	USAGE LANGUAGE
	Foreign Server		USAGE	**Us**	**UFS**	USAGE FOREIGN SERVER
	Foreign Data Wrapper		USAGE	**Us**	**UFDW**	USAGE FOREIGN DATA WRAPPER
	Табличное пространство (Tablespace)		USAGE	**Us**	**Us**	Usage
			CREATE	**Cr**	**CrTS**	CREATE TABLESPACE
	Large Objects		SELECT	**S**	**SLO**	SELECT LARGE OBJECT
			UPDATE	**Up**	**UpLO**	UPDATE LARGE OBJECT

Требуемый объект доступно найти или по имени в строке поиска или спускаясь по списку объектов БД.

Пиктограмма вызова окна назначения привилегий появляется при наведении курсора на правую сторону строки объекта.

Для каждого из типов объектов и непосредственно объектов, окно назначения привилегий имеет собственный набор привилегий, как представлено в таблице 9.2.

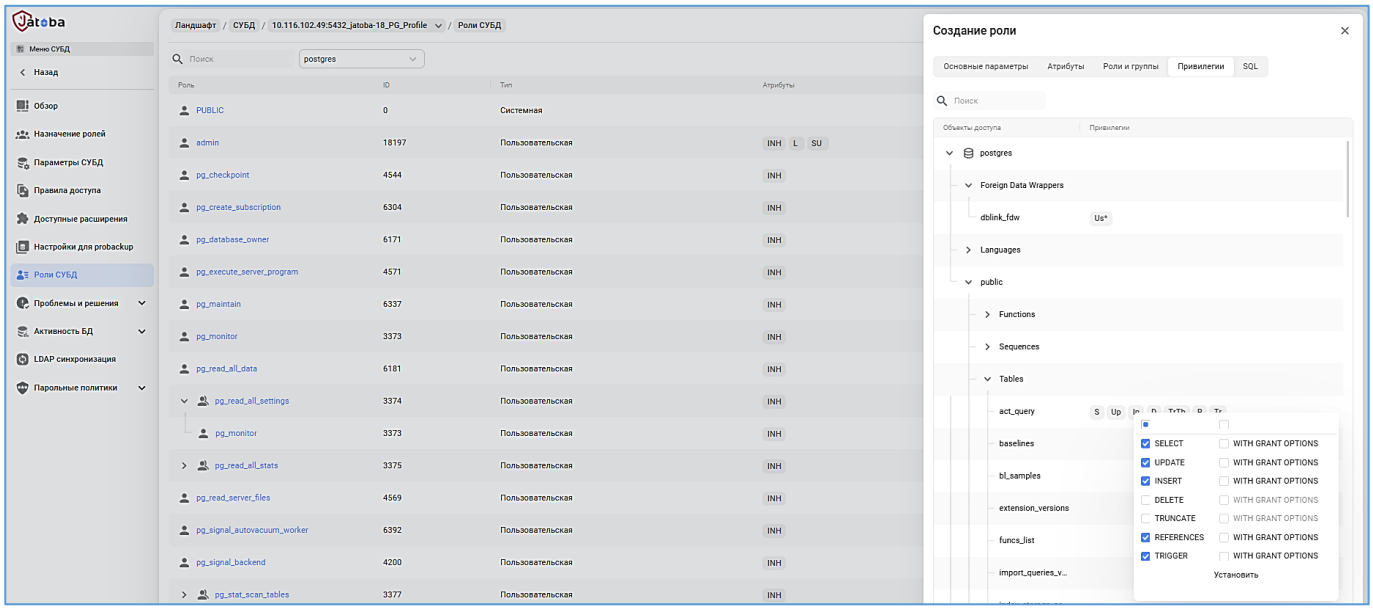

Рисунок 9.13 – Окно назначение привилегий

Привилегии устанавливаются или снимаются флагами в строке наименования привилегии.

Флагами, расположенными в первой строке, устанавливаются или снимаются все доступные привилегии.

Уже назначенные привилегии отображаются аббревиатурами.

Аббревиатуры в разделе «DB roles» частично отличаются от аббревиатур привилегий используемых в разделах JDS User Risk и Access Matrix.

9.2.5. Вкладка «SQL»

В вкладке «SQL» отображаются сформированные SQL-команды доступные только для ознакомления.

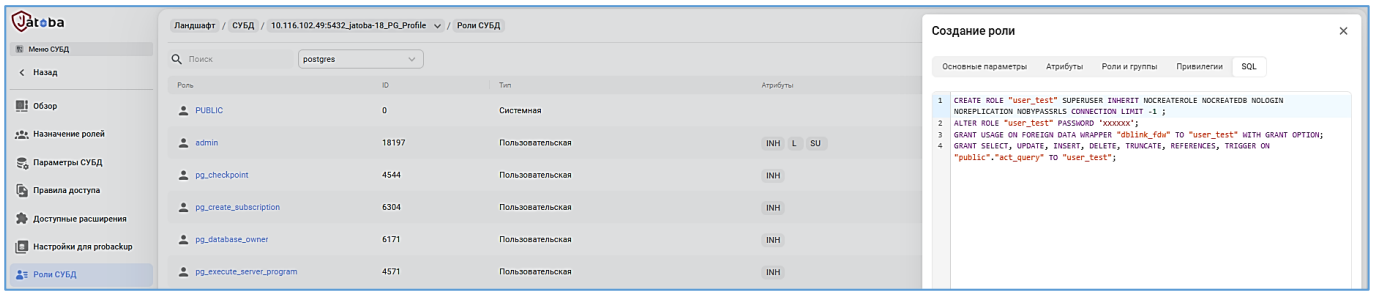

Рисунок 9.14 – Вкладка «SQL»

Команды формируются в логической последовательности выполнения.

Пользователь создается после нажатия кнопки «Сохранить» (Save). При успешном выполнении будет выведено информационное сообщение.

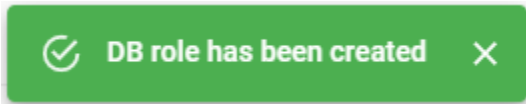

Рисунок 9.15 – Сообщение о создании роли

9.3. Редактирование роли

Окно редактирования роли вызывается нажатием на имени роли или выбором кнопки редактирования в строке роли.

На всех вкладках будут отражены ранее установленные права и привилегии.

На вкладе «Основные параметры» доступна функциональная возможность смены пароля пользователя СУБД с помощью кнопки «Задать пароль».

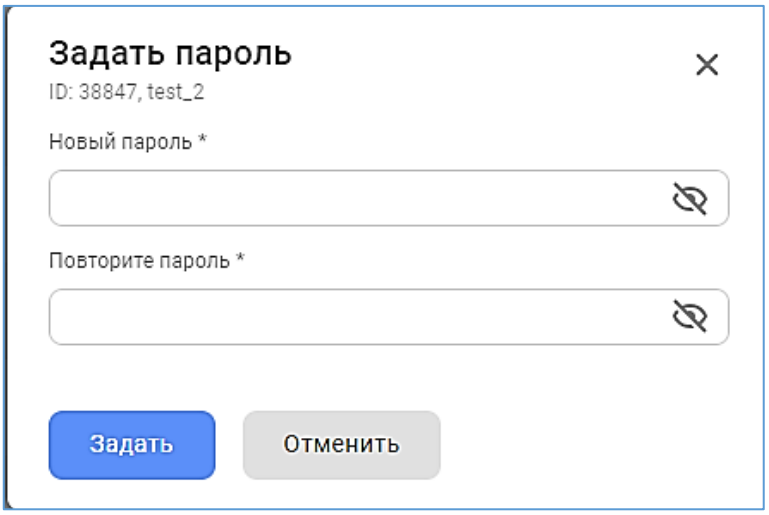

Рисунок 9.16 – Смена пароля пользователя СУБД

Смена пароля пользователя произойдет сразу, после нажатия кнопки «Задать», без отражения SQL-команды на вкладке «SQL».

9.4. Недоступные функциональные возможности. «Работа с блокировками»

Во вкладке «Роли СУБД» недоступна функциональная возможность блокирования/разблокирования пользователей СУБД. Данная функциональность реализована во вкладке «Парольные политики» см. п.п. 14.3 «Вкладка «Работа с блокировками».

9.5. Удаление роли

Кнопка удаления роли появляется при наведении на строку роли в карточке списка ролей. Нажатие на кнопку вызывает модальное окно «Удаление роли» (см. рис. 9.17).

Удаление роли потребует подтверждения нажатием кнопки «OK».

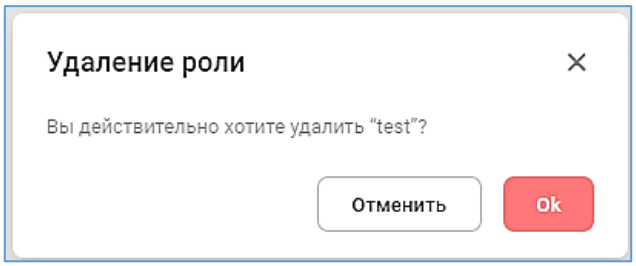

Рисунок 9.17 – Окно «Удаление роли»

Корректное удаление роли доступно после снятия назначенных привилегий и переназначения владельца созданных объектов от имени и с правами удаляемой роли. В силу указанной причины, если зависимости существуют, то компонент выведет окно сообщения «Конфликты зависимостей».

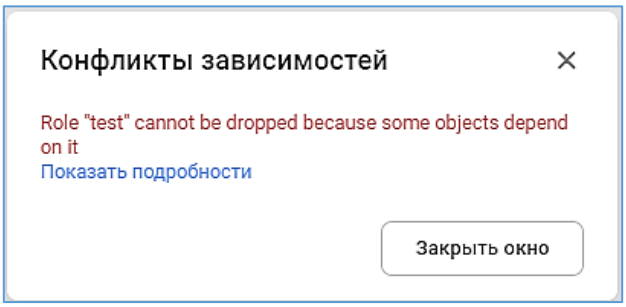

Рисунок 9.18 - Окно сообщения «Конфликты зависимостей»

Нажатие на гиперссылку «Показать подробности» расширит окно. В окне будут показаны объектовые привилегии и SQL-команда для снятия зависимостей. SQL-команду возможно скопировать в буфер обмена через пиктограмму.

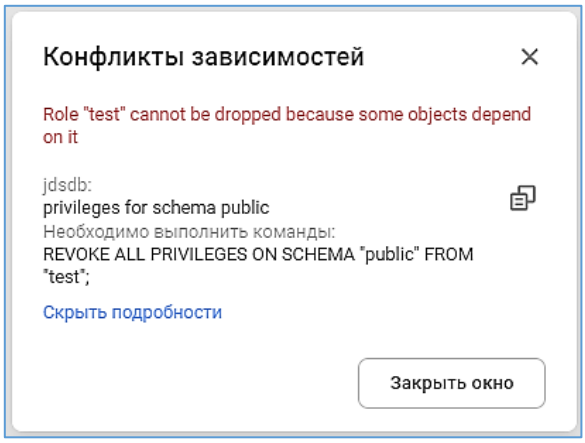

Рисунок 9.19 – Окно «Конфликты зависимостей» с выводом подробной информации

9.6. Псевдороль «Public»

Псевдороль «Public» первой отображается в общем списке ролей и имеет статус «System». Для нее недоступна операция удаления, но возможно снятие/назначение привилегий.

10. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «СПИСОК СОБЫТИЙ» (EVENT LIST)

«Список событий» предназначен для просмотра событий безопасности каждой из установок (instans) СУБД.

Вкладка Event List служит для просмотра событий выбранного сервера СУБД с целью:

— обнаружения ошибок в работе СУБД;

— получения отладочной информации;

— выявления и расследования инцидентов безопасности;

— получения информации о действиях отдельных пользователей, как рядовых пользователей, так и администраторов (РСБ.8), в том числе полнотекстовой записи привилегированных команд (РСБ.2а).

JDS обладает функциональной возможностью централизованного сбора и просмотра событий с целевых СУБД. События собираются в служебной БД JDS.

Подробно настройка сбора событий СУБД описано в документе «Руководство по настройке. Часть 12. Централизованный сбор записей событий СУБД. Компонент «ja_Log». 643.72410666.00067-07 98 01-12».

Компонент автоматически определит СУБД с установленным Созданную базу данных для хранения событий СУБД надо добавить, как цель (Target) в JDS. Тогда раздел «Event List» сможет загрузить события СУБД.

10.1. Выбор служебной БД

Выбор служебной БД выполняется нажатием кнопки выпадающего списка выбора цели, расположенной в правом верхнем углу окна.

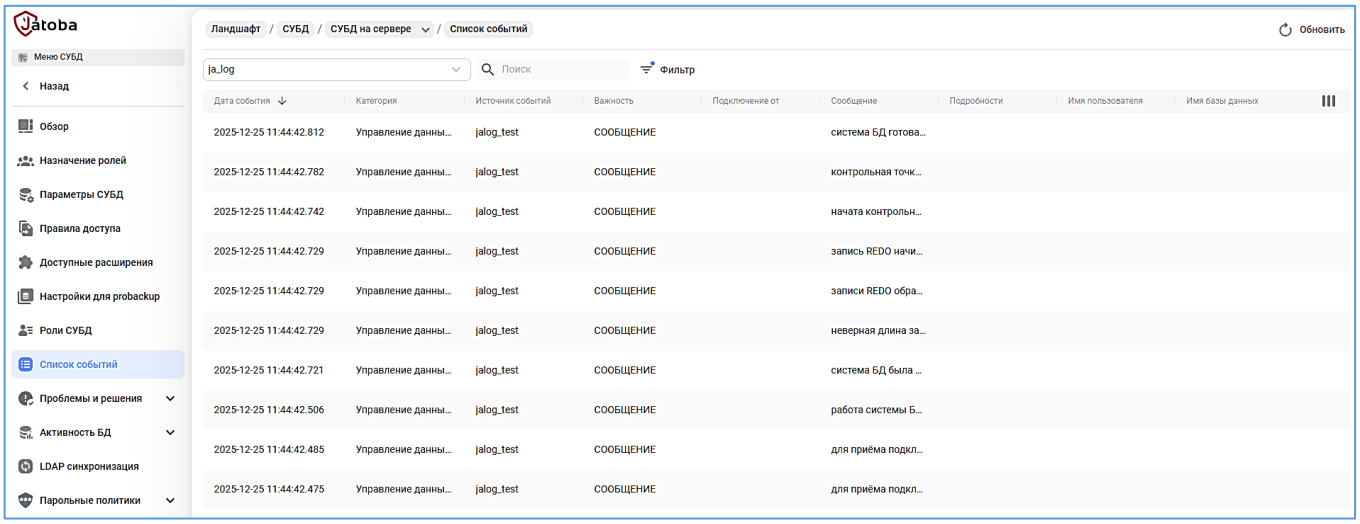

Рисунок 10.1 – Вкладка «Список событий»

Корректная работа раздела обеспечивается установленным компонентом «ja_Log» версией не ниже 2.0. В противном случае компонент выдаст предупреждение и удалит неактуальный элемент цели.

В разделе «Список событий» (Event List) возможно выбрать только один сервер СУБД.

Цель добавляется через раздел «Ландшафт». В случае если компонент ранее был установлен на хосте, то в целях добавится автоматически. При удалении компонента, цель удаляется из выпадающего списка целей.

10.2. Фильтр событий

По умолчанию компонент отобразит список событий за последний месяц. Данный параметр установлен по умолчанию в фильтре событий. Используемые поля и их параметры приведены в таблице 10.1.

Таблица 10.1 – Поля фильтра событий

Наименование	Наименование ENG	Тип поля	Обязат.	Ограничения (max)	Значение по умолчанию
Дата события	Event date	календарь для выбора периода	X	1 мес.	Сегодня
Цель	Target	выпадающий список	–		
Важность	Severity	выпадающий список	–		
Категория	Category	выпадающий список	–		

Наименование	Наименование ENG	Тип поля	Обязат.	Ограничения (max)	Значение по умолчанию
Имя БД	Database name	текстовое	—	20	
Имя пользователя	User name	текстовое	—	20	
Имя приложения	Application name	текстовое	—	20	
Подключение от	Connection from	текстовое	—	30	
SQLstate код	SQLstate code	текстовое	—	8	

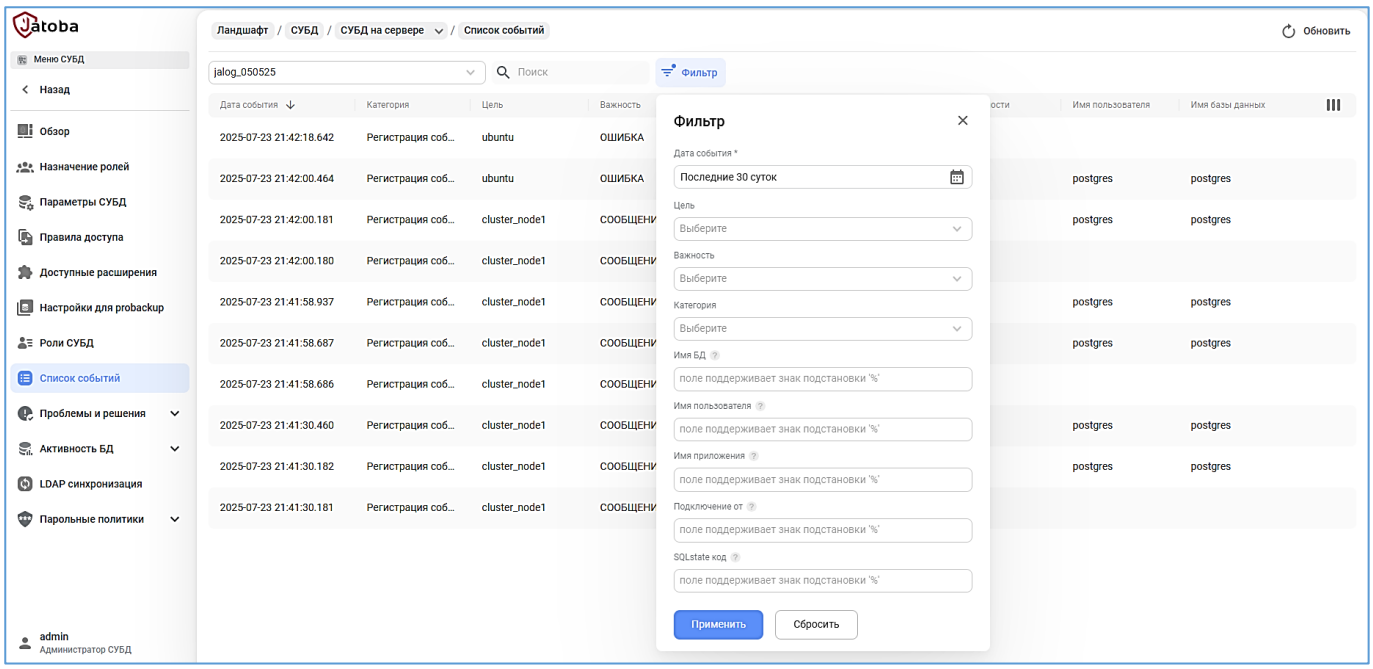

Рисунок 10.2 – Фильтр событий

Дата события

Поле «Дата события» имеет календарь, в котором предустановлены периоды:

— Свой период;

— Последний 1 час;

— Последние 6 часов;

— Последние 24 часа;

— Последние 2 суток;

— Последние 7 суток;

— Последние 30 суток;

— Сегодня;

— Вчера;

— Текущая неделя;

— Прошлая неделя.

Цель

СУБД «Jatoba» с компонентами «ja_Log» и «JDS» обеспечивают централизованный сбор событий безопасности. Поэтому в журнале аудита регистрируется имя хоста СУБД для последующей его идентификации.

В поле «Цель» допустимо выбрать одну или все цели, либо оставить поле пустым.

Важность

В поле «Важность» допустимо выбрать одно или все значения, либо оставить поле пустым.

Выбираются значения:

— Отладка;

— Сообщение;

— Информация;

— Замечание;

— Предупреждение;

— Ошибка;

— Важно;

— Паника.

Категория

В поле устанавливается выбор событий по следующим категориям, которые соответствуют мерам защиты информации:

— Управление доступом (УПД);

— Идентификация (ИАФ);

— Управление данными;

— Контроль целостности (ОЦЛ);

— Регистрация событий безопасности (РСБ);

— Кластеризация (ОДТ);

— Резервное копирование (ОДТ);

— Прочее;

— Контроль целостности данных (ОЦЛ).

SQLstate код

Доступно использование знака подстановки «%» для замены любого количества любых символов, в полях фильтра списка событий.

10.3. Просмотр списка событий

Установленный временной диапазон сформирует список событий (рис. 10.3).

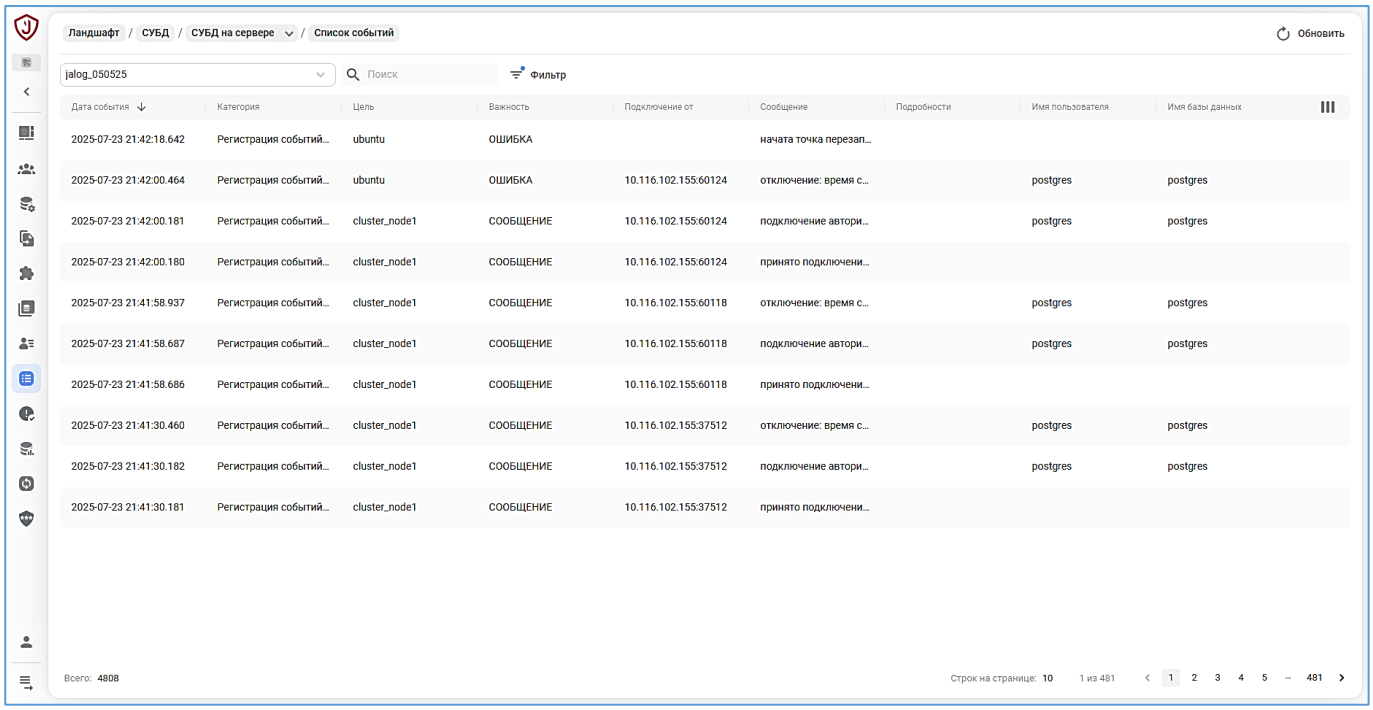

Рисунок 10.3 – Список событий

В правой нижней части окна расположены пиктограммы страниц списка событий.

10.4. Выбор столбцов (Columns)

Пиктограмма «Столбцы» (Columns) расположена в правом верхнем углу окна.

При нажатии на которую раскроется меню с списком столбцов, приведенных в таблице 10.2.

Таблица 10.2 – Список столбцов

Наименование (RU)	Наименование (ENG)	По умолчанию
Идентификатор события	**ID**	X
Категория события	**Category**	X
Цель	**Target**	X
Дата события	**Event data**	X
Важность	**Severity**	X
Подключение от	**Connection from**	X
Сообщение	**Message**	X
Подробности	**Detail**	X
Имя пользователя	**User name**	X
Имя базы данных	**Database name**	X
Время вставки в лог	**LOG insertion time**	
Идентификатор процесса	**Process ID**	
Идентификатор сессии	**Session ID**	
Номер строки каждой сессии	**Per-session line number**	
Тег команды	**Command tag**	
Время начала сессии	**Session start time**	
Виртуальный идентификатор транзакции	**Virtual transaction ID**	
Идентификатор транзакции	**Regular transaction ID**	
SQLSTATE Код	**SQLSTATE code**	
Подсказка	**Hint**	
Внутренний запрос	**Internal query that led to the error**	
Номер символа внутреннего запроса, где произошла ошибка	**Internal query character number where the error occurred**	
Контекст	**Error context**	
Запрос пользователя	**User query that led to the error**	
Номер символа в запросе пользователя	**User query character number where the error occurred**	
Расположение ошибки в исходном коде	**The location of the error in the PostgreSQL source code**	
Имя приложения	**Application name**	
Тип процесса СУБД	**DBMS process type**	

Соответствие событий СУБД категориям мер защиты приказов ФСТЭК России приведено в Приложении к документу «Реализация функций безопасности»

Выбор столбцов осуществляется установкой флажков.

При использовании расширения «pgAudit» в столбец «Message» включаются дополнительные столбцы, представленные в таблице 10.3.

Таблица 10.3 – Структура столбца «Error message»

Наименование основного столбца	Наименование дополнительного столбца	Описание
Error message		Сообщение об ошибке
	Event recording type	Тип записи события
	Expression No.	№ выражения
	Subexpression No.	№ подвыражения
	Event class	Класс события
	SQL operation	SQL - операция
	DB object type	Тип объекта БД
	DB object name	Имя объекта БД
	Full text of the SQL query (script)	Полный текст SQL-запроса (скрипта)
	SQL query parameters (script)	Параметры SQL-запроса (скрипта)

10.5. Сортировка списка событий

Сортировка событий возможна по каждому выбранному столбцу и вызывается нажатием на выбранный столбец:

— 1 нажатие – сортировка по возрастанию;

— 2 нажатия – сортировка по убыванию;

— 3 нажатия – отмена сортировки.

10.6. Полнотекстовый поиск событий

Полнотекстовый поиск событий осуществляется через строку поиска, представленную на рисунке 10.4. В поиск включаются все столбцы таблицы, включая не отображаемые в текущий момент. Запись отображается при условии, что:

— условие выполняется хотя бы для одного из столбцов;

— выполняется и условия поиска, и условия фильтрации.

Поиск ограничивается 30 регистронезависимыми символами.

События фильтруются по нажатию клавиши «Ввод».

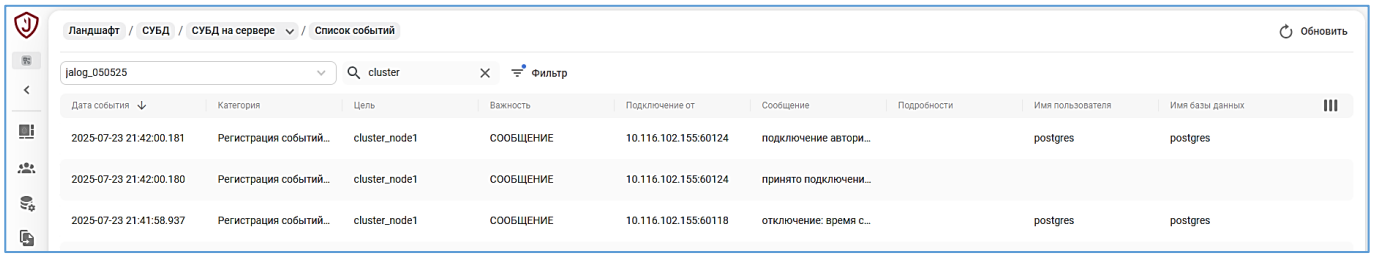

Рисунок 10.4 – Строка поиска и вывод

11. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «ПРОБЛЕМЫ И РЕШЕНИЯ» (PROBLEMS & SOLUTIONS)

«Problems & Solutions» это инструмент, который позволяет определять ряд проблем, существующих в целевой СУБД. Для определения проблемы созданы скрипты (скрипт обнаружения) и для исправления проблемы – динамические скрипты (шаблон таблетки).

Функциональные возможности подраздела доступны на уровне целевой СУБД в разделе «Ландшафт».

11.1. Вкладка «Правила сканирования»

При первом открытии вкладки компонент JDS предложит создать первое правило сканирования.

Нажатие на пиктограмму «Создать» вызовет окно «Создание правила сканирования».

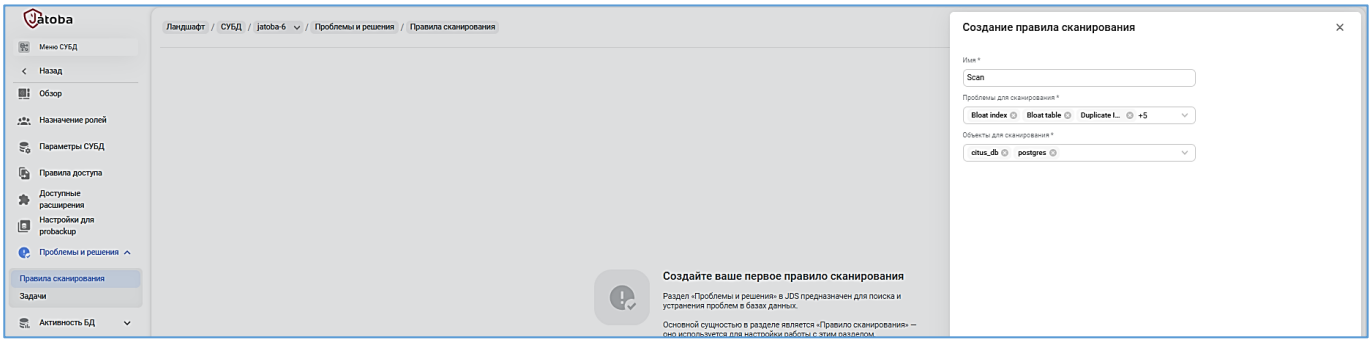

Рисунок 11.1 – Выпадающий список проблем для сканирования

В выпадающем списке доступен множественный выбор проблем для сканирования, представленных в таблице 11.1.

Таблица 11.1 – Перечень определяемых проблем в СУБД

Проблемы	Описание проблемы
Bloat index	Индекс, занимающий дополнительное пространство
Bloat table	Таблица фрагментирована и занимает дополнительное пространство
Duplicate index	Дублированные индексы, занимающие дополнительное пространство
Missing Foreign Key index	Пропущенный индекс внешнего ключа
Missed index	Пропущенный индекс, который может привести к снижению производительности табличных запросов
Not analyzed table	Не анализированные таблицы более 100 дней
Not vacuumed table	Таблица дефрагментирована и содержит много мертвых строк
Sequence Limit	Предел последовательности

Проблемы	Описание проблемы
Unused index	Давно не использованные индексы, переполненные таблицы

Следующим шагом выбираются объекты сканирования.

В качестве объектов сканирования могут быть базы данных целиком и/или схемы данных. При выборе объектов доступен множественный выбор.

Правило сканирования сохраняется нажатием на кнопку «Сохранить».

Созданные правила сканирования отображаются в общем списке.

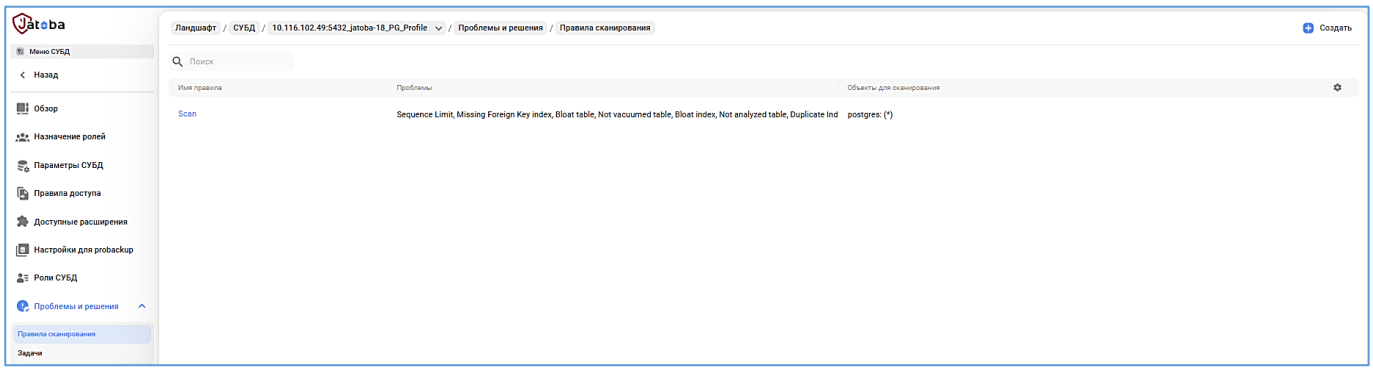

Рисунок 11.2 – Список созданных правил сканирования

11.2. Режим сканирования

Переход в режим сканирования выполняется при нажатии на гиперссылку в имени правила сканирования в одноименной вкладке.

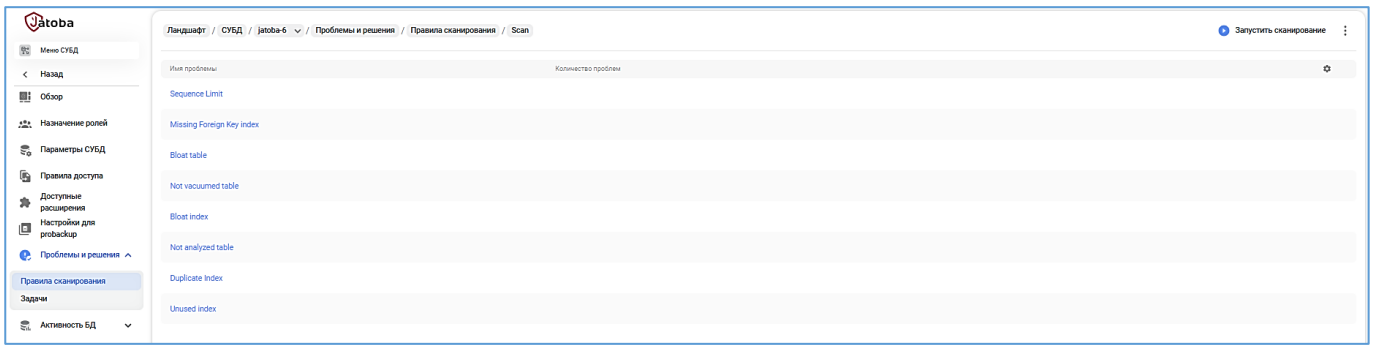

Рисунок 11.3 – Вкладка «Результаты сканирования»

Сканирование возможно:

– По всем проблемам через пиктограмму «Запустить сканирование» находящейся в правом верхнем углу окна;

– Выборочное сканирование через одноименную пиктограмму в строке проблемы.

В случае если сканирование проводилось ранее, то просмотреть результаты возможно через нажатие на гиперссылку в имени проблемы.

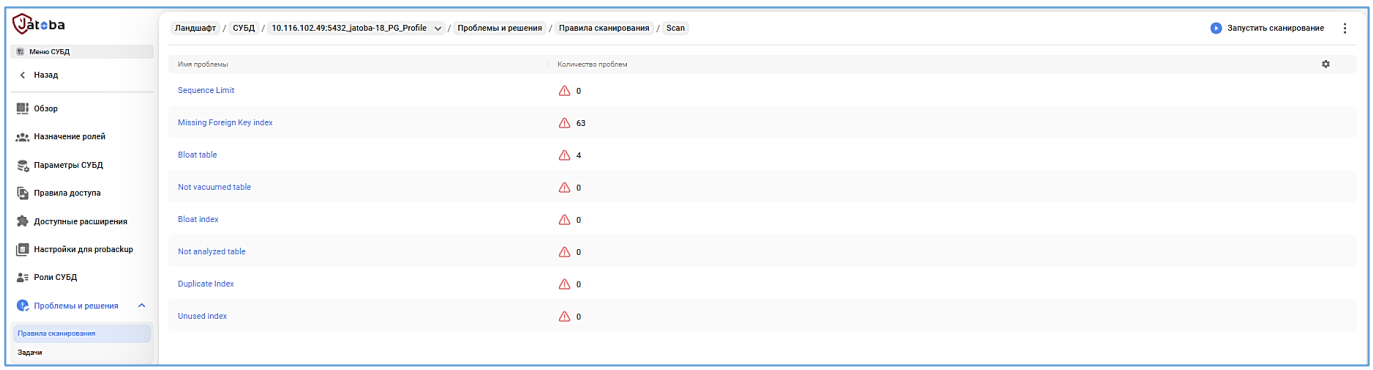

Рисунок 11.4 – Список ранее найденных проблем

Для выявленных проблем отображается их статус в виде пиктограмм.

Таблица 11.2 – Описание пиктограмм

Пиктограмма	**Описание**
	Найдена проблема
	Запланировано исправление
	Поставлена в очередь
	Исправление запущено

Для проблемы «Duplicate Index» отображается дополнительная информация об объектах

Перейдя в по гиперссылке имени проблемы отобразится их перечень, в котором доступен поиск по любым значениям.

При сканировании объектов компонент определяет возможные варианты исправления. В результате, компонент предоставляет предопределённый, оптимальный вариант решения и предоставляет выбор решения проблемы пользователю.

Варианты решения проблем представлены на схеме 11.5.

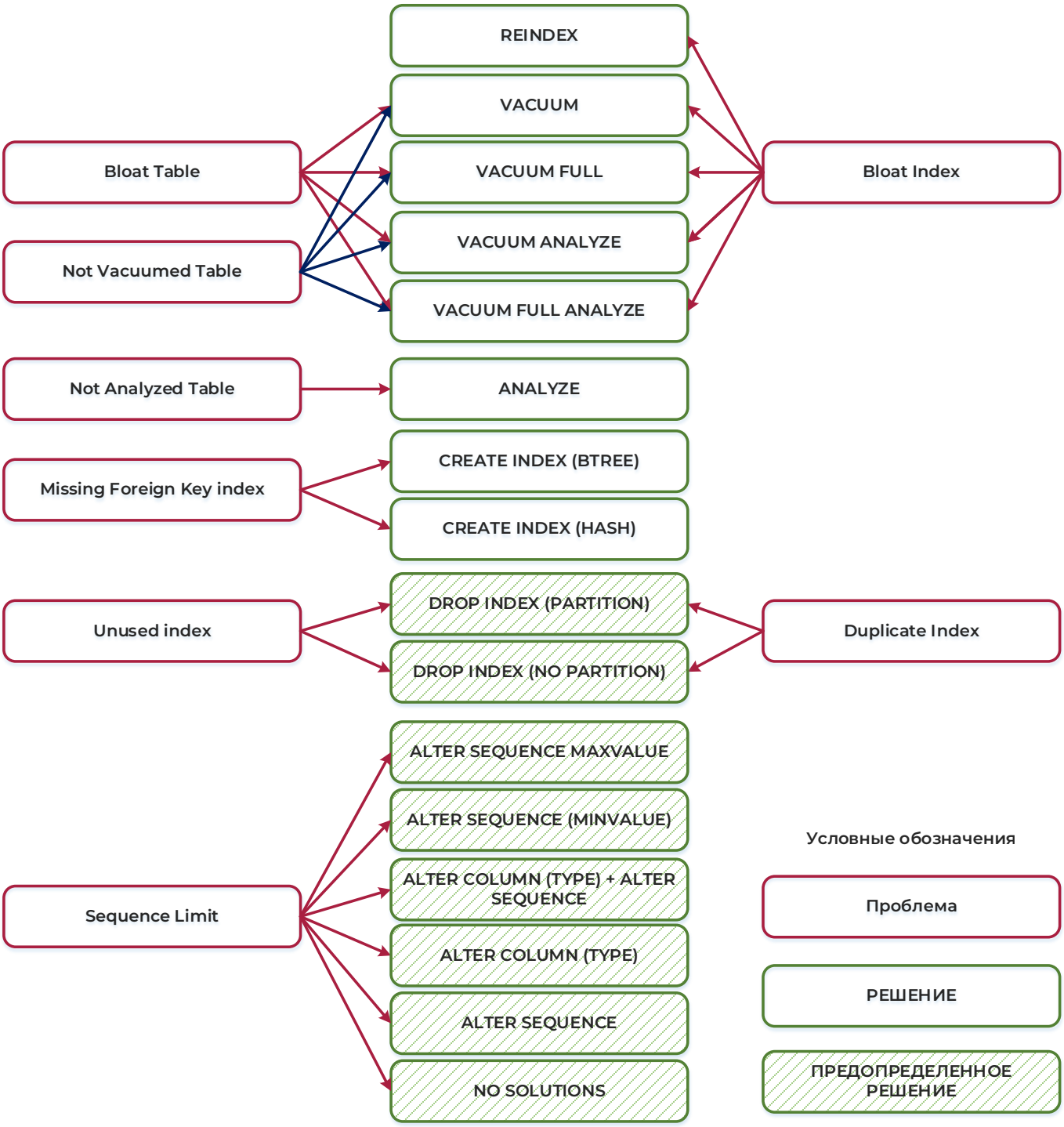

Рисунок 11.5 – Схема возможных вариантов исправления

Каждая из найденных проблем лечится индивидуально, т.к. требует квалифицированного подхода. Для этого необходимо нажать на строке проблемы. Тем самым вызвать окно «Исправление проблемы».

В открывшимся окне доступен:

— выбор параметров исправления;

— просмотр SQL-команды исправления;

— выбор временного диапазона выполнения задачи;

— указание комментария.

При установленном флаге «Выполнить сейчас» задача исправления выполнится немедленно.

Снятый флаг активирует установку даты и времени выполнения исправления в календаре.

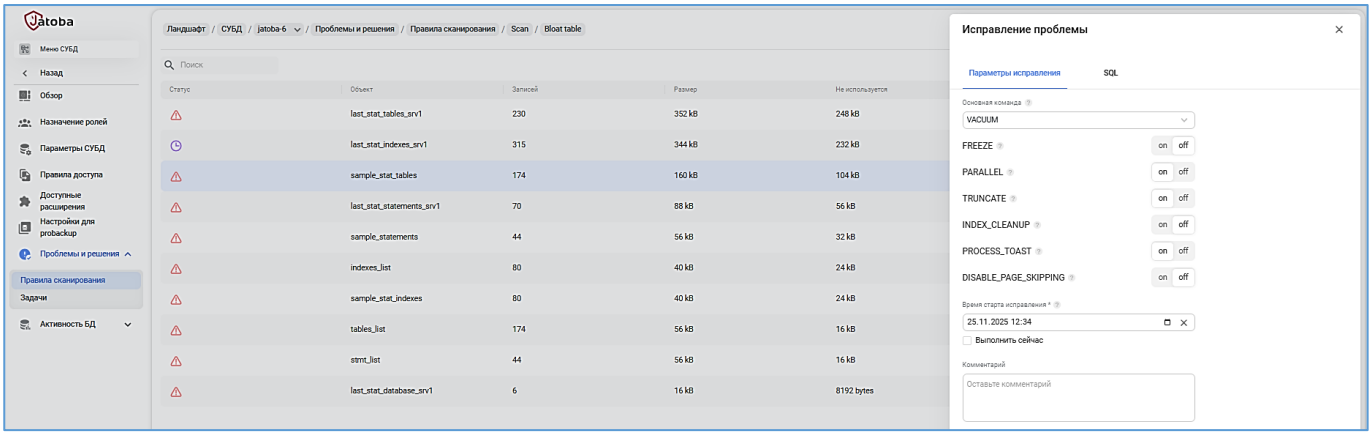

Рисунок 11.6 – Установка параметров и даты исправления проблемы

Каждый из параметров окна оснащен интерактивной подсказкой.

Для каждой проблемы предоставляются разработанные варианты исправления.

SQL-команды отображаются во вкладке SQL и не доступны для редактирования.

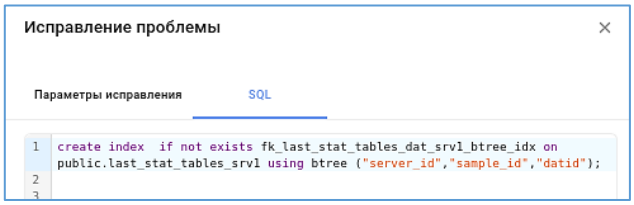

Рисунок 11.7 – Отображение выполняемых SQL-команд

11.3. Вкладка «Задачи»

Выбранные проблемы для исправления передаются в общий список на вкладке «Задачи».

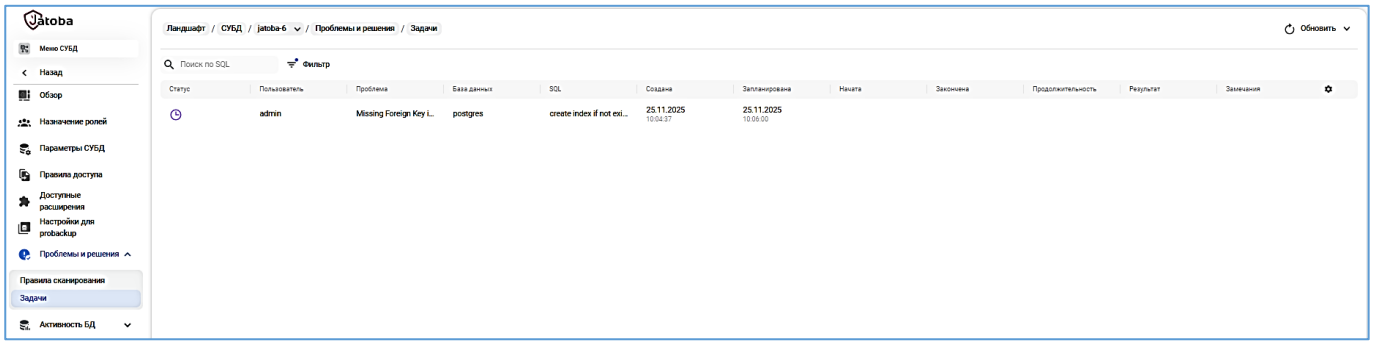

Рисунок 11.8 – Список задач на вкладке «Задачи»

В списке задач доступно:

— выполнить контекстный поиск по SQL через поле «Поиск»;

— отфильтровать список через меню «Фильтр»;

— просмотреть информацию о продолжительности выполнения задачи;

— обновить список задач или установить автоматическое обновление во временном диапазоне:

- 30 секунд;
- 1 минута;
- 5 минут.

В меню «Фильтр» доступен выбор по полям:

— Пользователи;

— Проблемы;

— Статусы;

— Создана;

— Запланирована;

— Начата.

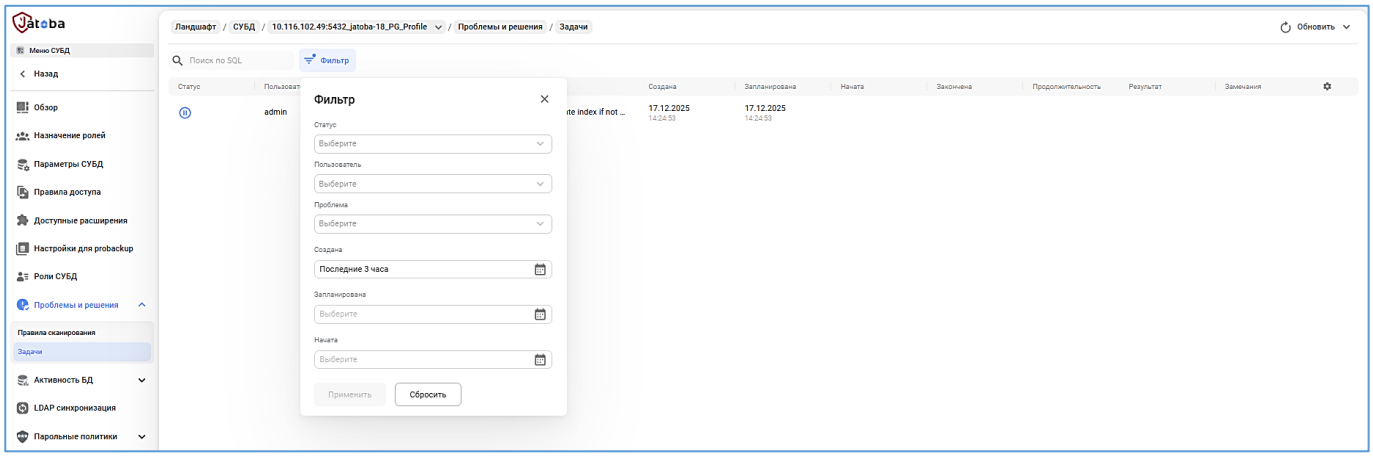

Рисунок 11.9 – Окно «Фильтр»

Задачи в списке могут иметь статус:

— Запланирована;

— Поставлена в очередь;

— Запущена;

— Завершена успешно;

— Завершена с предупреждением;

— Завершена с ошибкой;

— Отменена.

В поле выбора периода отображения задач по умолчанию установлен период «Последние 3 часа».

Доступен выбор параметров:

— Свой период;

— Последние 5 минут;

— Последние 20 минут;

— Последний 1 час;

— Последние 3 часа;

— Последние 6 часов;

— Последние 12 часов;

— Последние 24 часа;

— Последние 7 суток;

— Последние 30 суток

— Сегодня;

— Сегодня до наст. момента;

— Вчера;

— Этот день на прошлой неделе;

— Текущая неделя;

— Текущая неделя до наст. момента;

— Прошлая неделя.

В случае, когда задача завершилась с ошибкой, при клике на неё открывается окно с основными параметрами, рекомендациями и пояснениями в силу каких причин исправление не было произведено.

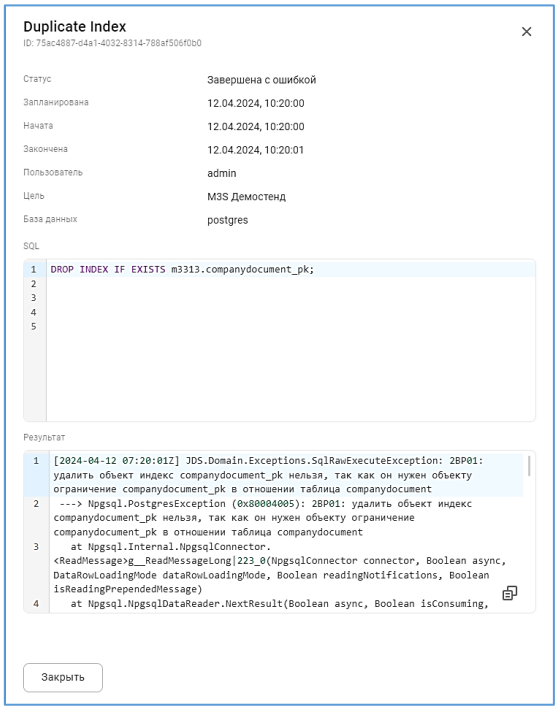

Рисунок 11.10 – Общая информация о задаче и рекомендациями по исправлению

В случае, когда временные затраты на исправление проблемы велики, исправление проблемы выполняется в асинхронном режиме используя функциональные возможности службы «jds-doctor.service», вне зависимости от активности компонента JDS.

Запланированную задачу возможно отменить, нажав на нее в списке задач и в открывшемся окне, нажав кнопку «Отменить задачу».

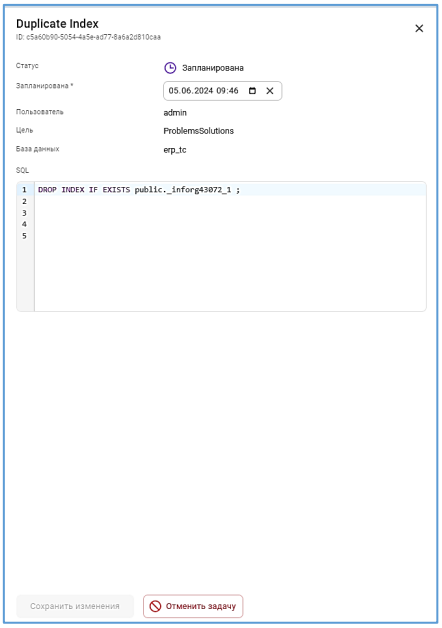

Рисунок 11.11 – Отмена запланированной задачи

При этом обязательно указывается комментарий с причинами отмены в одноименном поле во всплывающем окне «Отмена задачи».

Задачи со статусом «Поставлена в очередь» и «Запущена» отменить нельзя

Задачи со статусом «Запланирована» доступны для редактирования.

11.4. Работа нескольких пользователей с подразделом «Проблемы и решения» (Problems & Solutions)

Подраздел «Проблемы и решения» (Problems & Solutions) может быть доступен пользователям, имеющим административные функции в СУБД и имеющим доступ к разделу.

При входе в подраздел станут доступны созданные конфигурации и рекомендации для исправления.

Рекомендации для исправления отображаются для всех пользователей, имеющих доступ к разделу «Проблемы и решения» (Problems & Solutions) и доступны функциональные возможности по решению обнаруженных проблем.

12. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «АКТИВНОСТЬ БД» (DB ACTIVITY)

Вкладка «Активность БД» (DB Activity) предназначена 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.

Вкладка доступна в разделе «Ландшафт» при переходе на уровень СУБД.

12.1. Вкладка «Сессии» (Session)

При выборе цели компонент JDS автоматически отобразит текущие сессии.

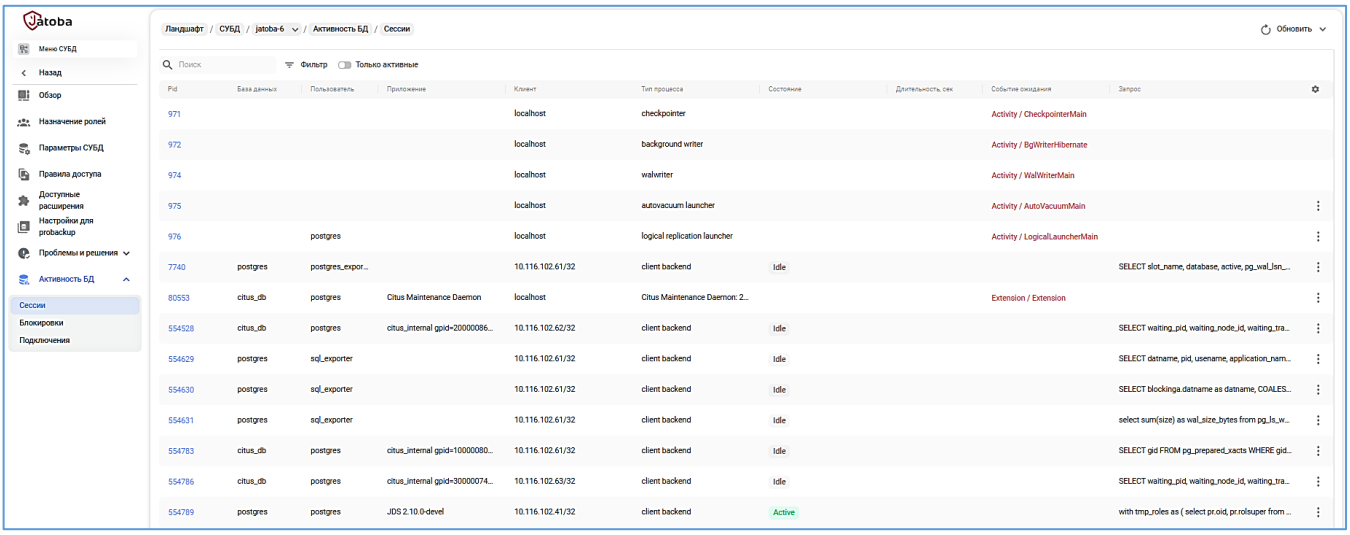

Рисунок 12.1 – Отображение текущих сессий

В вкладке «Сессии» отображаются столбцы, представленные в таблице 12.1.

Таблица 12.1 – Столбцы вкладки «Сессии»

Название (RU)	**Название (ENG)**	**Описание**	**Значения поля**
Pid	Pid	Идентификатор процесса	
БД	Database	Имя БД, к которой подключен процесс	
Пользователь	User	Имя подключенного пользователя	
Приложение	Application	Вывод названия приложения (application_name) и/или версии приложения (application_version)	
Клиент	Host	IP-адрес или имя компьютера клиента	
Тип процесса	Backend type	Тип процесса	
Состояние	State	Текущее состояние	Таблица 12.2
Длительность, сек	Duration, s	Длительность работы последней команды, сек	
Событие ожидания	Wait event	Тип события ожидания / имя события ожидания	Таблица 12.3
Запрос	Query	Текст последнего запроса	

Столбцы возможно показать или скрыть через пиктограмму «Выбор столбцов» (Columns), расположенную в верхнем правом углу вкладки.

По умолчанию будут активны все столбцы.

Поле «Состояние» (State) может принимать значения, приведенные в таблице 12.2.

Таблица 12.2 – Возможные значения поля «Состояние» (State)

Значение	Описание
active	Серверный процесс выполняет запрос
idle	Серверный процесс ожидает новой команды от клиента
idle in transaction	Серверный процесс находится внутри транзакции, но в настоящее время не выполняет никакой запрос
idle in transaction (aborted)	Серверный процесс находится внутри транзакции, но один из операторов в транзакции вызывал ошибку
fastpath function call	Серверный процесс выполняет fast-path функцию
disabled	Серверный процесс отключен

Для сессий в статусе «idle» значения этих полей должны быть пустыми.

Поле «Событие ожидания» (Wait event) может принимать значения, приведённые в таблице 12.3.

Таблица 12.3 – Типы событий ожидания

Тип события ожидания	Описание
Activity	Серверный процесс простаивает. Состояние «Activity» показывает, что процесс ожидает активности в основном цикле обработки
BufferPin	Серверный процесс ожидает исключительного доступа к буферу данных
Client	Серверный процесс ожидает в сокете некоторую активность пользовательского приложения. Сервер ждёт наступления события, не зависящее от его внутренних процессов
Extension	Серверный процесс ожидает условия, возникающего в модуле расширения
IO	Серверный процесс ожидает завершения операции ввода/вывода
IPC	Серверный процесс ожидает взаимодействия с другим процессом
Lock	Серверный процесс ожидает тяжёлую блокировку
LWLock	Серверный процесс ожидает лёгкую блокировку
Timeout	Серверный процесс ожидает истечения определённого времени. В поле «wait_event» обозначается конкретное место ожидания

В правом верхнем углу вкладки располагается пиктограмма «Обновить».

Нажатие на нее обновит отображаемые значения на вкладке. Вызвав контекстное меню пиктограммы «Обновить» возможно установить автообновление вкладки через интервалы времени:

— 1 секунда;

— 5 секунд;

— 10 секунд;

— 30 секунд;

— 60 секунд.

На вкладке «Сессии» доступны следующие виды сортировки:

— «Фильтр»;

Фильтр выполняет фильтрацию по полям «База данных», «Пользователь» и «Тип процесса» с возможностью поиска значения и множественного выбора.

— Тумблер «Только активные»;

По умолчанию тумблер выключен, т.е. выводятся все сессии. Установкой тумблера в активный режим отсортирует список сессий, имеющих статус «Active».

- Сортировка вывода;

Каждый из столбцов вкладки, указанный в таблице 12.1, имеет функциональную возможность прямой и обратной сортировки пользователем.

12.1.1. Завершение сессии (End session)

Завершении сессии доступно:

— из контекстного меню строки таблицы;

— при клике на строку сессии.

В правой части вкладки откроется дополнительное окно с вспомогательными полями, представленными в таблице 12.4.

Таблица 12.4 – Вспомогательные поля окна завершения сессии на вкладке «Сессии»

Название (RU)	Название (ENG)	Описание
Запрос	Query	Текст запроса
База данных	Database	Имя БД, к которой подключен процесс
Пользователь	User	Имя подключенного пользователя
Приложение	Application	Название приложения
Клиент	HOST	Хост клиента
Тип процесса	Backend type	Тип процесса
Состояние	State	Текущее состояние сессии
Длительность	Duration, s	Длительность работы последней команды, сек

Название (RU)	Название (ENG)	Описание
Запрос	Query	Текст запроса
Тип события ожидания	Wait event type	Тип события, которого ждёт обслуживающий процесс
Событие ожидания	Wait event	Тип события ожидания / имя события ожидания
ID базы данных	DB ID	OID базы данных, к которой подключен процесс
IP-адрес клиента	Client address	IP-адрес клиента
Порт клиента	Client port	Номер TCP-порта, который используется клиентом для соединения с этим процессом
Компьютер клиента	Client host	Имя компьютера клиента
Запуск процесса	Backend start	Время запуска процесса
Начало транзакции	Xact start	Время начала текущей транзакции
Начало запроса	Query start	Время начала выполнения активного/последнего запроса
Изменение состояния	State change	Время последнего изменения состояния (поля state)
ID верхнего уровня транзакции	Backend xid	Идентификатор верхнего уровня транзакции

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

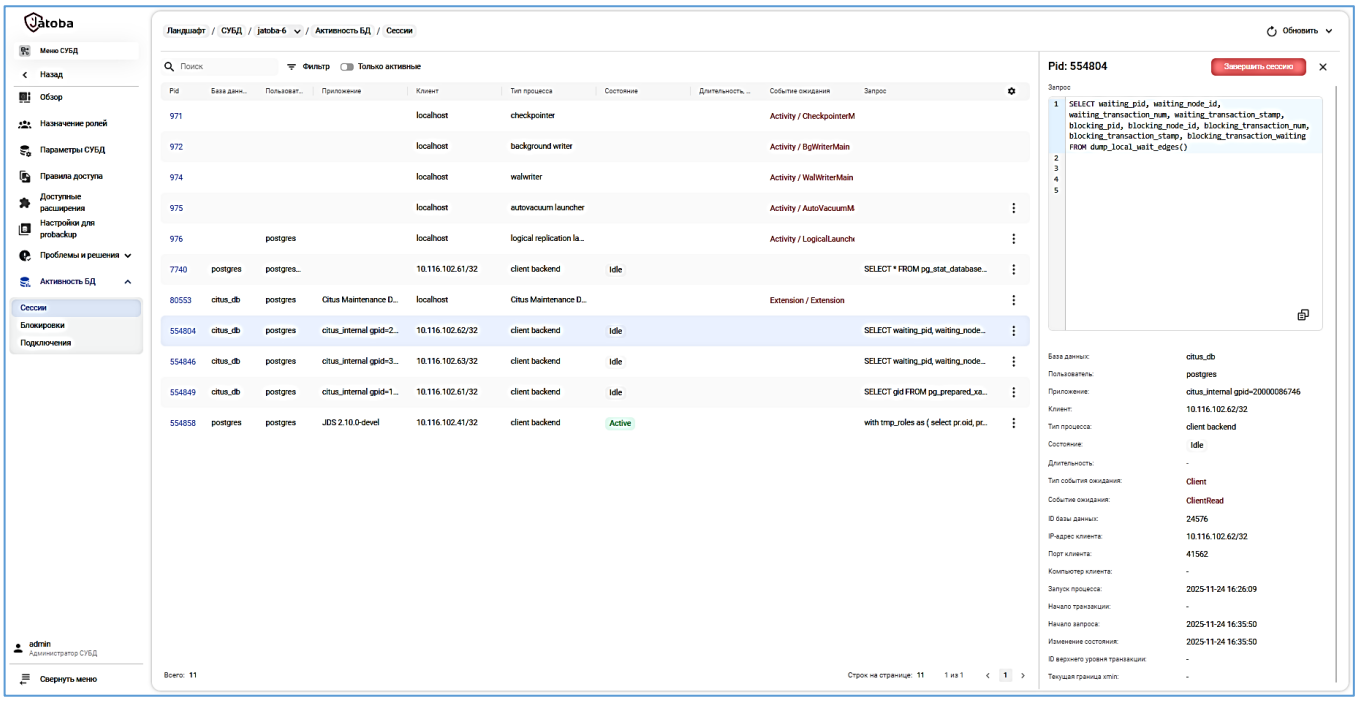

Рисунок 12.2 – Дополнительное окно «Завершение сессии» в вкладке «Сессии»

Нажатие на кнопку «Завершение сессии» (End session) вызовет окно подтверждения действия «Завершение сессии» (Session ending).

Подтвердив действие, выбранная сессия завершится.

Компонент различает служебные, серверные и клиентские запросы. В случае, если завершение процесса может привести к неработоспособности СУБД или компонента «JDS», будет выведено акцентированное сообщение.

12.2. Вкладка «Блокировки» (Locks)

На вкладке «Блокировки» отображаются заблокированные сессии в СУБД.

После выбора цели в вкладе «Блокировки» автоматически отобразятся существующие блокировки в СУБД.

На вкладке «Блокировки» отображаются столбцы, представленные в таблице 12.5.

Таблица 12.5 – Основные отображаемые поля вкладки «Блокировки»

Название (RU)	Название (ENG)	Описание
Pid	Pid	Идентификатор процесса
Длительность, сек	Duration, s	Длительность работы последней команды, сек
Событие ожидания	Wait event	Тип события ожидания / имя события ожидания
Пользователь	User	Имя подключенного пользователя
Приложение	Application	Название приложения
Удерживаемый / запрошенный режим	Inquired / lock mode	Запрошенный режим блокировки для блокируемых сессий, удерживаемый – для корневых
Состояние	State	Текущее состояние сессии
БД	Database	Имя БД, к которой подключен процесс
Запрос	Query	Текст последнего запроса

Столбцы возможно показать или скрыть через пиктограмму «Выбор столбцов» (Columns), расположенную в верхнем правом углу вкладки, аналогично как описано в п. 12.1.

Одни сессии могут блокировать работу других сессий и представлены в виде уровней зависимостей (иерархии).

12.2.1. Завершение заблокированной сессии

Завершении сессии доступно при клике на строку сессии. В правой части вкладки откроется дополнительное окно с вспомогательными полями, представленными в таблице 12.6.

Таблица 12.6 – Вспомогательные поля окна завершения сессии на вкладке «Блокировки»

Название (RU)	Название (ENG)	Описание
Длительность	Duration, s	Длительность работы последней команды, сек
Тип события ожидания	Wait event type	Тип события, которого ждёт обслуживающий процесс
Событие ожидания	Wait event	Тип события ожидания / имя события ожидания
пользователь	User	Имя подключенного пользователя
Приложение	Application	Название приложения
Удержание / запрошенный режим	Inquired / lock mode	Запрошенный режим блокировки для блокируемых сессий, удерживаемый – для корневых
Состояние	State	Текущее состояние сессии
База данных	Database	Имя БД, к которой подключен процесс
Кем заблокирован (pid)	Locked by pid	Pid блокирующей сессии
Режим блокировки	Locked by mode	Режим блокировки блокирующей сессии
Тип блокировки	Lock type	Тип блокируемого объекта
Объект	Object	Имя объекта, являющегося целью блокировки
ID отношения	Relation	OID отношения, являющегося целью блокировки
Страница	Page	Номер страницы в отношении, являющейся целью блокировки
Кортеж	Tuple	Номер кортежа на странице, являющегося целью блокировки запроса
Виртуальный ID транзакции	Virtual xid	Виртуальный идентификатор транзакции, являющийся целью блокировки
ID транзакции	Transaction ID	Идентификатор транзакции, являющийся целью блокировки
ID системного каталога	Class ID	OID системного каталога, содержащего цель блокировки
ID цели	Object ID	OID цели блокировки в соответствующем системном каталоге
Номер столбца	Object subid	Номер столбца, являющегося целью блокировки (на саму таблицу указывают classid и objid), ноль, если это некоторый другой обычный объект базы данных
ID базы данных	DB ID	OID базы данных, к которой подключен процесс
IP-адрес клиента	Client address	IP-адрес клиента
Порт клиента	Client port	Номер TCP-порта, который используется клиентом для соединения с этим процессом
Компьютер клиента	Client hostname	Имя компьютера клиента
Начало транзакции	Xact start	Время начала текущей транзакции

Название (RU)	Название (ENG)	Описание
Начало запроса	Query start	Время начала выполнения активного/последнего запроса
Изменение состояния	State change	Время последнего изменения состояния (поля state)
ID верхнего уровня транзакции	Backend xid	Идентификатор верхнего уровня транзакции

Нажатие на кнопку «Завершение сессии» (End session) вызовет окно подтверждения действия «Завершение сессии» (Session ending).

Тем самым вызовется функция СУБД «pg_terminate_backend», которая завершает процесс с указанным PID.

Подтвердив действие, выбранная сессия завершится.

12.3. Вкладка «Подключения»

Вкладка «Подключения» отображает количество подключений к выбранной СУБД, позволяя выполнить меру безопасности, установленную Приказом № 17 ФСТЭК России:

<u>Мера защиты УПД.9 (3) в части следующих требований:</u>

— контроль и отображение администратору числа активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей.

После выбора цели отображаются столбцы:

— «Пользователь/роль»;

— «Количество подключений»;

— «Квота подключений».

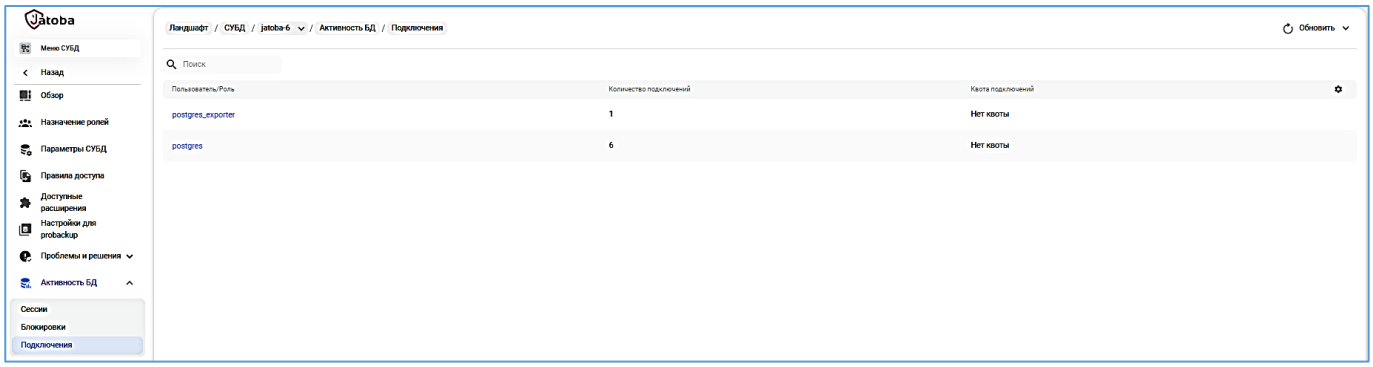

Рисунок 12.3 – Вкладка «Подключения»

Имена пользователей отражены в виде активной ссылки, при нажатии на которую:

— произойдет переключение на вкладку «Сессии» (см. п. 12.1);

— автоматически установится фильтр по выбранному пользователю.

В правом верхнем углу расположена кнопка «Обновить» с выпадающим списком выбора времени автоматического обновления отображаемой информации.

Окно поиска

Окно поиска расположено в левом верхнем углу вкладок «Сессии» и «Блокировки». Поиск выполняется по буквенным, числовым значениям, по всем столбцам.

13. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «LDAP СИНХРОНИЗАЦИЯ» (LDAP SYNC)

Вкладка «LDAP синхронизация» (LDAP Sync) является графическим интерфейсом компонента «ja_Sync_LDAP», предназначенного для синхронизации учетных записей групп пользователей активного каталога с учетными записями СУБД.

Перед работой с данным подразделом необходимо ознакомиться с документацией:

— «Руководство администратора. 643.72410666.00067-07 95 01»;

— «Руководство по настройке. Часть 2. Контроль субъектов доступа. Компонент «Jatoba data vault». 643.72410666.00067-07 98 01-02»;

— «Руководство по настройке. Часть 8. Синхронизация учетных записей служб каталогов и СУБД. Компонент «ja_Sync_LDAP». 643.72410666.00067-07 98 01-08».

Параметры кластера отображаются на уровне службы «jadog». Для просмотра параметров кластера необходимо перейти по пути: Раздел Ландшафт → СУБД → Дерево инфраструктуры → Хост → СУБД → Служба jadog.

Вкладка «LDAP синхронизация» отображается на уровне СУБД. Для работы с вкладкой необходимо перейти по пути: Раздел Ландшафт → СУБД → Дерево инфраструктуры → Хост → СУБД → LDAP синхронизация.

Настройка синхронизации учетных записей служб каталогов с СУБД описана в документе «Руководство по настройке. Часть 8. Синхронизация учетных записей служб каталогов и СУБД. Компонент «ja_Sync_LDAP»

Табличная область вкладки «LDAP Sync» разделена на 3 части, расположенные в логической последовательности:

— Профили (Profiles);

— Маппинг (Mapping);

— Журнал (Log).

В левом верхнем углу расположена кнопка «Select Target», при нажатии вызывается окно выбора сервера целевой СУБД «Jatoba».

Перейдя во вкладку выберите БД с установленным расширением «ja_sync_ldap» после чего:

— установится соединение с БД;

— выполнится функция «ldapsync.get_sync_profiles», что соответствует SQL-команде:

```
select ja_sync_ldap.get_sync_profiles();
```

Если профили синхронизации сформированы, то они отразятся в табличной части «Profiles».

13.1. Табличная часть «Профили» (Profiles)

В табличной части «Профили» (Profiles) доступны функциональные возможности для профилей синхронизации:

— Добавление (Add);

— Редактирование (Edit);

— Удаление (Delete).

13.1.1. Создание профиля синхронизации с Active Directory

Профиль синхронизации добавляется через кнопку «Добавить».

Нажатие кнопки вызовет окно создания профиля синхронизации «Создание профиля» (Create profile), в котором требуется последовательно заполнить поля:

— Наименование профиля (Profile name) – имя профиля;

— Хост (Host) – IP-адрес сервера активного каталога;

— Порт (Port) – порт подключения к серверу активного каталога, по умолчанию используется значение 389;

— Логин (Login) – имя учетной запись на сервере активного каталога, имеющей административные полномочия управления учетными записями пользователей;

— Пароль (Password) – пароль вышеописанной учетной записи.

Заполненные поля сгенерируют SQL-команду:

```
SELECT ja_sync_ldap.set_sync_profile(in_profile_id int,
in_profile_name text, in_host_ip text, in_port text, in_login
text, in_pswd text);
```

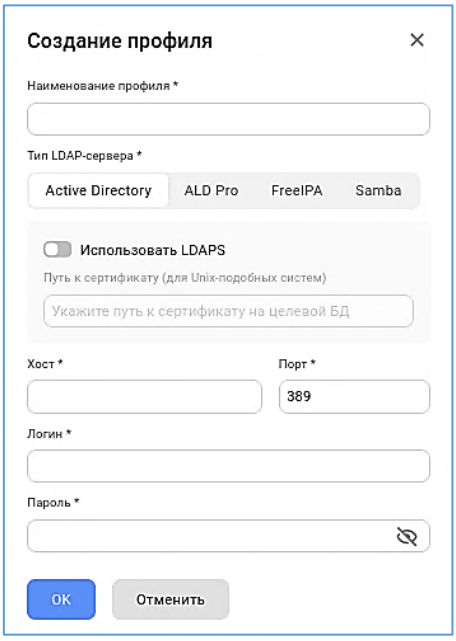

Рисунок 13.1 – Окно создания профиля синхронизации в версии JDS

В описываемом примере SQL-команда будет иметь вид:

```
select
ja_sync_ldap.set_sync_profile(null,'ad_users','10.96.1.200','38
9','admin','Password');
```

При сохранении созданного профиля синхронизации, он появится в списке профилей и в верхней центральной части раздела появится сообщение: «Ldapsync профиль создан».

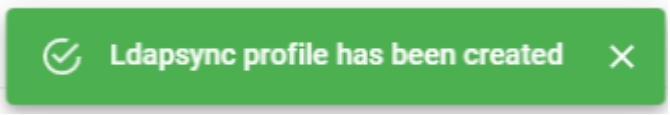

Рисунок 13.2 – Сообщение создания профиля

13.1.2. Создание профиля синхронизации с ALD Pro

ALD Pro – это альтернативное программное обеспечение MS Active Directory для управления активным каталогом, поддерживаемое на ОС GNU/Linux.

Для создания профиля синхронизации с сервером ALD Pro требуется выполнить следующие шаги:

— нажать кнопку «Добавить» (Add) в табличной части «Профили» (Profiles);

— в открывшимся окне «Создание профиля» (Create profile) выбрать вкладку «ALD Pro»;

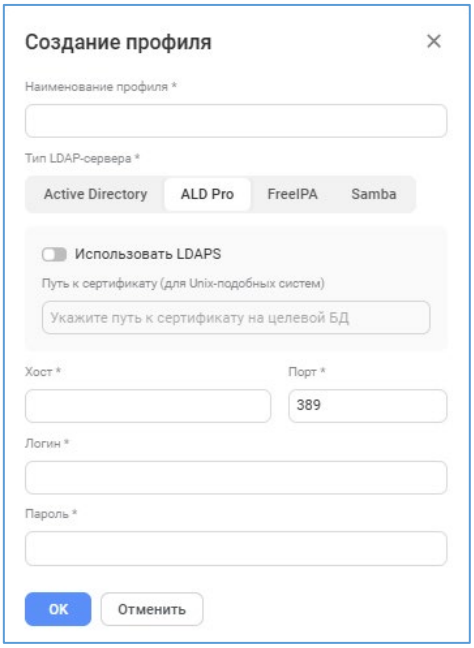

Рисунок 13.3 – Вкладка «ALD Pro»

— в поле «Имя профиля» (Profile name) указать имя создаваемого профиля синхронизации;

— в поле «Хост» (Host) указать IP-адрес сервера ALD Pro;

— в поле «Порт» (Port) по умолчанию установлено значение «389», если значение входящего порта не менялось, то оставить значением без изменений;

— в поле «Логин» (Login) указать параметр <admin DN>;

Строка параметра может иметь следующий вид:

```
uid=admin,cn=users,cn=accounts,dc=ald,dc=local
```

— в поле «Пароль» (password) указать пароль администратора сервера ALD Pro.

На данном шаге создание профиля синхронизации с сервером активного каталога ALD Pro закончено.

Создание профиля маппинга описано в п. 13.2.2 «Создание профиля маппинга ALD Pro».

13.1.3. Создание профиля синхронизации с FreeIPA

FreeIPA (Free Identity, Policy and Audit) — это дистрибутив Linux с открытым исходным кодом, который обеспечивает централизованное управление удостоверениями, аутентификацию и авторизацию, а также централизованное хранение атрибутов пользователей и групп. Он разработан для упрощения управления удостоверениями в среде Linux и может быть использован для создания каталогов, служб единого входа и других приложений, требующих централизованного управления удостоверениями.

Для создания профиля синхронизации с сервером FreeIPA требуется выполнить следующие шаги:

— нажать кнопку «Добавить» (Add) в табличной части «Профили» (Profiles);

— в открывшимся окне «Создание профиля» (Create profile) выбрать вкладку «FreeIPA»;

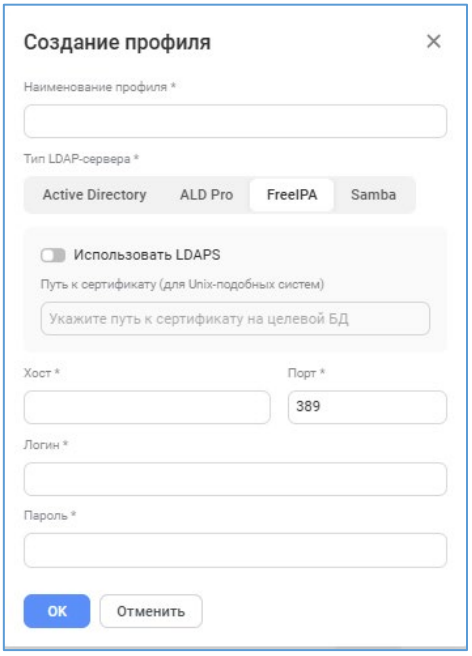

Рисунок 13.4 – Вкладка «FreeIPA»

— в поле «Имя профиля» (Profile name) указать имя создаваемого профиля синхронизации;

— в поле «Хост» (Host) указать IP-адрес сервера FreeIPA;

— в поле «Порт» (Port) по умолчанию установлено значение «389», если значение входящего порта не менялось, то оставить значением без изменений;

— в поле «Логин» (Login) указать параметр <admin DN>;

Строка параметра может иметь следующий вид:

```
uid=admin,cn=users,cn=accounts,dc=freeipa,dc=local)
```

— в поле «Пароль» (password) указать пароль администратора сервера FreeIPA.

На данном шаге создание профиля синхронизации с сервером активного каталога FreeIPA закончено.

13.1.4. Создание профиля синхронизации с Samba

Samba Active Directory Server обеспечивает среду, похожую на Windows, для управления учетными записями пользователей, правами доступа и ресурсами в сети на основе Samba. Он позволяет централизованно управлять аутентификацией пользователей, контролем доступа и совместным использованием ресурсов, что упрощает обслуживание и обеспечение безопасности смешанной среды.

С помощью Samba Active Directory Server интегрируются Linux, macOS и другие системы, отличные от Windows, в домен, что упрощает управление разрешениями пользователей, совместным доступом к файлам и доступом к принтерам на всех сетевых устройствах.

Для создания профиля синхронизации с сервером Samba требуется выполнить следующие шаги:

— нажать кнопку «Добавить» (Add) в табличной части «Профили» (Profiles).

— в открывшимся окне «Создание профиля» (Create profile) выбрать вкладку «Samba»;

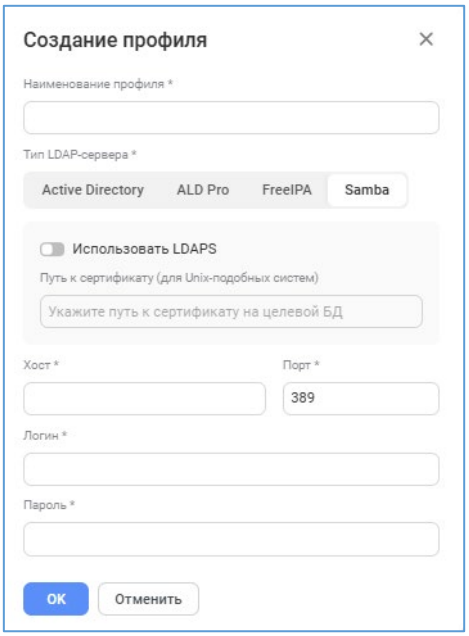

Рисунок 13.5 – Окно создания профиля Samba

— в поле «Имя профиля» (Profile name) указать имя создаваемого профиля синхронизации;

Например

```
samba_usr
```

— в поле «Хост» (Host) указать адрес сервера Samba;

Допускается указывать доменное имя или IP-адрес сервера Samba.

Например

IP-адрес сервера Samba

```
10.116.101.114
```

или доменное имя сервера Samba

```
dc.domain.test
```

— в поле «Порт» (Port) по умолчанию установлено значение «389», если значение входящего порта не менялось, то оставить значением без изменений;

В рассматриваемом примере используется значение «636».

— в поле «Логин» (Login) указать «UID» администратора сервера Samba;

«UID» администратора сервера Samba получается выполнением команды в терминале от имени и с правами «root»:

```
samba-tool user show administrator
```

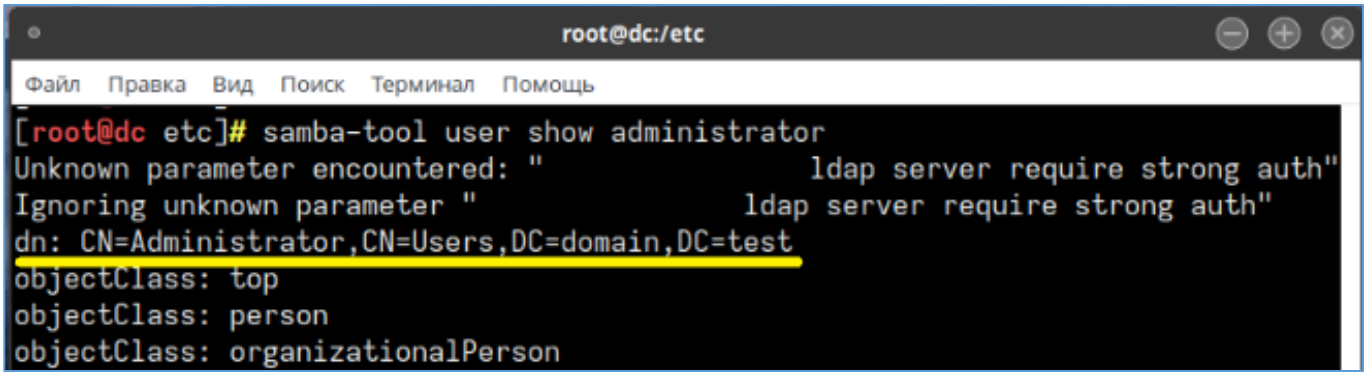

Рисунок 13.6 – «UID» администратора сервера Samba

Строка параметра может иметь следующий вид:

```
cn=administrator,cn=users,dc=domain,dc=test
```

— в поле «Пароль» (password) указать пароль администратора сервера Samba.

На данном шаге создание профиля синхронизации с сервером активного каталога Samba закончено.

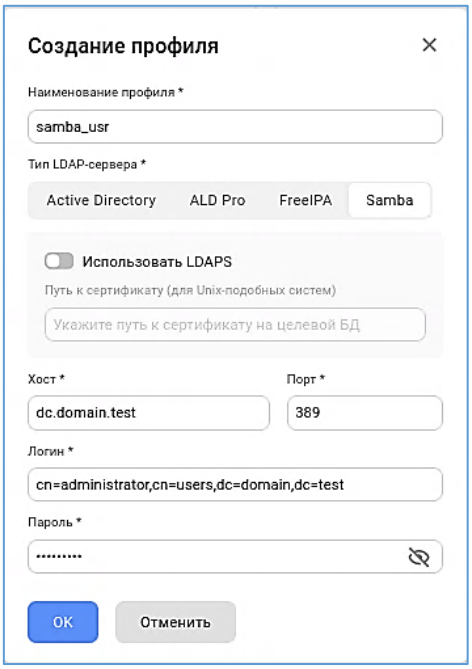

Рисунок 13.7 – Создание профиля синхронизации с сервером активного каталога «Samba»

Выполняемые действия будут аналогичны выполнению SQL-команде на сервере СУБД «Jatoba» с установленным расширением ja_Sync_LDAP:

```
SELECT
ja_sync_ldap.set_sync_profile(null,'samba_usr','dc.domain.test'
,'636','CN=Administrator,CN=Users,DC=domain,DC=test',
'P@ssword', 'samba');
```

Создание профиля маппинга описано в п. 13.2.4 «Создание профиля маппинга Samba».

13.1.5. Настройка LDAPS для сервера СУБД в ОС семейства Windows и GNU/Linux

Для использования LDAPS для сервера СУБД в ОС семейства Windows достаточно выполнить следующие шаги:

— перевести тумблер в положение «включено»;

— указать имя сертификата.

Предварительно сертификат должен быть экспортирован с сервера Active Directory и установлен на сервер СУБД в доверенные корневые центры сертификации.

Для использования LDAPS для сервера СУБД в ОС GNU/Linux достаточно выполнить следующие шаги:

— перевести тумблер в положение «включено»;

— указать путь и имя сертификата.

Скопировать сертификат pfx в любую директорию в ОС с СУБД, на которую есть права у пользователя postgres.

Например:

```
/var/lib/jatoba/<версия>/)
```

Получить из сертификата pfx сертификат crt:

```
openssl pkcs12 -in <cert_name>.pfx -nokeys -out <cert_name>.crt
```

Назначить владельцем сертификата пользователя postgres:

```
chown postgres:postgres /путь/до/<cert_name>.crt
```

Полное описание настроек по ОС приведено в документе «Руководство по настройке. Часть 8. Синхронизация учетных записей служб каталогов и СУБД. Компонент «ja_Sync_LDAP».

13.1.6. Редактирование и удаление профиля синхронизации

Имеющиеся профили синхронизации возможно редактировать или удалить через контекстное меню строки, как представлено на рисунке 13.8.

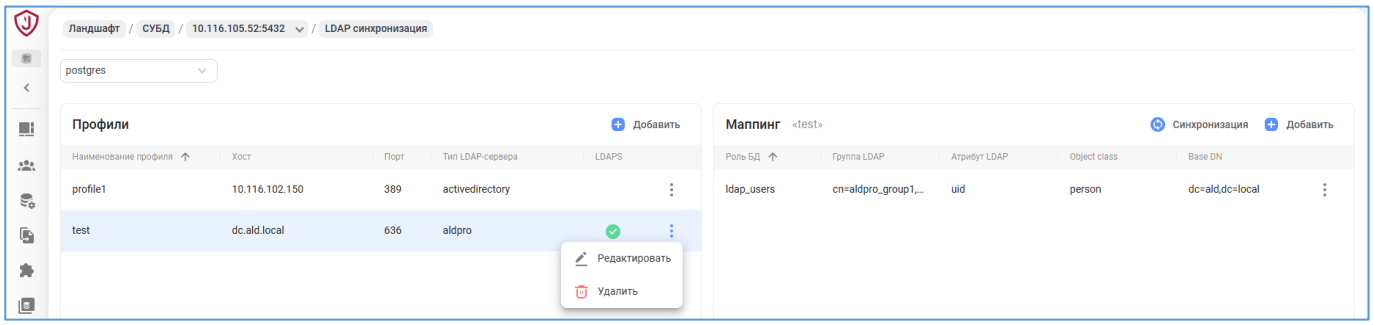

Рисунок 13.8 – Контекстное меню редактирования профиля

Удаление профиля синхронизации идентично выполненной SQL-команде, где номер профиля подставляется автоматически:

```
select ja_sync_ldap.drop_sync_profile(in_profile_id int);
```

13.2. Табличная часть «Маппинг» (Mappings)

В табличной части Маппинг (Mapping) отражаются профили маппинга соответствующие профилю синхронизации. Профиль синхронизации может иметь несколько профилей маппинга и при выборе профиля синхронизации, в табличной части «Profiles», отразятся принадлежащие ему профили.

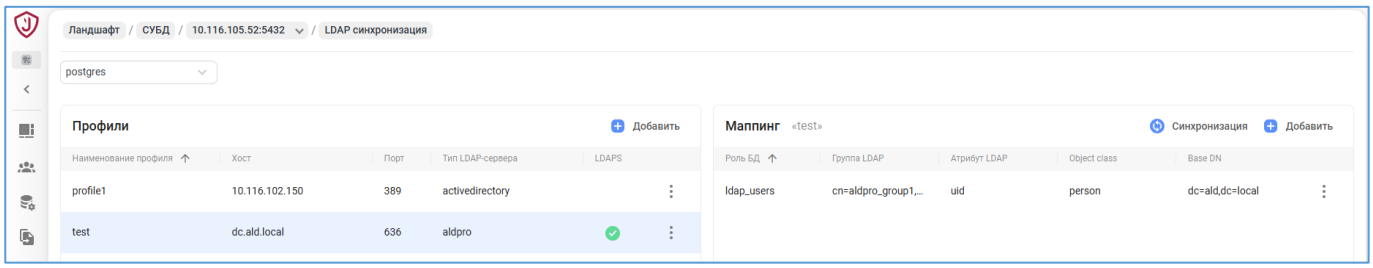

Рисунок 13.9 – Профили маппинга

Выбор профиля синхронизации вызовет функцию «ldapsync.get_sync_profile_maps», что идентично выполнению SQL-команды:

```
select ja_sync_ldap.get_sync_profile_maps(in_profile_id int);
```

номер профиля (profile_id) подставляется автоматически.

В табличной части «Mapping» доступны функциональные возможности для профилей маппинга, такие как:

— создание (Add);

— редактирование (Edit);

— удаление (Delete).

13.2.1. Создание профиля маппинга Active Directory

Нажатие пиктограммы создания профиля маппинга вызовет окно «Создание маппинга» (Create mapping).

Заполняемые поля показано в таблице 13.1.

Таблица 13.1 – Наименование полей профиля маппинга

№	Наименование поля	Тип поля
1	DB role *	Обязательное
2	LDAP group *	Обязательное
3	LDAP attribute *	Обязательное
4	Object class	Необязательное
5	Base DN	Необязательное

Окно создания профиля маппинга представлены на рисунке 13.10

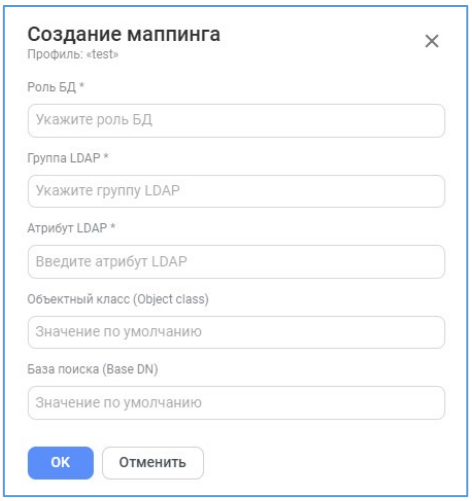

Рисунок 13.10 – Окно создания профиля маппинга

В поле «DB role» указывается групповая роль, в которую будут добавлены создаваемые пользователи в целевой СУБД.

В поле «AD group/LDAP group» указывается атрибут «DistinguishedName» группы пользователей «db_users» Microsoft Active Directory.

В поле «AD attribute/LDAP attribute» указывается атрибут записи в Microsoft Active Directory, по которому будет осуществляться поиск учетных записей пользователей и выполняться синхронизация с СУБД. В качестве атрибутов синхронизации могут использоваться атрибуты:

— sAMAccountName;

— cn;

— name.

Заполненные поля окна сгенерируют SQL-команду:

```
SELECT ja_sync_ldap.set_sync_profile_map(in_map_id int,
in_profile_id int, role_bd text, role_ad text, in_attribute
text);
```

В описываемом примере SQL-команда будет иметь вид:

```
SELECT
ja_sync_ldap.set_sync_profile_map(null,1,'ad_users','CN=db_user
s,CN=Users,DC=jatoba,DC=corp', 'cn');
```

Поля «Object class» и «Base DN» не обязательны при заполнении и заполнятся автоматически.

При сохранении созданного профиля маппинга, он появится в списке профилей и в верхней центральной части раздела появится сообщение: «Ldapsync профиль маппинга создан».

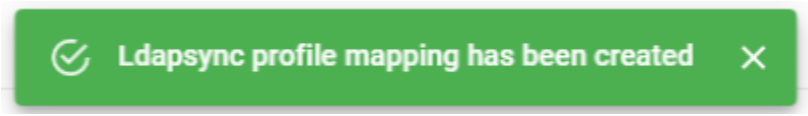

Рисунок 13.11 – Сообщение создание профиля маппинга

После чего станет доступна пиктограмма выполнения синхронизации «Synchronization».

13.2.2. Создание профиля маппинга ALD Pro

Для создания такого профиля мапинга с сервером ALD Pro требуется выполнить следующие шаги:

— нажать кнопку «Добавить» (Add) в табличной части «Маппинг» (Mappings), что вызовет окно «Создание профиля» (Create mapping);

— в поле «Роль БД» (DB role) указывается групповая роль в СУБД, в которую будут добавлены создаваемые пользователи;

— в поле «Группа LDAP» (LDAP group) указать имя группы пользователей на сервере ALD Pro, пользователи которой будут синхронизированы с пользователями СУБД;

Строка параметра может иметь следующий вид:

```
cn=lpadmin,cn=groups,cn=accounts,dc=ald,dc=local
```

— в поле «Атрибут LDAP» (LDAP attribute) указать атрибут, по которому будет осуществляться поиск учетных записей пользователей и выполняться синхронизация с СУБД;

В качестве атрибута поиска на сервере ALD Pro используется атрибут:

```
uid
```

Атрибут UID (User ID) — это уникальный идентификатор пользователя в системе. Он используется для идентификации и отличия пользователей в операционной системе. Каждый пользователь в системе имеет свой собственный UID, который присваивается ему при создании учетной записи.

— в поле «Объектный класс» (Object class) указать параметр:

```
person
```

либо параметр заполнится автоматически.

— в поле «База поиска» (Base DN) указать параметр <basedn>. При заполнении обязательных полей поле заполниться автоматически.

Строка параметра может иметь следующий вид:

```
dc=ald,dc=local
```

13.2.3. Создание профиля маппинга FreeIPA

Для создания такого профиля мапинга с сервером FreeIPA требуется выполнить следующие шаги:

— нажать кнопку «Добавить» (Add) в табличной части «Маппинг» (Mappings), что вызовет окно «Создание профиля» (Create mapping);

— в поле «Роль БД» (DB role) указать групповую роль в СУБД, в которую будут добавлены создаваемые пользователи;

— в поле «Группа LDAP» (LDAP group) указать имя группы пользователей на сервере FreeIPA, пользователи которой буду синхронизированы с пользователями СУБД;

Строка параметра может иметь следующий вид:

```
CN=freeipa,CN=groups,CN=accounts,DC=freeipa,DC=local
```

— в поле «Атрибут LDAP» (LDAP attribute) указать атрибут по которому будет осуществляться поиск учетных записей пользователей и выполняться синхронизация с СУБД;

В качестве атрибута поиска на сервере FreeIPA используется атрибут:

```
uid
```

Атрибут UID (User ID) — это уникальный идентификатор пользователя в системе. Он используется для идентификации и различения пользователей в операционной системе. Каждый пользователь в системе имеет свой собственный UID, который присваивается ему при создании учетной записи.

— в поле «Объектный класс» (Object class) указать параметр:

```
person
```

— в поле «База поиска» (Base DN) указать параметр <basedn>.

Строка параметра может иметь следующий вид:

```
dc=freeipa,dc=local
```

Параметр «basedn» отражается в файле:

```
/etc/ipa/default.conf
```

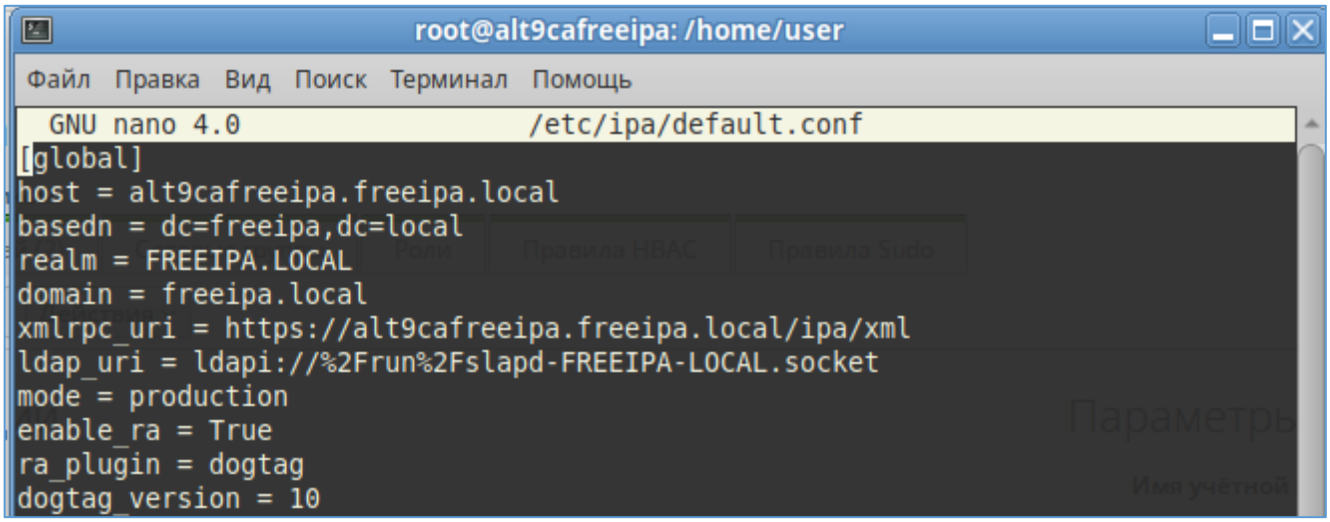

Рисунок 13.12 – Содержимое файла «default.conf»

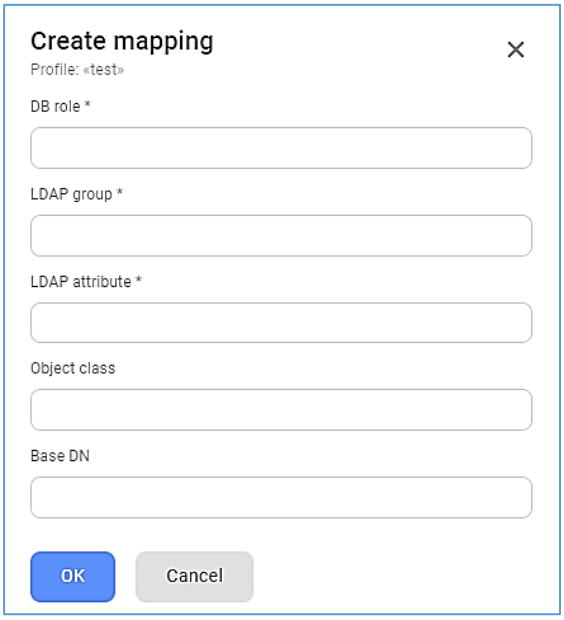

Рисунок 13.13 – Окно создания профиля маппинга для сервера FreeIPA

13.2.4. Создание профиля маппинга Samba

Для создания такого профиля маппинга с сервером Samba требуется выполнить следующие шаги:

— нажать кнопку «Добавить» (Add) в табличной части «Маппинг» (Mappings), что вызовет окно «Создание профиля» (Create mapping). ID маппинга сформируется автоматически;

— в поле «Роль БД» (DB role) указать групповую роль в СУБД, в которую будут добавлены создаваемые пользователи;

Например

```
db_users_smb
```

Групповую роль возможно предварительно создать в разделе «Роли БД» описанного в п. 9 настоящего документа.

— в поле «Группа LDAP» (LDAP group) указать имя группы пользователей на сервере Samba, пользователи которой буду синхронизированы с пользователями СУБД.

Например

При синхронизации УЗ по атрибуту 'sAMAccountName', требуется получить его из вывода свойств группы пользователей на сервере активного каталога Samba командой:

```
samba-tool group show db_user
```

В данном случае, группа пользователей db_user должна быть создана на сервер активного каталога и содержать пользователей ОС.

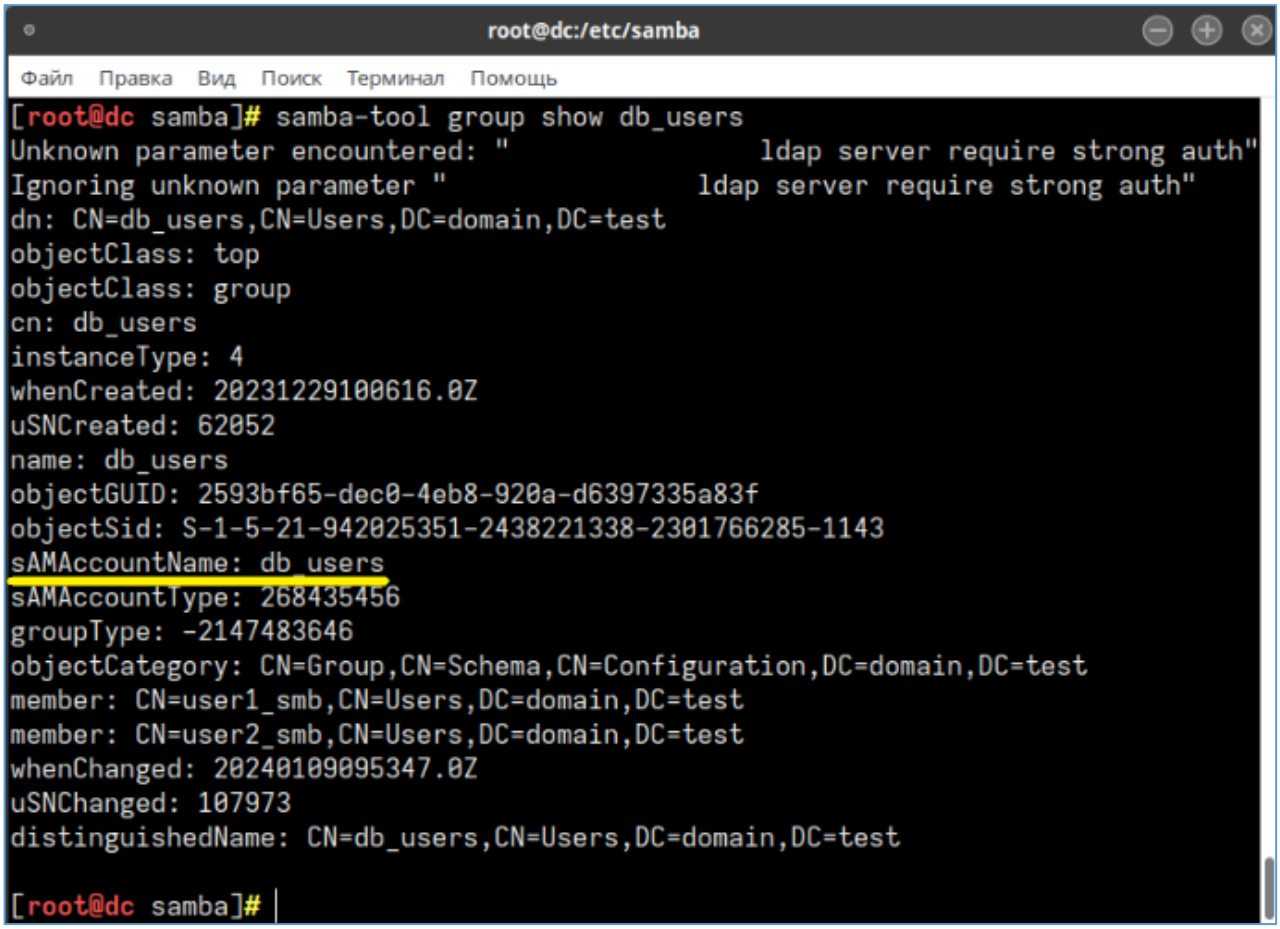

Рисунок 13.14 – Вывод свойства группы

Для атрибута «sAMAccountName» используется значение «DistinguishedName»:

```
CN=db_users,CN=Users,DC=domain,DC=test
```

— в поле «Атрибут LDAP» (LDAP attribute) указать атрибут, по которому будет осуществляться поиск учетных записей пользователей и выполняться синхронизация с СУБД.

В качестве атрибута поиска на сервере Samba используется атрибут:

```
sAMAccountName
```

— в поле «Объектный класс» (Object class) указать параметр:

```
user
```

Параметр выбирается из строки значение «DistinguishedName»

```
CN=Users
```

- в поле «База поиска» (Base DN) указать параметр <dn>.

Например

```
dc=domain,dc=test
```

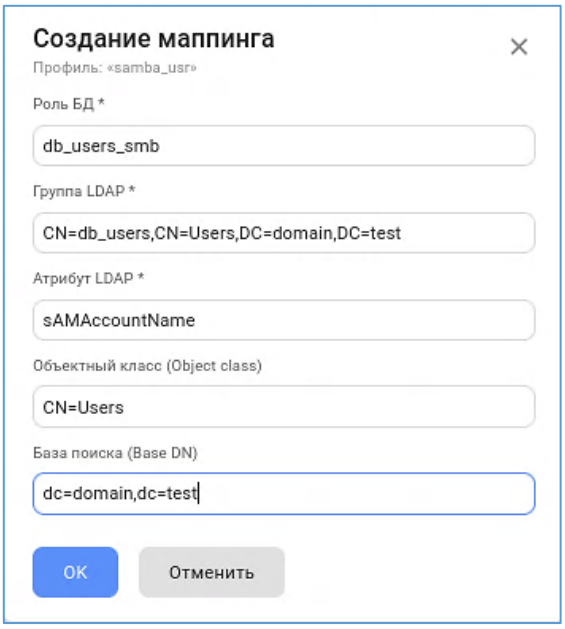

Рисунок 13.15 – Окно создания профиля маппинга для сервера Samba

13.2.5. Редактирование и удаление профиля маппинга

Имеющиеся профили маппинга возможно редактировать или удалить через контекстное меню строки, как представлено на рисунке 13.16.

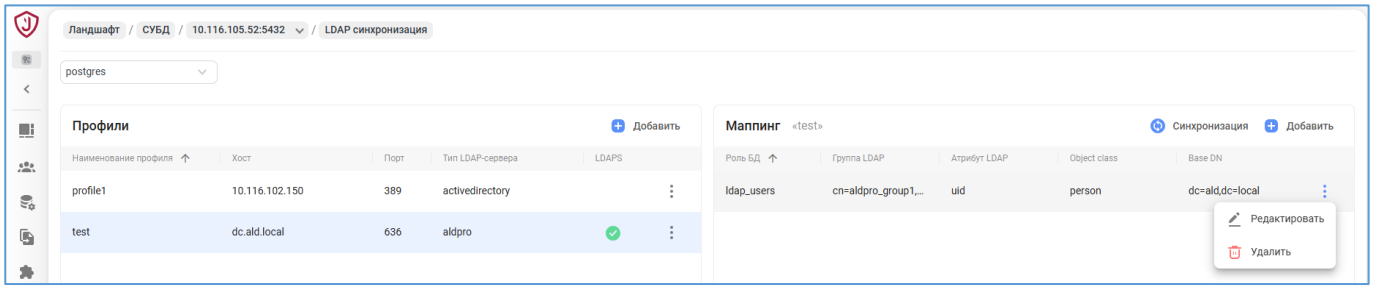

Рисунок 13.16 – Контекстное меню редактирования профиля маппинга

Удаление существующего профиля маппинга идентично выполненной SQL-команде, где номер профиля подставляется автоматически:

```
SELECT ja_sync_ldap.drop_sync_profile_map(in_map_id int);
```

При выборе пиктограммы редактирования профиля маппинга «Edit» откроется окно «Edit mapping».

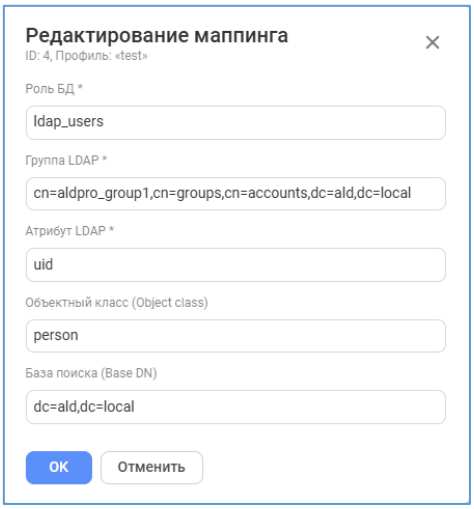

Рисунок 13.17 – Окно редактирования профиля маппинга

Поле «Profile» недоступно для редактирования, т.к. профиль маппинга соотносится к определенному профилю синхронизации.

Поля «DB role», «AD group» и «AD attribute» доступны для редактирования.

13.3. Табличная часть «Журнал» (Log)

В журнале «Log» отображаются события выполнения синхронизации учетных записей пользователей активного каталога с учетными записями СУБД «Jatoba».

Имеется функциональная возможность просмотра, удаления выбранных событий и отдельных событий.

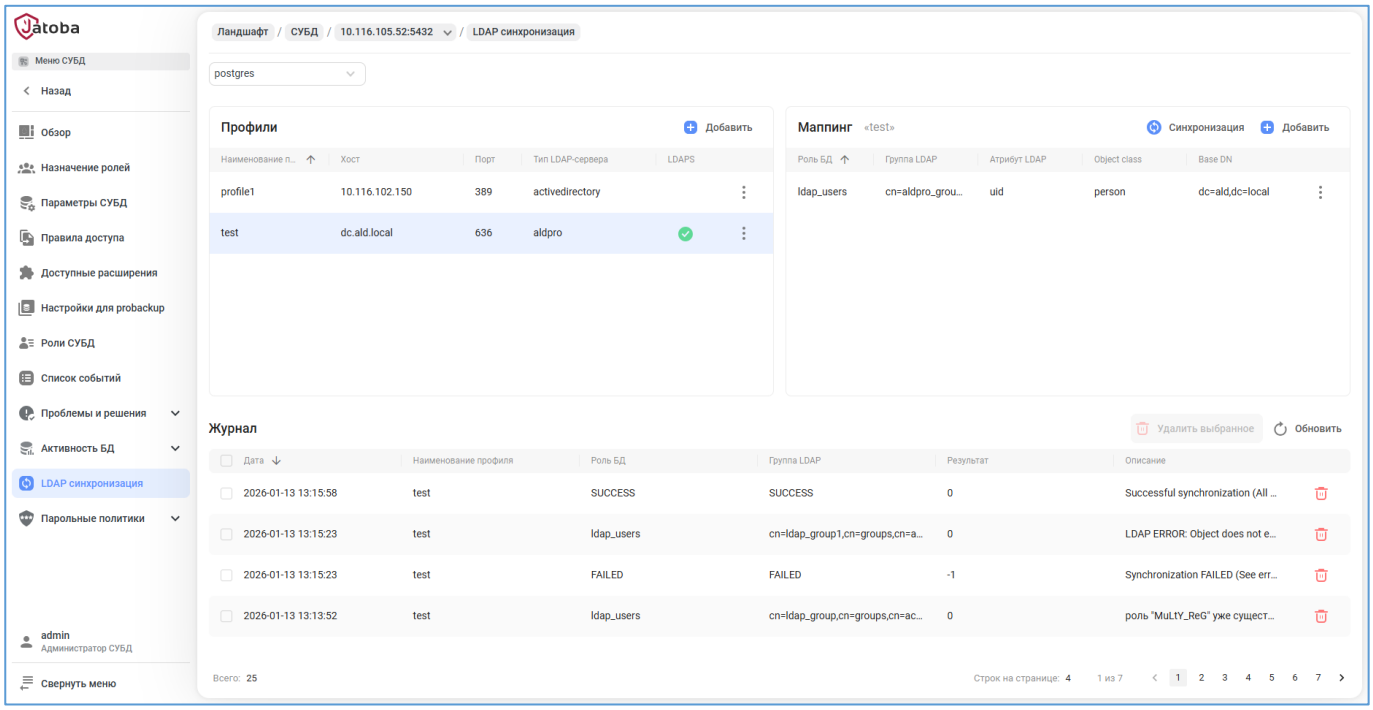

Рисунок 13.18 – Журнал

14. РАЗДЕЛ «ЛАНДШАФТ». СУБД. ВКЛАДКА «ПАРОЛЬНЫЕ ПОЛИТИКИ» (PASSWORD POLICIES)

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) (п. 14.1);

— Привязка ролей (Role Binding) (п. 14.2);

— Работа с блокировками (п. 14.3).

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».

Функциональные возможности подраздела доступны на уровне целевой СУБД в разделе «Ландшафт».

14.1. Вкладка «Управление политиками» (Policy management)

Во вкладке отображаются парольные политики:

– Default – профиль парольной политики используемой по умолчанию;

– 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.

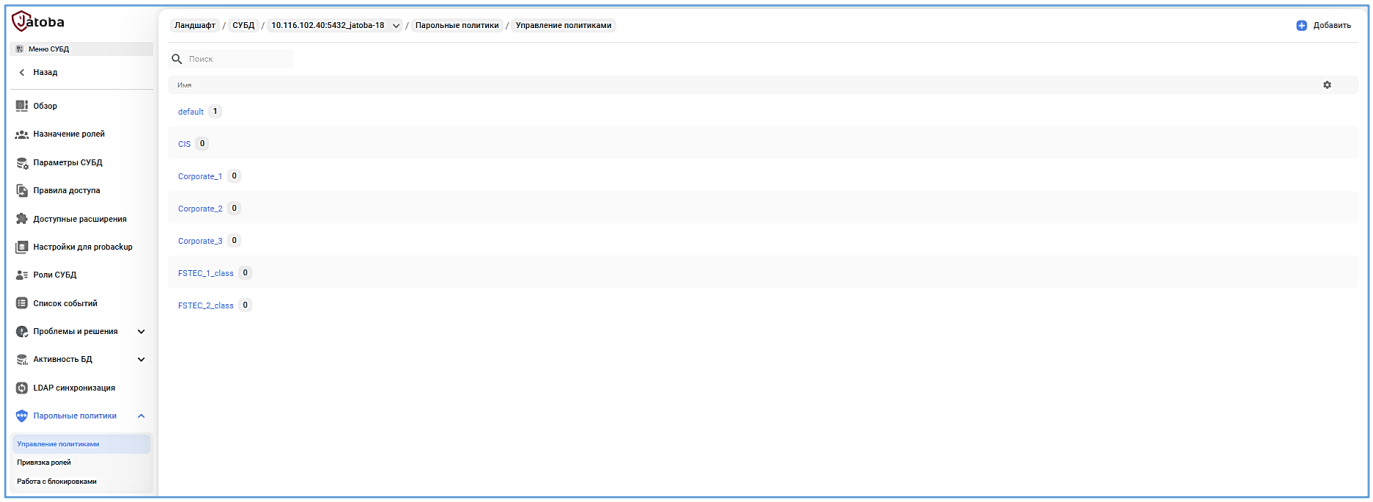

Рисунок 14.1 – Вкладка «Редактирование политик»

Во вкладе доступно редактирование, удаление предустановленных политик и создание новых основанных на парольной политике по умолчанию (Default).

14.2. Вкладка «Привязка ролей» (Role Binding)

Во вкладке «Привязка ролей» отображаются роли СУБД, распределенные по парольным политикам.

В раскрывшимся списке парольной политики отображается список пользователей с установленными и унаследованными от групповых ролей атрибутами.

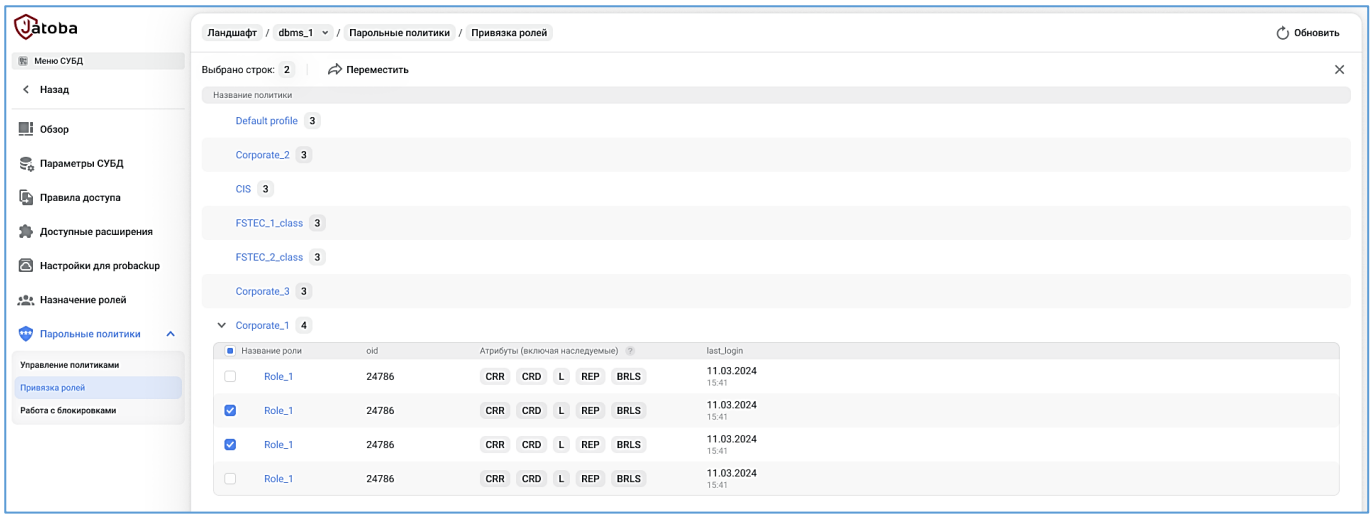

Рисунок 14.2 – Список пользователей привязанных к парольной политике

Редактирование парольных политик недоступно. Возможен только просмотр.

Ко всем ролям СУБД применяется парольная политика по умолчанию «default». Для применения предустановленных парольных политики или созданных, требуется установить чекбокс на одной или нескольких ролях и переместить между парольными политиками.

Парольная политика применится при следующей идентификации пользователя в СУБД.

14.3. Вкладка «Работа с блокировками»

Вкладка «Работа с блокировками» делится на два окна (вкладки) «securityprofile» и «checksum». Вкладки отображают роли СУБД и их статусы блокировки.

Статусы ролей, заблокированных из-за нарушения парольных политик, отображаются во вкладке «securityprofile» и заблокированные в следствии нарушения контроля целостности СУБД отображаются во вкладке «checksum».

14.3.1. Вкладка «securityprofile»

Во вкладке отображается список пользователей (ролей) СУБД.

Доступно отфильтровать заблокированные роли установкой тумблера «Только заблокированные».

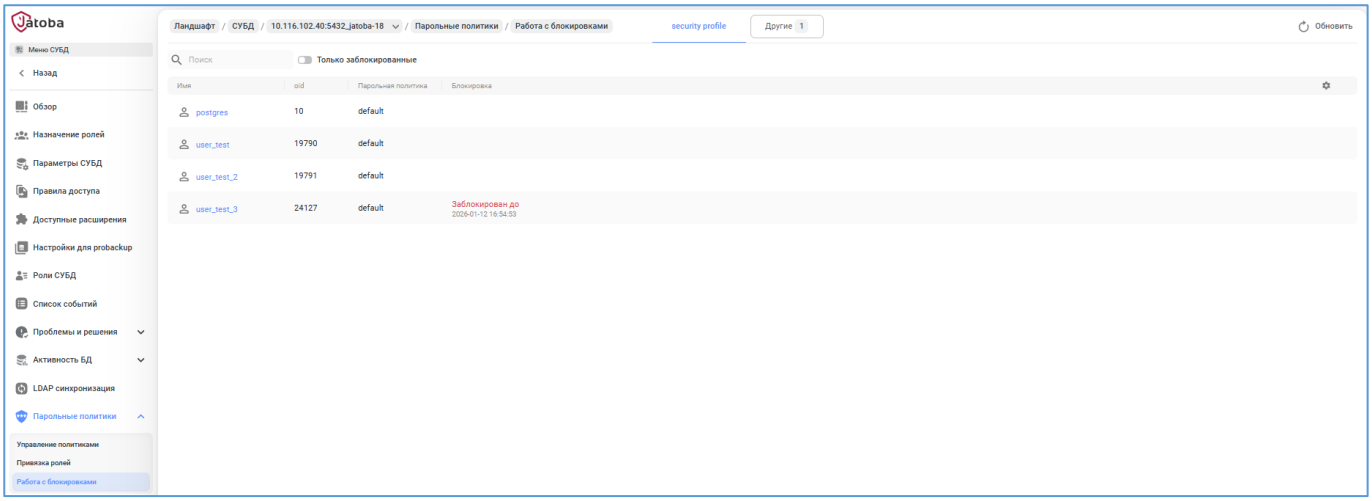

Рисунок 14.3 – Вкладка «securityprofile»

Приказ ФСТЭК России от 14.04.2023 N 64 «Требования по безопасности информации к системам управления базами данных (выписка)» в разделе 9, не устанавливает требования к типу блокирования, поэтому, как описано в п. 6.2.1. «Блокирование и разблокирование учетных записей» документа Руководство администратора:

«По умолчанию блокировка пользователей выполняется в режиме «immediate». В данном режиме пользователь принудительно отключается без ожидания и непосредственного отката транзакций».

В силу указанных причин, использовать функциональную возможность, по блокированию роли или группы ролей, следует с максимальной осторожностью

В строке пользователя СУБД, при наведении курсора в конец строки вызывается кнопка «Блокировать/Разблокировать».

По умолчанию пользователь СУБД блокируется на 60 минут.

14.3.2. Вкладка «checksum»

Перед разблокировкой пользователей, заблокированных при нарушении контроля целостности СУБД, требуется вручную, на целевом хосте устранить причину нарушения или пересчитать контрольные суммы.

Во вкладке «checksum» отображаются группы пользователей:

— Пользователи БД;

— Администраторы БД;

— Администраторы СУБД;

— Прочие.

При нарушении контроля целостности СУБД или ограничения программной среды СУБД блокируется группа «Пользователи БД». Информация о блокировке выводится в строке группы в виде списка БД.

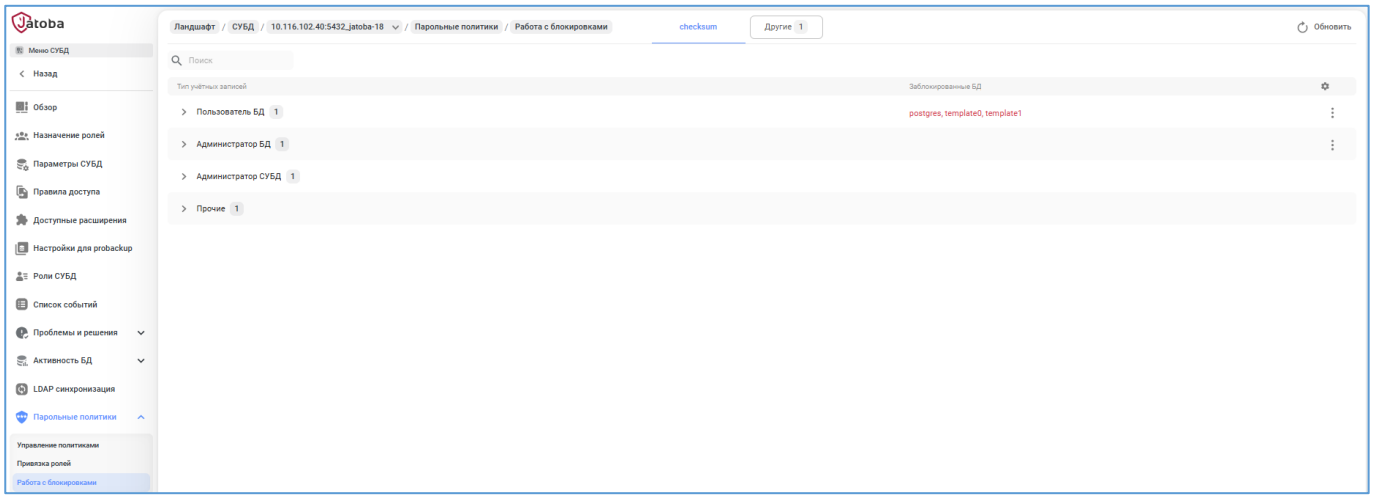

Рисунок 14.4 – Вкладка «checksum»

Контекстное меню разблокирования находится в строке группы.

В вызванном окне выбираются только БД, к которым требуется открыть доступ.

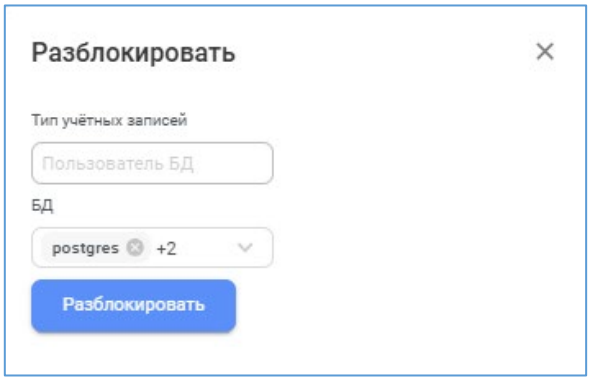

Рисунок 14.5 – Окно разблокирования группы пользователей

Нажатие кнопки «Разблокировать» инициирует выполнение SQL-команды разблокирования группы пользователей на целевом хосте.

Также доступна операция блокирования группы пользователей.

Блокирование доступно только для всех групп, кроме группы «Администраторы СУБД».

15. РАЗДЕЛ «ЛАНДШАФТ». БД. ВКЛАДКА «ОБЗОР»

В разделе Ландшафт существует вторая одноименная вкладка «Обзор» отображающая параметры БД.

Для перехода в нее требуется выбрать раздел «Ландшафт» → «Дерево инфраструктуры» → хост → СУБД → БД.

Нажатие на гиперссылку БД откроет вкладку «Обзор», в которой отобразятся основные параметры БД.

Отображаемые параметры представлены в таблице 15.1.

Таблица 15.1 - Список отображаемых параметров БД

Наименование поля	Вид отображения	Описание поля
Владелец	текст	Администратор БД
Описание	текст	Комментарий к БД
Размер	текст	Объем дискового пространства занимаемого БД
Текущие сессии	число (ссылка)	Количество текущих подключений к БД
Табличное пространство	текст	Используемое табличное пространство
Схемы	текст (список)	Схемы БД
Кодировка	текст	Кодировка символов в БД
Категория сортировки	текст	Устанавливает значение LC_COLLATE в окружении ОС сервера баз данных
Категория типов символов	текст	Устанавливает значение LC_CTYPE в окружении ОС сервера баз данных
Шаблон	да/нет	Допускается ли использование БД в качестве шаблона
Разрешено подключение	да/нет	Допускается ли подключение пользователей к БД
Лимит подключений	число	Ограничение количества одновременных подключений к БД

Вид вкладки показан на рисунке 15.1.

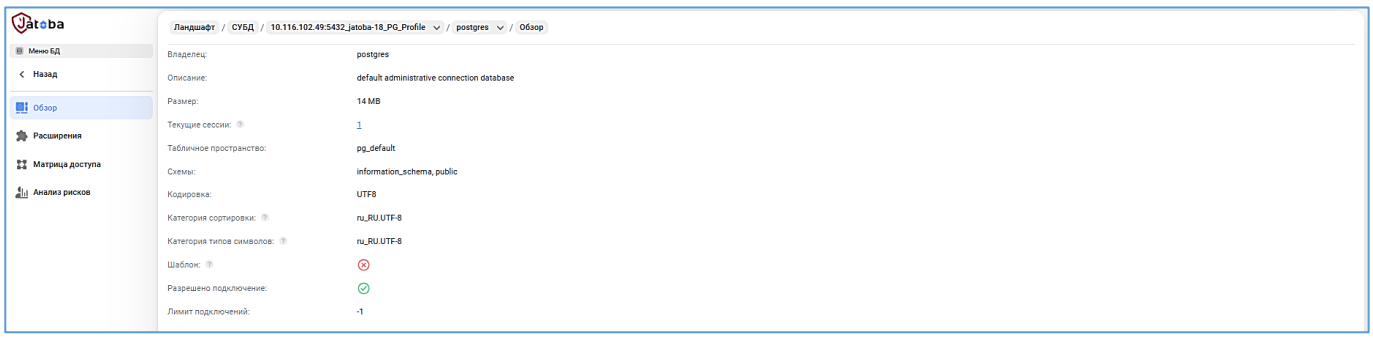

Рисунок 15.1 - Вкладка «Обзор» БД

16. РАЗДЕЛ «ЛАНДШАФТ». БД. ВКЛАДКА «Расширения»

Перед установкой расширений СУБД «Jatoba» убедитесь, что компонент контроля целостности «ja_CSum» отключен или переведен в режим информирования (permissive). Поскольку, «ja_CSum» функционируя совместно компонентом парольных политик «SecurityProfile», пересчитав контрольные суммы СУБД и найдя в них расхождения с эталонными значениями, передаст команду компоненту «SecurityProfile» на блокирование пользователей СУБД.

Функциональная возможность управления контрольными суммами СУБД отсутствует.

Пересчет контрольных сумм СУБД выполняется вручную.

16.1. Установка расширения в БД

Установка расширения в БД доступно при:

— выборе БД в общем списке баз данных СУБД;

— переходе во вкладку «Управление расширениями».

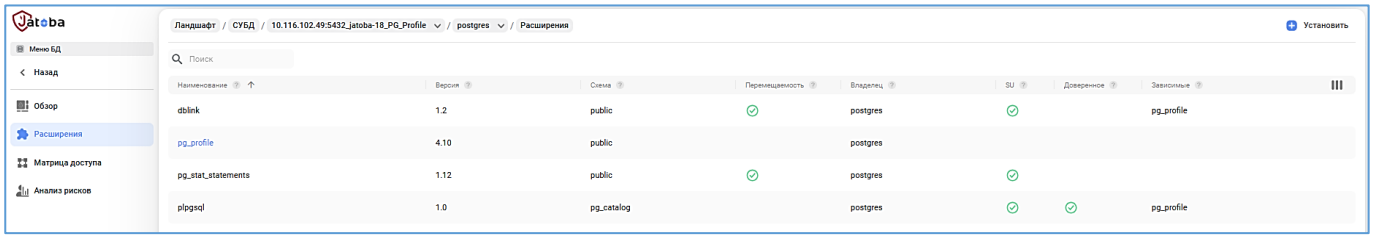

Рисунок 16.1 – Вкладка «Управление расширениями»

Модальное окно «Установка расширений» вызывается нажатием кнопки «Установить».

В окне последовательно выбирается устанавливаемое расширение, его версия и схема БД.

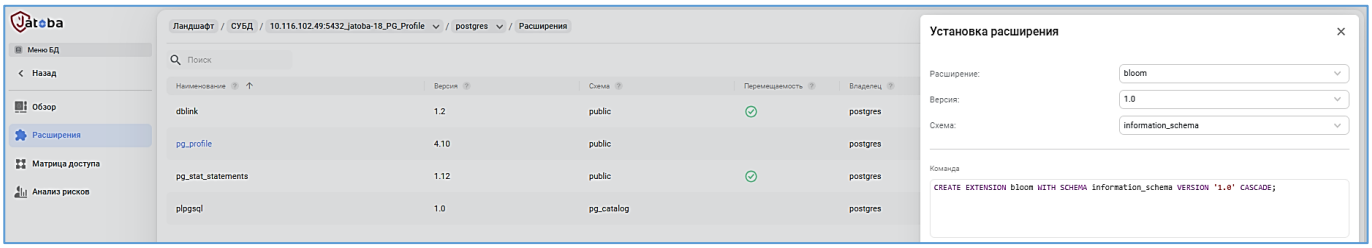

Рисунок 16.2 - Окно «Установка расширений»

Отобразится SQL-команда установки расширения, без возможности редактирования. Расширение установится по нажатию кнопки «Установить».

После операции установки расширения оно отобразится в общем списке во вкладке «Управление расширениями». В списке доступны операции по:

— сортировке списка;

— контекстному поиску расширений;

— редактированию расширения (изменение версии расширения и схемы установки);

— удалению расширения.

При большом количестве установленных расширений их список разбивается на страницы в правом нижнем углу вкладки.

16.1.1. Удаление расширений БД

Список доступных расширений СУБД отображается во вкладке «Доступные расширения».

Расширения устанавливаются в конкретную БД. Для удаления расширения требуется разделе «Ландшафт» перейти до уровня БД во вкладку «Расширения».

Во вкладке «Расширения» наведя курсор на строку установленного расширения появится кнопка «Удалить».

Выбрав операцию удаления расширения в БД, в любой другой отличной от служебной, компонент выдаст окно подтверждения операции.

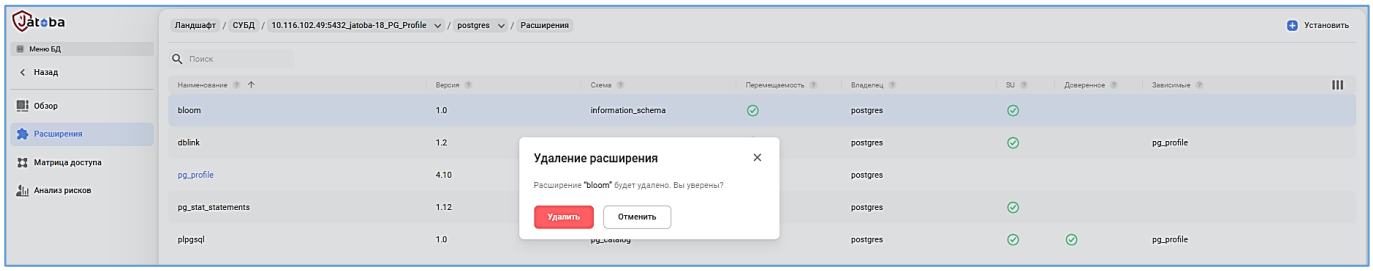

Рисунок 16.3 – Удаление расширения в БД и окно подтверждения

Расширение plpgsql нельзя удалить из служебной БД JDS.

16.2. БД. Установка расширения pg_profile

Расширение pg_profile имеет более тонкую настройку в отличие от других расширений СУБД. В следствии чего для его настройки разработано отдельное представление в компонента.

Расширение устанавливается в порядке описанном в п.п. 16 «Раздел «Ландшафт». БД. Вкладка «».

Расширение pg_profile установленное средствами раздела «Ландшафт» автоматически появится в разделе «Снимки и отчеты» (Snapshots & Reports) (см. п.п. 24)

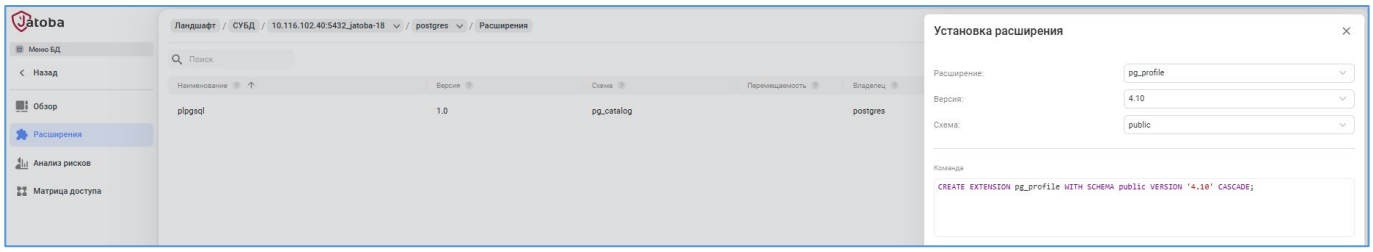

Рисунок 16.4 – Окно уставки расширения pg_profile

Установка выполняется методом «CASCADE» и вместе с ним установится расширение dblink.

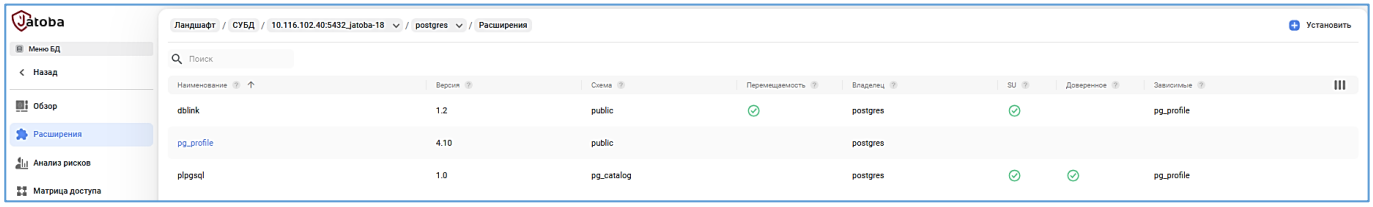

Рисунок 16.5 – Установленные расширения на целевой СУБД

В списке установленных расширений расширение pg_profile имеет гиперссылку, ведущую в отдельные вкладки:

— Обзор;

— Настройки сервера;

— Параметры.

Вкладка «Обзор» расширения

Во вкладке «Обзор» отображаются не редактируемые строки:

— Версия – версия расширения;

— Владелец – владелец расширения;

— Расположение – путь к хосту СУБД на котором установлено расширение.

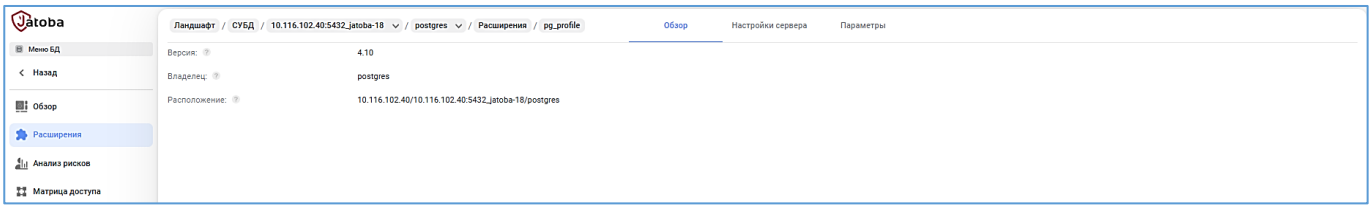

Рисунок 16.6 - Вкладка «Обзор» расширения

Вкладка «Настройки сервера»

Во вкладке «Настройки сервера» отображаются виртуальные сервера расширения.

Виртуальный сервер «local» устанавливается автоматически при установке расширения. Виртуальные сервера доступно создавать и редактировать.

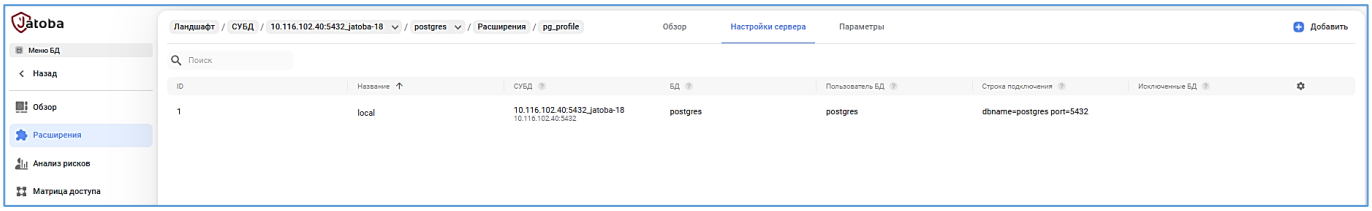

Рисунок 16.7 – Вкладка «Настройки сервера»

Нажатие кнопки «Добавить» вызовет окно «Добавление сервера». В данном окне устанавливаются параметры нового виртуального сервера приведенные в таблице 16.1

Таблица 16.1 – Параметры создаваемого виртуального сервера

Раздел	Параметр	Описание	Редактирование
Настройки подключения			
	Название: *	Наименование создаваемого виртуального сервера	X
	СУБД: *	Выпадающий список из СУБД подключенных в разделе «Ландшафт»	X
	БД: *	База данных	X
	Пользователь БД	Пользователь базы данных (Пользователь с назначением «Сбор снимков производительности»)	–
	Строка подключения	Отображение строки подключения к БД	–
Дополнительные параметры			
	Исключенные БД:	Выпадающий список с выбором БД с которых не будут сниматься снимки	X
	Снимать метрики при создании снимка:	включение сервера в набор серверов, на которых снимаются метрики при создании снимка	X
	Время жизни снимка на сервере:	Целое, положительное значение в днях определяющее время жизни снимка на сервере	X
	Описание:	Описание создаваемого сервера	X
Установка pg_stat_statements			
	Версия	Версия компонента	X
	Схема	Схема для установки	X

Примечание:

* - обязательные параметры.

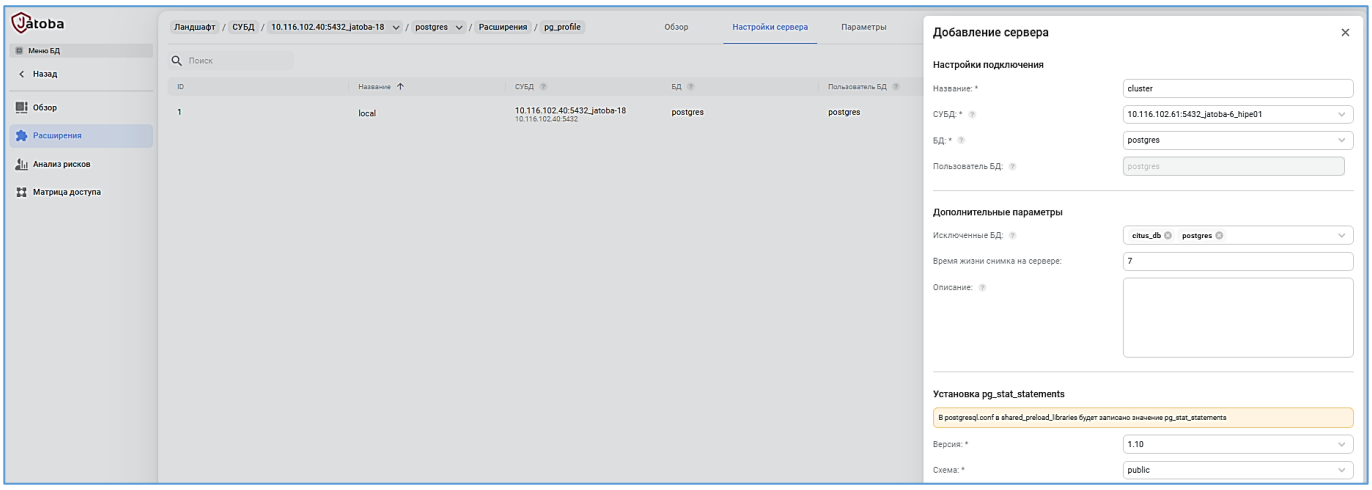

Рисунок 16.8 – Окно добавление нового сервера

Возможно добавлять серверы с других хостов СУБД, таким образом создавая иерархическую структуру сбора статистики.

Если в поле «Пользователь БД» указан не привилегированный пользователь (SU), то под полем отобразить сообщение:

```
Выбранному пользователю БД будут назначены привилегии:

 - доступ к схемам расположения расширений (если расширения
установлены) pg_stat_statements, pg_stat_kcache,
pg_wait_sampling

- возможность запуска функций (если расширения установлены)
pg_stat_statements_reset, pg_stat_kcache_reset,
pg_wait_sampling_reset_profile

- роль pg_read_all_stats
```

В процессе создания виртуального сервера, вышеуказанные действия будут выполнены.

Блок «Установка pg_stat_statements» активируется, если расширение «pg_stat_statements» не установлено, что сопровождается соответствующим сообщением.

Появляются поля «Версия» и «Схема», установив параметры в которых установится расширение. Пакет компонента должен быть установлен предварительно на хосте.

Завершение установки «pg_stat_statements» может быть произведено с перезагрузкой СУБД. Поэтому будет выведено модальное окно «Применение параметров» с выбором желаемого действия, таким как «Продолжить без перезагрузки» и «Перезагрузить сейчас».

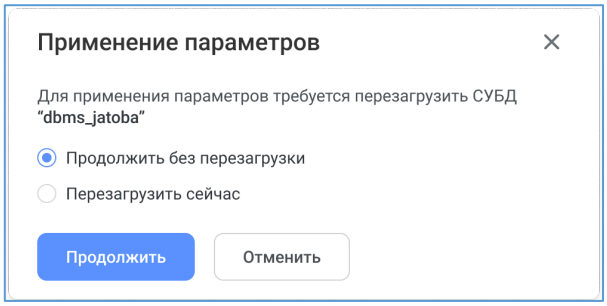

Рисунок 16.9 – Окно применения параметров

Далее созданная структура виртуальных сервером отразится в подразделе «Снимки и отчеты» описанного в разделе 24 настоящего документа.

Вкладка «Параметры»

Во вкладке «Параметры» отображаются параметры расширения, установленные по умолчанию.

Параметры расширения приведены в таблице 16.2.

Таблица 16.2 – Параметры расширения

Параметры	Значение
Количество выбираемых первых объектов (операторов, отношений и т. д.), которое будет выдаваться в каждой отсортированной по некоторому критерию таблице отчёта. Этот параметр влияет на размер выборки	20
Время хранения снимков в днях	7
Если этот параметр включен, pg_profile будет отслеживать подробные временные интервалы	off
Ограничение длины запроса для отчетов	20000

Имеющиеся параметры доступны для редактирования.

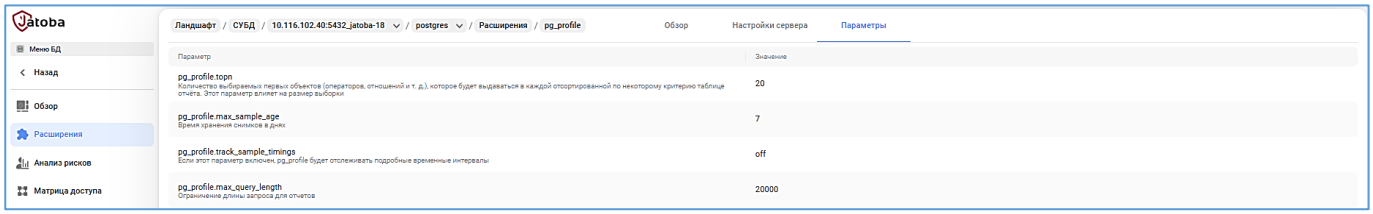

Рисунок 16.10 - Вкладка «Параметры»

16.3. БД. Установка расширения securityprofile (парольные политики)

Для активации компонента в СУБД «Jatoba» на целевом хосте, в разделе «Ландшафт» достаточно выбрать расширение для установки. Автоматически внесутся изменения конфигурационный файл postgresql.auto.conf, прописав следующие строки:

```
shared_preload_libraries = 'securityprofile'
```

Указание в конфигурационном файле postgresql.conf опции shared_preload_libraries = 'securityprofile' активирует компонент управления парольными политиками и создается политика по умолчанию с именем «default».

```
securityprofile.db_name = 'dbname'
```

Параметр «dbname» определяет имя БД, в которой будет создаваться или уже создано расширение sercurityprofile, значение по умолчанию postgres.

Внесенные изменения применяются без перезагрузки СУБД.

Компонент securityprofile выполняет функции безопасности в СУБД и влияет на работу всех пользователей и администраторов СУБД, поскольку:

— применяет парольные политики;

— блокирует пользователей и администраторов СУБД при нарушении парольных политик;

— блокирует пользователей при нарушении контроля целостности СУБД.

Расширение устанавливается в порядке описанном в п.п. 16 «Раздел «Ландшафт». БД. Вкладка «». При этом дополнительно указывается БД для установки и устанавливается флаг для автоматического внесения изменений в конфигурационный файл postgresql.auto.conf.

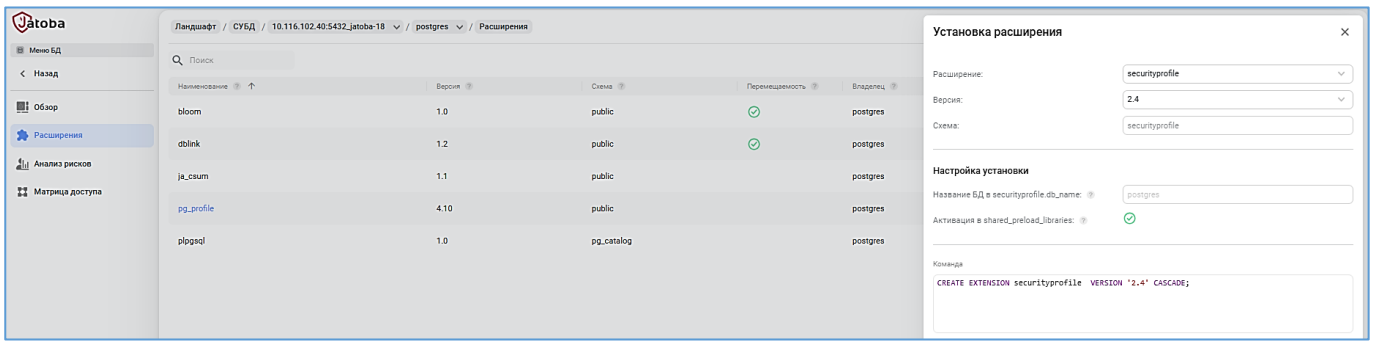

Рисунок 16.11 – Установка расширения securityprofile

После установки компонента securityprofile немедленно обновите пароль для пользователя postgres.

Дополнительно измените аутентификационную информацию в разделах для подключения к целевой СУБД.

В случае если блокировка произошла, выполните действия, описанные в документе «Руководство администратора» в п.п.:

— 16.1. Временная блокировка пользователей СУБД и суперпользователя;

— 16.2. Блокировка суперпользователя СУБД.

После установки расширения оно отобразится в форме гиперссылки во вкладке «Управление расширениями».

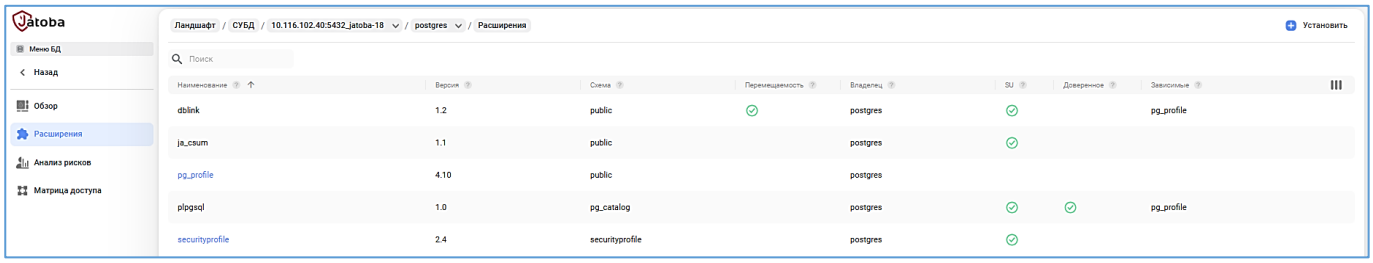

Рисунок 16.12 – Гиперссылка расширения securityprofile

Переход по гиперссылке раскроет вкладки «Обзор» и «Параметры».

Во вкладке «Обзор» отображаются параметры:

— Версия – версия расширения;

— Владелец – владелец расширения;

— Расположение – IP-адрес СУБД / версия СУБД/ БД в которой установлено расширение.

Во вкладке «Параметры» отображаются параметры приведенные в таблице 16.3.

Таблица 16.3 – Отображаемые параметры расширения securityprofile

Параметр	**Значение**	**Описание параметра**
Profiles_cache_limit	10	Максимальное количество профилей, хранимых в кэше
Accounts_cache_limit	1000	Максимальное количество пользовательских аккаунтов, хранимых в кэше
Password_history_cache_limit	10000	Максимальное количество парольных хэшей (md5), хранимых в кэше
Status_cache_limit	100	Максимальное количество статусов блокировки пользователей, хранимых в кэше

Настройки парольных политик описана в разделе 14 «Раздел «Ландшафт». СУБД. Вкладка «Парольные политики» (Password policies).

16.4. БД. Установка расширения ja_csum (контроль целостности)

Рекомендуется устанавливать расширения «ja_CSum» и «SecurityProfile» вручную в соответствии с документом «Руководство по настройке. Часть 14. Контроль целостности. Компонент «ja_CSum».

Установка расширения «ja_CSum» требует предварительного внесения параметра загрузки расширения в конфигурационном файле «postgresql.conf» вручную на целевом хосте или используя раздел JDS «Параметры СУБД» (см. раздел 6).

В разделе «Shared Library Preloading», для последующей загрузки расширения, устанавливается параметр:

```
shared_preload_libraries = 'ja_csum'
```

При совместном использовании компонентов «securityprofile» и «ja_CSum», в разделе «Shared Library Preloading» для последующей загрузки расширений устанавливаются параметры:

```
shared_preload_libraries = 'securityprofile, ja_csum'
```

Применив параметры станет доступна установка расширения «ja_CSum» в стандартном порядке установки расширений.

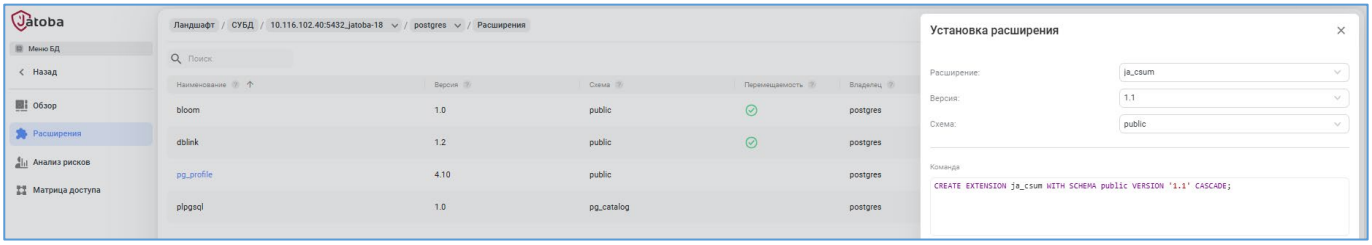

Рисунок 16.13 – Окно установки расширения ja_csum

17. РАЗДЕЛ «ЛАНДШАФТ». БД. ВКЛАДКА «МАТРИЦА ДОСТУПА» (ACCESS MATRIX)

Матрица доступа отражает назначенные атрибуты пользователей, объекты доступа и имеющиеся привилегии пользователей относительно этих объектов.

Объектами доступа являются:

— схемы (schemas);

— таблицы (tables);

— представления (views);

— мат. представления (views);

— функции (functions);

— последовательности (sequences).

Подраздел «Матрица доступа» располагается на уровне базы данных.

Для перехода к нему потребуется в разделе «Ландшафт» выбрать СУБД во вкладке «Дерево инфраструктуры» и в раскрывающемся списке перейти на уровень БД.

Матрица доступа построится автоматически относительно всех субъектов доступа и объектов доступа.

Субъектами доступа являются пользователи СУБД, т.е. роли обладающие, как минимум атрибутом «Login». При этом учитываются привилегии, установленные групповыми ролями, к которым отнесен пользователь.

Атрибуты пользователей отражаются после имени пользователя в виде аббревиатур, которые приведены в таблице 17.1, в виде пиктограммы.

Таблица 17.1 – Аббревиатуры атрибутов ролей

SU	SUPERUSER
INH	INHERIT
CRR	CREATEROLE
CRDB	CREATEDB
L	LOGIN
REP	REPLICATION
BRls	BypassRls

Аббревиатуры атрибутов ролей идентичны в разделах User Risk и Access matrix.

Привилегии пользователей отражаются в полях сформированной таблицы в виде аббревиатур, которые приведены в таблице 17.2, разделенные точками.

Таблица 17.2 – Условные обозначения привилегий пользователей

S	Select
In	Insert
Up	Update
D	Delete
T	Truncate
Ex	Execute
Us	USAGE

Системные привилегии в матрице доступа не отображаются.

17.1. Выбор субъектов

Выбор субъектов доступа доступен через пиктограмму, расположенную в правой верхней части окна.

Нажатие на пиктограмму вызовет окно субъектов доступа (пользователей), в котором снятием флагов ограничивается список субъектов для обновления матрицы.

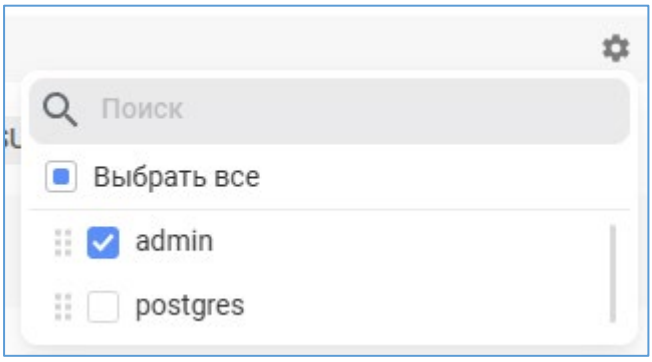

Рисунок 17.1 – Окно субъектов доступа

При установке или снятии флага матрица перестраивается автоматически.

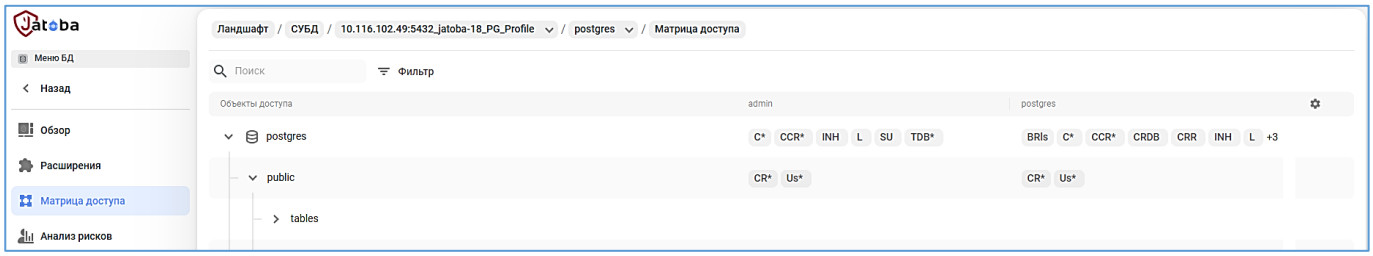

Рисунок 17.2 – Вид «Матрицы доступа»

17.2. Фильтр «Матрицы доступа»

Сформированную матрицу доступа возможно отфильтровать по требуемым критериям. К таким критериям относятся:

— Объекты доступа (Access objects);

— Роли (Roles);

— Атрибуты ролей (Role attributes);

— Привилегии ролей (Role privileges).

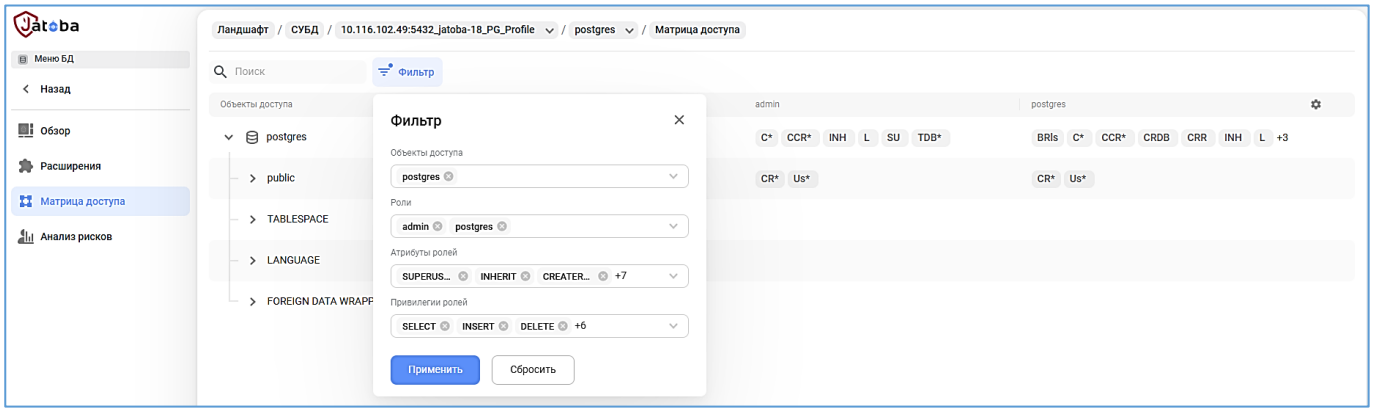

Рисунок 17.3 – Вид окна фильтра «Матрицы доступа»

В фильтре отсутствуют прямые зависимости между полями фильтрации.

Отфильтровать «Матрицу доступа» возможно по каждому из параметров полей или в сочетании параметров.

Поле «Объекты доступа» (Access objects)

В поле допустим выбор объектов только через выпадающий список. Окно «Фильтрация объектов доступа» (Access objects filtering) отображает в древовидной форме структуру БД.

В отражаемой структуре реализованы следующие функциональные возможности, которые можно выбрать простановкой соответствующих флагов:

— выбор объектов по типу;

— выбор конкретного объекта;

— выбор всех объектов (Select All).

Также поиск по названию объекта, который выполняется вводом названия искомого объекта.

Древовидная форма структуры БД перестроится без сокрытия типов объектов, отобразит найденные объекты. Требуемые объекты отмечаются флагом.

Список объектов и их количество отразится в поле «Объекты доступа».

Поле «Роли»

В поле «Роли» выбираются те роли СУБД, по которым требуется сформировать матрицу доступа.

Роли (пользователи) СУБД отображаются в выпадающем списке, в алфавитном порядке.

В списке ролей реализованы следующие функциональные возможности, которые можно выбрать простановкой соответствующих флагов:

— контекстный поиск и выбор роли;

— единичный выбор роли;

— множественный выбор ролей;

— выбор всех ролей (Select All).

Для контекстного поиска достаточно ввести в поле «Роли» от 1 символа и более. Список ролей будет автоматически перестраиваться.

Поле «Атрибуты ролей» (Role attributes)

В поле «Атрибуты ролей» возможно выбрать атрибуты для фильтрации матрицы доступа.

В списке ролей реализованы следующие функциональные возможности, которые можно выбрать простановкой соответствующих флагов:

— контекстный поиск атрибута роли;

— единичный атрибута роли;

— множественный атрибутов ролей;

— выбор всех атрибута роли (Select All).

Поле «Привилегии ролей» (Role privileges)

В поле «Привилегии ролей» отображаются привилегии ролей относительно объектов БД.

Поле обладает всеми функциональными возможностями, которые были описаны выше в других полях фильтра матрицы доступа.

18. РАЗДЕЛ «ЛАНДШАФТ». БД. ВКЛАДКА «АНАЛИЗ РИСКОВ» (USER RISK)

Вкладка «Анализ рисков» (User Risk) логически связана с вкладкой «Матрица доступа» (Access Matrix) (17), т.к. в совокупности полученных данных можно получить объективную картину доступа субъектов доступа к объектам доступа. При этом в разделах отражается информация о групповых ролях и назначенным им атрибутам и привилегиям, которые наследуют роли пользователей.

В частности, «Анализ рисков» (User Risk) предоставляет количественные показатели системных привилегий и атрибутов ролей относительно схемы данных в БД, функционирующей на выбранном сервере.

Представленный отчет выполнен в виде матрицы и диаграммы «Privileges chart».

Подраздел «Анализ рисков» располагается на уровне базы данных.

Для перехода к нему потребуется в разделе «Ландшафт» выбрать СУБД во вкладке «Дерево инфраструктуры» и в раскрывающемся списке перейти на уровень БД.

18.1. Выбор схемы данных (Schema)

Первоначально раздел не выстраивается автоматически. Для построения отчета требуется выбрать схему данных в выпадающем списке, расположенному в левом верхнем углу окна.

18.2. Отображение матрицы

По умолчанию роль PUBLIC отображается в начале списка, приоритет имеют цифры, далее в алфавитном порядке с приоритетом верхнего регистра. Сортировка по столбцам атрибутов и привилегий осуществляется по наличию атрибута/привилегии.

В настройке отображения столбцов таблицы присутствую и выбраны по умолчанию атрибуты и привилегии, приведенные в таблице 18.1.

Таблица 18.1 – Условные обозначения системных привилегий и атрибутов ролей

Обозначение	**Привилегии и атрибуты**	**Описание**	**Отображение по умолчанию**
Привилегии пользователей на вложенные объекты уровня БД			
STb	SELECT TABLE	Чтение	X
UpTb	UPDATE TABLE	Создание	X
ITb	INSERT TABLE	Изменение	X

Обозначение	Привилегии и атрибуты	Описание	Отображение по умолчанию
DTb	DELETE TABLE	Удаление	X
TrTb	TRUNCATE TABLE	Удаление всех строк	X
Системные привилегии			
RTb	REFERENCES TABLE	Использование зависимых таблиц	X
TgTb	TRIGGER TABLE	Установка триггеров на таблицы	X
EFn	EXECUTE FUNCTION	Выполнение функций	X
EPr	EXECUTE PROCEDURE	Выполнение процедур	X
SSq	SELECT SEQUENCE	Получение значения счетчиков	
UpSq	UPDATE SEQUENCE	Обновление значения счетчиков	
USq	USAGE SEQUENCE	Использование счетчика	
CrDB	CREATE DATABASE	Создание базы данных	
CnDB	CONNECT DATABASE	Подключение к базе данных	
TDB	TEMPORARY DATABASE	Использование временных таблиц	
CrTS	CREATE TABLESPACE	Создание табличного пространства	
CrSc	CREATE SCHEMA	Создание схемы	
USc	USAGE SCHEMA	Использование схемы	
UpLO	UPDATE LARGE OBJECT	Изменение данных в больших объектах	
SLO	SELECT LARGE OBJECT	Получение больших объектов	
UFDW	USAGE FOREIGN DATA WRAPPER	Использование внешних источников данных	
UFS	USAGE FOREIGN SERVER	Использование внешних серверов	
UD	USAGE DOMAIN	Использование домена	
ULn	USAGE LANGUAGE	Использования языка программирования	
UTy	USAGE TYPE	Использование тип	X
Атрибуты ролей			
SU	SUPERUSER	Роль «Супер пользователь» обладает полными правами доступа к СУБД	X
INH	INHERIT	Роли, имеющие атрибут «INHERIT», автоматически используют права всех ролей, членами которых они являются, в том числе и унаследованные этими ролями права	X
CRR	CREATEROLE	Роль имеет разрешение на создание других ролей	X

Обозначение	Привилегии и атрибуты	Описание	Отображение по умолчанию
CRD	CREATEDB	Роль имеет разрешение на создание базы данных	X
L	LOGIN	Роль с атрибутом «LOGIN» рассматривается, как роль пользователя базы данных, а также может использоваться для начального подключения к базе данных	X
REP	REPLICATION	Роль имеет разрешение на запуск потоковой репликации	X
BRLS	BYPASSRLS	Атрибут роли, определяющий игнорирование все политики защиты на уровне строк (RLS – Row Level Security)	X

18.3. Диаграмма

Диаграмма представляет количественную оценку суммарного количества предоставленных системных привилегий и количества установленных атрибутов пользователей.

Цветовая индикация SU (Superuser) и выбранного столбца отображается на диаграмме (рисунок 18.1).

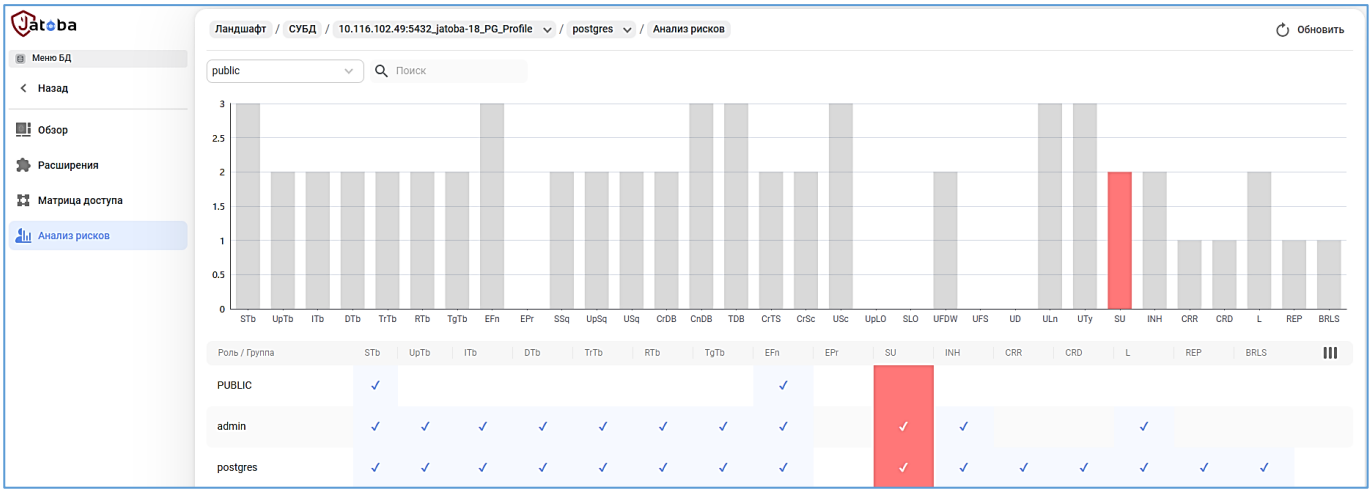

Рисунок 18.1 – Цветовая индикация

19. РАЗДЕЛ «ЛАНДШАФТ». ВКЛАДКА «КЛАСТЕРЫ JADOG»

Работа компонента по управлению кластером полностью описана в документе «Руководство по настройке. Часть 1. Управление режимом работы узлов кластера. Компонент «jaDog». 643.72410666.00067-07 98-02-01».

Подключение к существующему кластеру описано в документе «Руководство по безопасности».

Вкладка «Кластеры» в разделе «Ландшафт», отображает список подключенных кластеров.

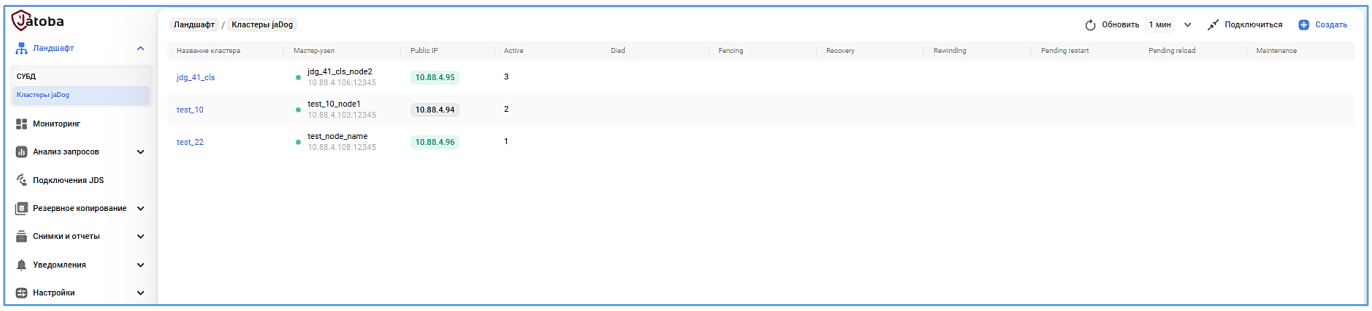

Рисунок 19.1 – Отображение структуры кластера

19.1. Навигация в разделе

Сущности кластера «jaDog» располагаются в двух подразделах с вкладками по следующим путям:

– Раздел Ландшафт → СУБД → Дерево инфраструктуры → Хост → СУБД → Служба jadog:

- Обзор (см. п.п 19.1.1);
- Структура (см. п.п. 19.1.2);
- Репликация (см. п.п. 19.1.3);

– Раздел Ландшафт → Кластеры jaDog:

- Обзор;
- Список узлов (см. п.п. 19.1.5):
  - Параметры.

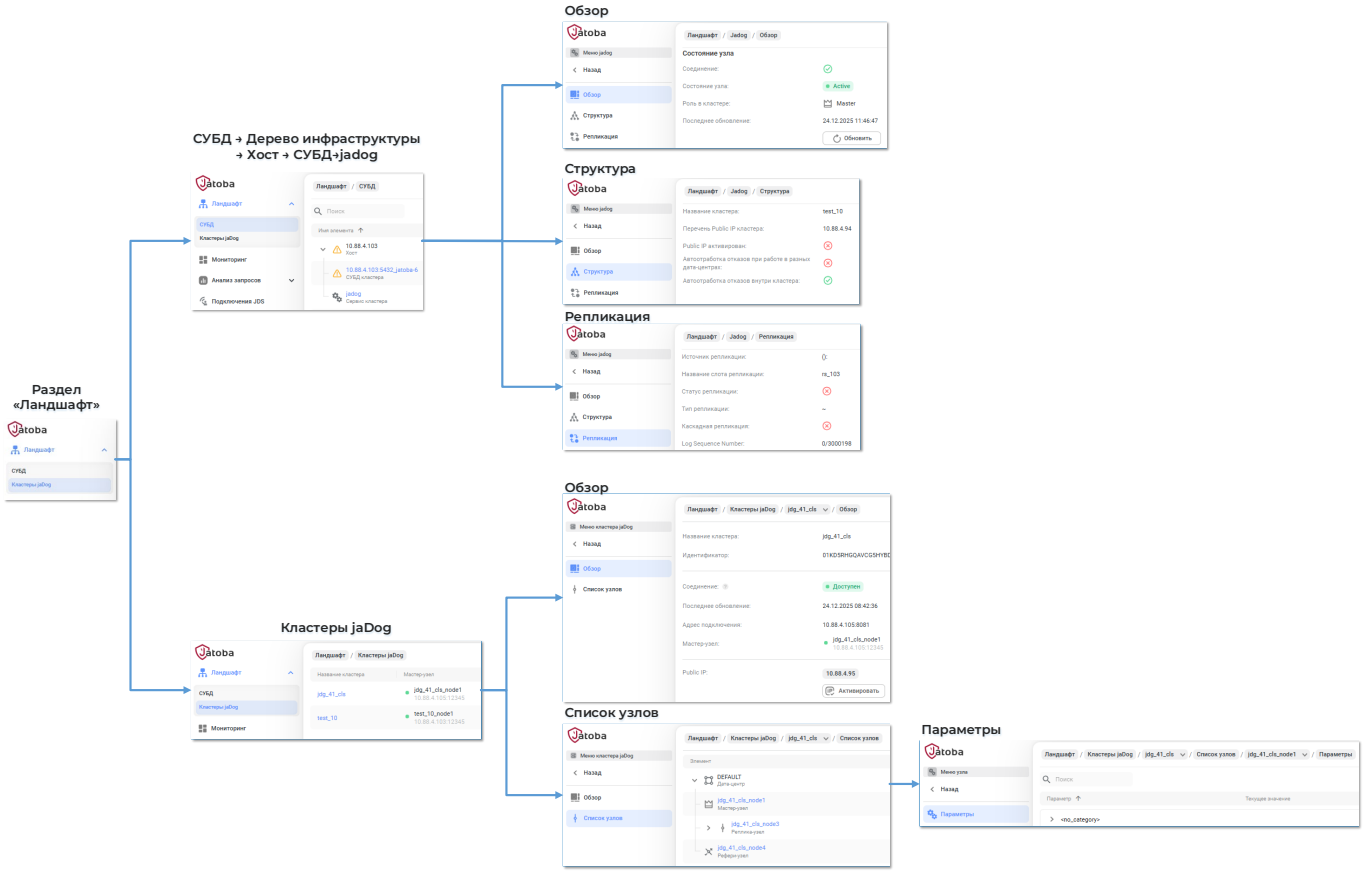

Рисунок 19.2 – Навигация в подразделах Ландшафта

Параметры кластера отображаются на уровне службы «jadog». Для просмотра параметров кластера необходимо перейти по пути: Раздел Ландшафт → СУБД → Дерево инфраструктуры → Хост → СУБД → Служба jadog.

Рисунок 19.3 – Путь к параметрам кластера

Параметры кластера распределены по вкладкам:

— Обзор (см. п.п 19.1.1);

— Структура (см. п.п. 19.1.2);

— Репликация (см. п.п. 19.1.3);

19.1.1. Вкладка «Обзор» параметров узла

Обзор параметров узла кластера сгруппирован по блокам приведенным в таблице 19.1.

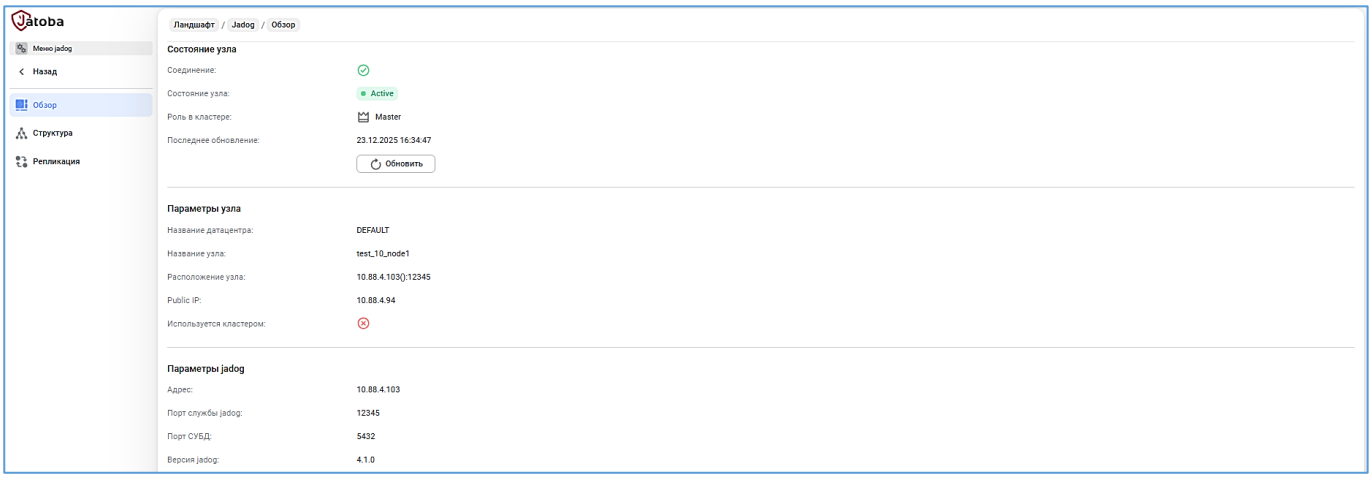

Рисунок 19.4 – Вкладка «Обзор» параметров кластера

Таблица 19.1 – Перечень параметров во вкладке «Обзор»

Параметр	**Описание параметра**
Состояние узла	
Соединение:	Отображается значение параметра «Connection state» в форме знаков true/false
Состояние узла:	Отображается значение параметра «NodeState»
Роль в кластере:	ClusterState Master/Slave/Referee
Последнее обновление	Дата и время последнего обновления состояния кластера
Параметры узла	
Название дата-центра	Отображается название дата-центра
Название узла	Название узла в кластере
Расположение узла	IP-адрес и порт узла
Public IP	Используемый публичный IP-адрес
Используется кластером	Знак true/false использования публичного IP-адреса
Параметры jadog	
Адрес:	IP-адрес узла
Порт службы jaDog	Порт узла
Порт СУБД	Порт СУБД
Версия jaDog	Версия компонента jaDog

19.1.2. Вкладка «Структура»

Во вкладке отображаются следующие не редактируемые параметры:

— Название кластера;

— Перечень Public IP кластера;

— Public IP активирован;

— Автоотработка отказов при работе в разных дата-центрах;

— Автоотработка отказов внутри кластера;

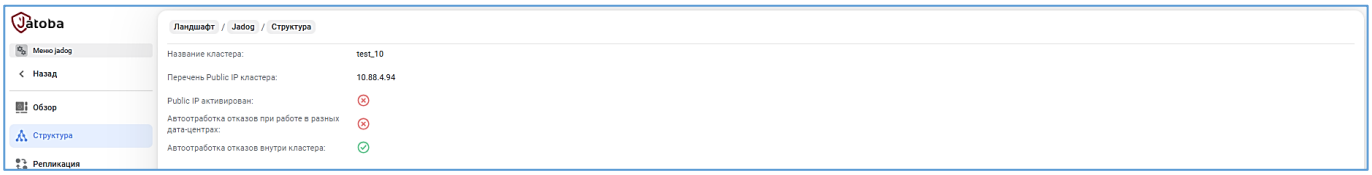

Рисунок 19.5 – Структура кластера

19.1.3. Вкладка «Репликация»

Во вкладке «Репликация» отображаются следующие не редактируемые параметры:

— Источник репликации;

— Название слота репликации;

— Статус репликации;

— Тип репликации;

— Каскадная репликация;

— Log Sequence Number.

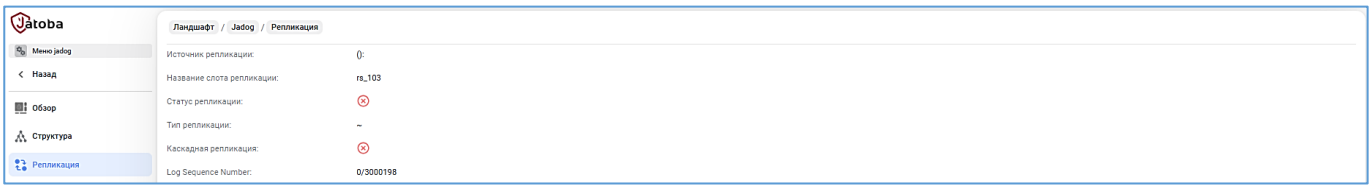

Рисунок 19.6 – Вкладка «Репликация»

19.1.4. Вкладка «Обзор» кластера

Во вкладке «Обзор» отображаются следующие не редактируемые параметры:

— Название кластера;

— Название кластера;

— Соединение;

— Последнее обновление;

— Адрес подключения;

— Мастер-узел;

— Public IP.

А также расположена кнопка Активации/деактивации Public IP кластера.

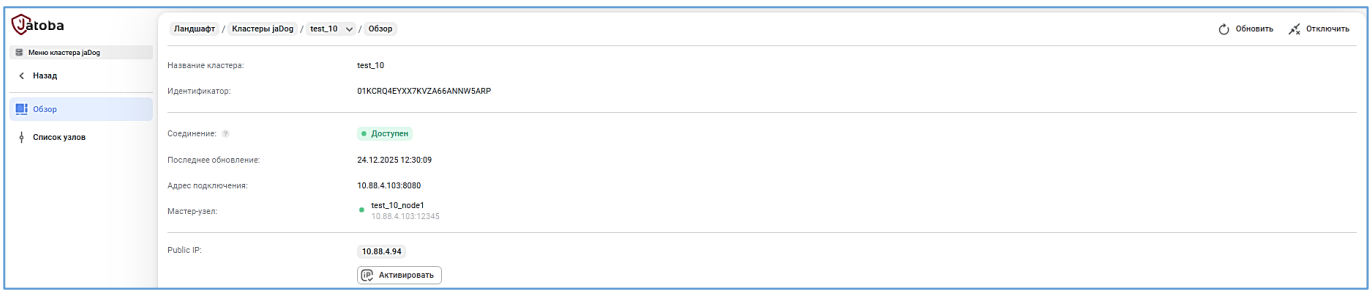

Рисунок 19.7 – Вкладка «Обзор» кластера

19.1.5. Вкладка «Список узлов»

Вкладка «Список узлов» является основной вкладкой, в которой отображается структура кластера и выполняются основные операции над кластером.

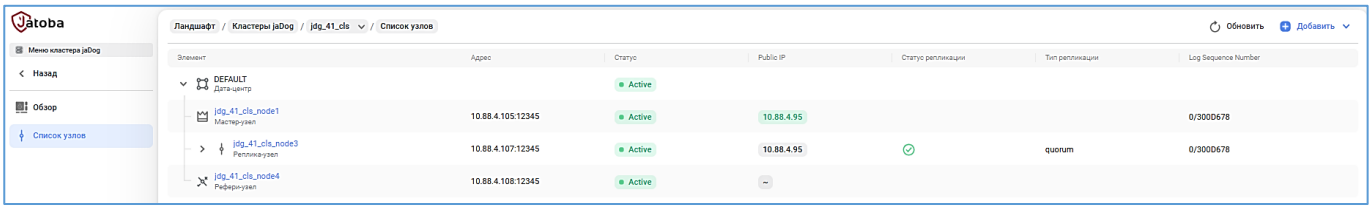

Рисунок 19.8 - Вкладка «Список узлов»

Структура кластера отражается в виде иерархического списка. По умолчанию узлы кластера будут соотнесены к дата-центру с именем «Default».

Узлы кластера отображаются гиперссылкой, переход по которой ведет во вкладку «Параметры» (см. п.п. 19.1.6).

В столбце «Адрес» отображается IP-адрес и порт.

В столбце «Статус» отображаются состояния узла:

— ACTIVE – устойчивое состояние узла;

— INACTIVE – не активный;

— DIED – неработоспособный;

— RECOVERY – узел в режиме восстановления;

— FENCING – узел оказался в сегменте кластера, где не достигнут кворум по выбору нового главного узла;

— PROMOTING – резервный узел в процессе преобразования в главный;

— REWINDING – резервный узел в процессе переключения на новый главный узел.

— STARTING – узел находится в состоянии запуска.

— RESTARTING – узел находится в состоянии перезапуска.

— DEMOTING – главный узел в процессе преобразования в резервный;

— DELETING – узел удаляется;

— STOPPED – узел остановлен;

— MAINTENANCE – узел в режиме технического обслуживания;

— CANDIDATE - узел в режиме выбора кандидата (голосование) на роль главного узла кластера (master)

— INIT – узел в состоянии инициализации.

В поле «Статус» Дата-центра отображаются возможные состояния:

— ACTIVE – активный,

— EMPTY – пустой,

— INACTIVE – не активный.

Public IP отображается у всех узлов кластера и отличается цветовой градацией. Только у узла с ролью «Master» Public IP подсвечен зеленым цветом.

Узлы кластера могут иметь роли и делиться по типам:

— «Master» - главный-узел;

— «Slave» - подчиненный резервный узел (Primary Slave) и подчиненный каскадный узел (Cascade Slave);

— «Referee» - узел-арбитр.

Операции над узлами кластера выполняются через контекстное меню строки узла.

Узел с ролью «Master» возможно только «Присоединить к дата-центру» и «Отсоединить от дата-центра».

Над узлом с ролью «Slave» доступны операции:

— «Присоединить к дата-центру»;

— «Отсоединить от дата-центра»;

— «Сделать мастером»;

— «Удалить узел».

Над узлом с ролью «Slave» с типом подчиненный каскадный узел (Cascade Slave) доступна операция «Удалить узел».

Над узлом с ролью «Referee» доступны операции:

— «Присоединить к дата-центру»;

— «Отсоединить от дата-центра»;

— «Удалить узел».

19.1.6. Вкладка «Параметры»

Параметры компонента «jaDog» отражены во вкладке «Параметры». Параметры являются редактируемыми, полный перечень которых приведен в документе «Управление режимом работы узлов кластера. Компонент «jaDog».

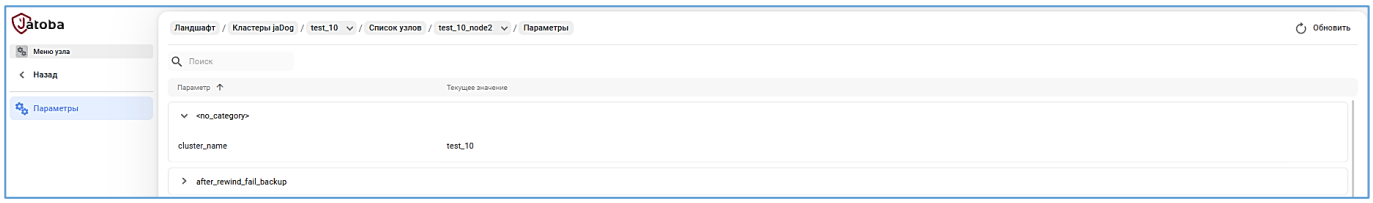

Рисунок 19.9 - Параметры компонента «jaDog»

Изменение значений подтверждается информационным сообщением. Новые значения параметра применяются моментально.

Однако, для отдельных параметров и их применения требуется перечитать конфигурацию, т.е. применить новые параметры в конфигурационном файле узла кластера.

В информационной строке выводится сообщение:

```
Узел требует перечитывания конфигурации.Перечитать
```

Нажатие гиперссылки «Перечитать» вызовет окно подтверждения и в итоге выполнит операцию пересчета и применения конфигурации узла кластера.

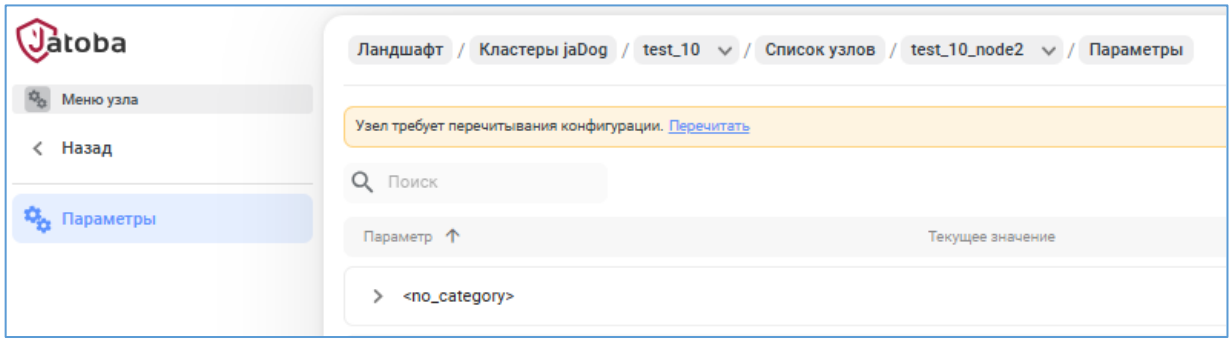

Рисунок 19.10 – Кнопки «Обновить» и «Перечитать конфигурацию»

19.2. Подключение к существующему кластеру

Подключение к существующему кластеру описано в документе «Руководство по безопасности».

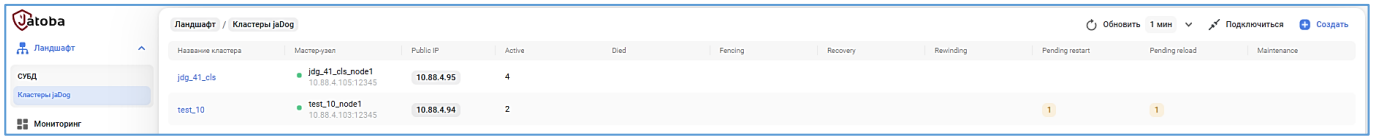

Рисунок 19.11 – Расположение кнопки «Подключить»

Кластер не может быть добавлен дважды. При подключении к существующему кластеру выполняется проверка уникальности идентификатора кластера.

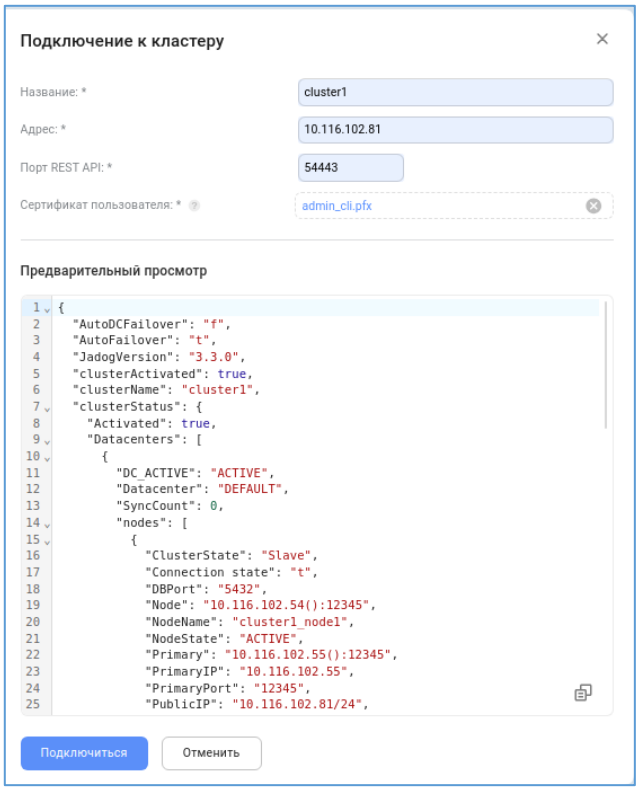

Рисунок 19.12 – Подключение к кластеру

19.3. Создание кластера

Создание кластера подразумевает следующую последовательность действий:

— администратор создает кластер на базе первого узла мастера;

— администратор добавляет X узлов с нужными ролями;

— администратор проводит необходимые настройки кластера;

— администратор переносит данные;

— администратор убеждается в корректности работы кластера;

— администратор разрешает клиентские подключения к кластеру через «Public IP», используя элемент в интерфейсе «Активировать Public IP» (см. п. 19.5).

Создание кластера доступно в разделе «Ландшафт», во вкладке «Кластеры jaDog» нажатием кнопки «Создать».

Рисунок 19.13 – Окно «Создание кластера»

Вызвав окно «Создание кластера» вводится:

— Имя кластера;

— Адрес REST API сервера, на базе которого создается кластер;

— Порт REST API сервера, через который будут проводится команды;

— Сертификат пользователя в формате *.pfx.

Компонент JDS не запрашивает порт экземпляра jaDog.

19.4. Подключение узла кластера

Добавление узла в кластер выполняется во вкладке «Список узлов», через кнопку «Добавить» и в меню выбрав опцию «Узел».

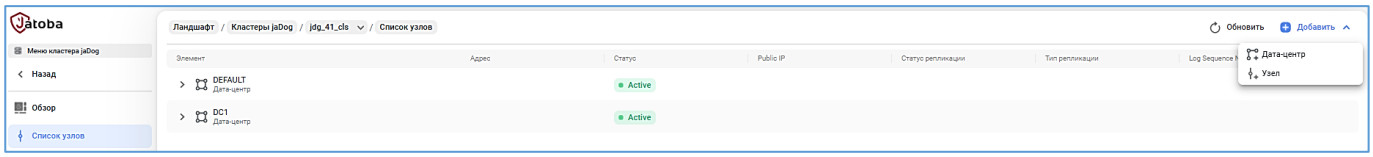

Рисунок 19.14 – Контекстное меню кластера

В окне «Добавление узла в кластер» требуется указать:

— Название;

— Адрес - IP-адрес или DNS-имя узла кластера;

— Порт подключения к узлу: 12345

По умолчанию используется порт 12345, однако порт может отличаться в зависимости от настроек компонента jaDog.

— Роль - роль узла Slave/Referee.

— Тип репликации (Асинхронная/Синхронная);

— Каскадная репликация – репликация с указанного узла Slave.

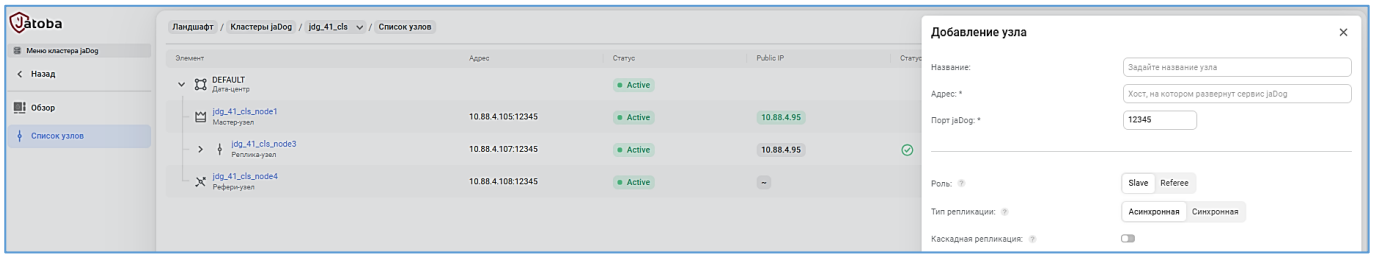

Рисунок 19.15 – Окно добавления узла в кластер

Если хост был ранее добавлен в раздел «Ландшафт», то после использования его в качестве узла кластера потребуется переустановить пароль в разделе «Назначение ролей»

19.4.1. Каскадная репликация

Возможно добавить узел кластера с каскадной репликацией только с ролью «Slave» от существующего узла кластера с ролью «Slave».

В окне «Добавление узла», при установке переключателя «Каскадная репликация», появится поле «Источник репликации» с выпадающим списком. В выпадающем списке отразятся узлы с ролью «Slave». От выбранного узла будет реплицироваться новый узел.

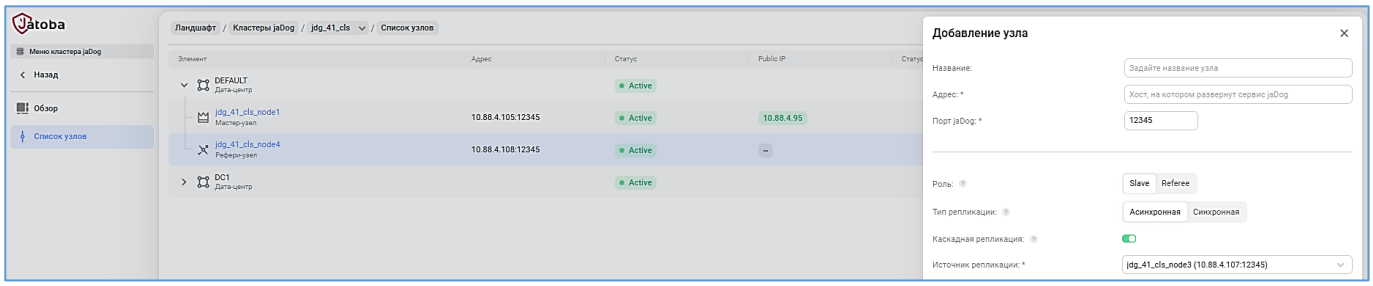

Рисунок 19.16 – Окно добавления узла в кластер с каскадной репликацией

19.5. Активация/деактивация PublicIP кластера

В настройках каждого jaDog узла есть параметр Public IP. При работе узлов в составе кластера, один из узлов работает в роли "Мастер". Если Public IP активирован, значение его параметра становится актуальным для соединения с кластером.

При обслуживании кластера, могут выполняться следующие действия:

— администратор запрещает клиентские подключения к кластеру через Public IP, используя элемент в интерфейсе «Деактивировать Public IP»;

— администратор читает журнал аудита компонентов, проверяет настройки, выясняет причину неполадок;

— администратор проводит необходимые действия по устранению причин неполадок;

— администратор убеждается в корректности работы кластера;

— администратор разрешает клиентские подключения к кластеру через Public IP, используя элемент в интерфейсе "Активировать Public IP".

Кнопка «Актировать/деактивировать» расположена по пути: Раздел «Ландшафт» - Вкладка «Кластеры» - уровень кластера в дереве кластеров.

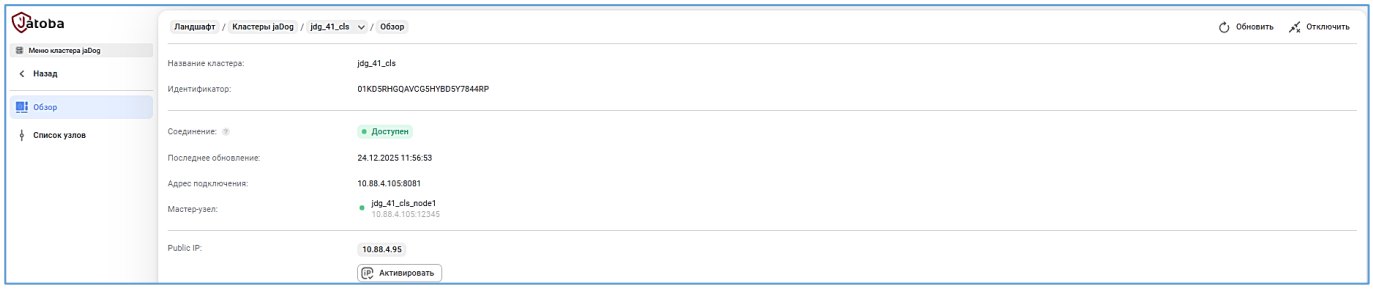

Рисунок 19.17 - Кнопка «Актировать/деактивировать»

19.6. Назначение узлу роли Мастер

Имеющийся узел с ролью «Slave» возможно назначить на роль «Master».

В строке узла потребуется вызвать контекстное меню и выбрать опцию «Сделать мастером».

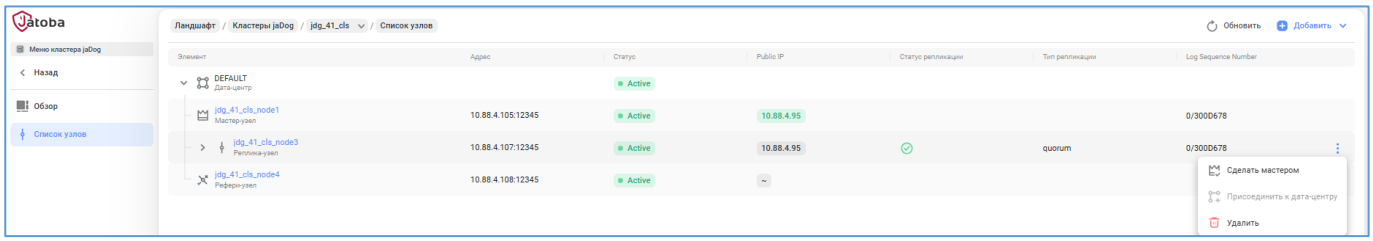

Рисунок 19.18 – Контекстное меню узла с ролью «Slave»

После чего компонент выведет окно предупреждения и получив подтверждение, начнётся процедура смены ролей кластера (switchover).

Для узла с каскадной репликацией назначение роли «Master» недоступно.

19.7. Удаление узла

Узел с ролью «Master» возможно удалить только после последовательного удаления всех связанных с ним узлов, таких как «Slave» или «Referee».

В строке узла потребуется вызвать контекстное меню и выбрать опцию «Удалить», как представлено на рисунке 19.18.

После чего компонент выведет окно предупреждения.

Удаленный узел не будет отражаться в списке узлов.

Удаление узлов в кластере с каскадной репликацией имеет свои особенности. Первоначально удаляется узел кластера с каскадной репликацией, после чего целесообразно удалять узел с ролью «Slave» относительно узла с ролью «Master».

19.8. Дата-центр

Дата-центр — это логическая сущность в JDS, позволяющая сопоставить узлы кластера по подсетям в Дата-центрах.

Узлы могут иметь статусу:

— ACTIVE – устойчивое состояние узла;

— INACTIVE – не активный;

— DIED – неработоспособный;

— RECOVERY – узел в режиме восстановления;

— FENCING – узел оказался в сегменте кластера, где не достигнут кворум по выбору нового главного узла;

— PROMOTING – резервный узел в процессе преобразования в главный;

— REWINDING – резервный узел в процессе переключения на новый главный узел.

— STARTING – узел находится в состоянии запуска.

— RESTARTING – узел находится в состоянии перезапуска.

— DEMOTING – главный узел в процессе преобразования в резервный;

— DELETING – узел удаляется;

— STOPPED – узел остановлен;

— MAINTENANCE – узел в режиме технического обслуживания;

— CANDIDATE - узел в режиме выбора кандидата (голосование) на роль главного узла кластера (master)

— INIT – узел в состоянии инициализации.

Работа кластера в разных подсетях и соответственно в разных Дата-центрах требует подготовительных действий, т.к. конфигурационный файл правил аутентификации в СУБД «pg_hba.conf» не настраивается автоматически на разные подсети при конфигурировании узла кластера.

Схема первоначального состояния узлов кластера представлена на рисунке 19.19

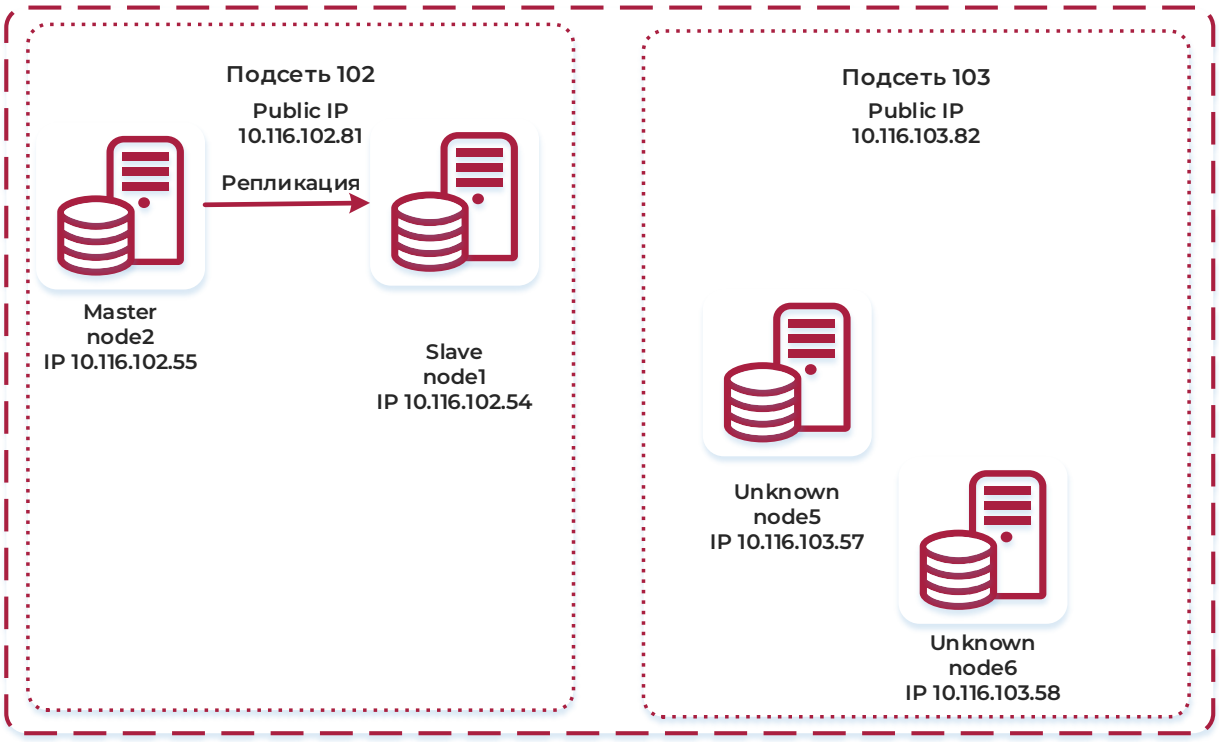

Рисунок 19.19 – Начальное состояние узлов кластера

В рассматриваемом примере узлы кластера имеют сетевую адресацию, представленную в таблице 19.2.

Таблица 19.2 – Сетевая адресация серверов стенда кластера «jaDog» для работы в Дата-центре

№	Имя сервера	IP-адрес	Маска подсети	Public IP	Роль/ состояние	Дата-центр
1	**JDS**	10.116.102.40	255.255.255.0			
	Подсеть 102					
2	**Node1**	10.116.102.54/24	255.255.255.0	10.116.102.81/24	Slave	dc1
3	**Node2**	10.116.102.55/24	255.255.255.0	10.116.102.81/24	Master	dc1
4	**Node3**	10.116.102.57/24	255.255.255.0			
5	**Node4**	10.116.102.58/24	255.255.255.0			
	Подсеть 103					
6	**Node5**	10.116.103.57/24	255.255.255.0	10.116.103.82/24	Unknown	dc2
7	**Node6**	10.116.103.58/24	255.255.255.0	10.116.103.82/24	Unknown	dc2

Дата-центры еще не сформированы.

Узел Node2 выполняет роль «Master», Узел Node1 выполняет роль «Slave» и сконфигурирован на публичный IP-адрес 10.116.102.81/24.

Узлы Node5 и Node6 являются свободными и сконфигурированы на публичный IP-адрес 10.116.103.82/24.

19.8.1. Подготовительные действия для создания кластера

На узле Node2 с роль «Master» потребуется внести дополнительные параметры для подключения узлов в другой подсети, внеся следующие строки:

```
host all                <имя пользователя> <адрес подсети> md5
host replication        <имя пользователя> <адрес подсети> md5
```

```
mc [root@node2]:/var/lib/jatoba/5/data
GNU nano 6.2          /var/lib/jatoba/5/data/pg_hba.conf *

# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     md5
# IPv4 local connections:
host    all             jadog_user      127.0.0.1/32            md5
host    all             jadog_user      10.116.102.0/24         md5
host    all             jadog_user      10.116.103.0/24         md5
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     md5
host    replication     all             127.0.0.1/32            md5
host    replication     jadog_user      10.116.102.0/24         md5
host    replication     jadog_user      10.116.103.0/24         md5
host    replication     all             ::1/128                 md5
```

Рисунок 19.20 – Параметры конфигурационного файлы pg_hba.conf на узле «Master»

Сохранить внесенные изменения.

Рекомендуется использовать надежный метод аутентификации «SCRAM-SHA-256»

Применение параметров целесообразнее выполнить не через перезагрузку служб, а через SQL-команду. Для чего от имени и справами пользователя «postgres», войти в СУБД и выполнить SQL-команду:

```
SELECT pg_reload_conf();
```

```
root@node2: /home/admin1
postgres@node2:/home$ cd /usr/jatoba-5/bin/
postgres@node2:/usr/jatoba-5/bin$ psql
Password for user postgres:
psql (15.5)
Type "help" for help.

postgres=# SELECT pg_reload_conf();
 pg_reload_conf
----------------
 t
(1 row)

postgres=#
```

Рисунок 19.21 – Выполнение перезагрузки параметров СУБД

Далее можно переходить к конфигурированию кластера в Дата-центрах в разделе JDS «Список кластеров».

19.8.2. Создание/удаление Дата-центров

Добавление узла в кластер выполняется во вкладке «Список узлов», через кнопку «Добавить» и в меню выбрав опцию «Дата-центр».

Нажатие на пиктограмму вызовет окно «Создание дата-центра» в правом углу вкладки.

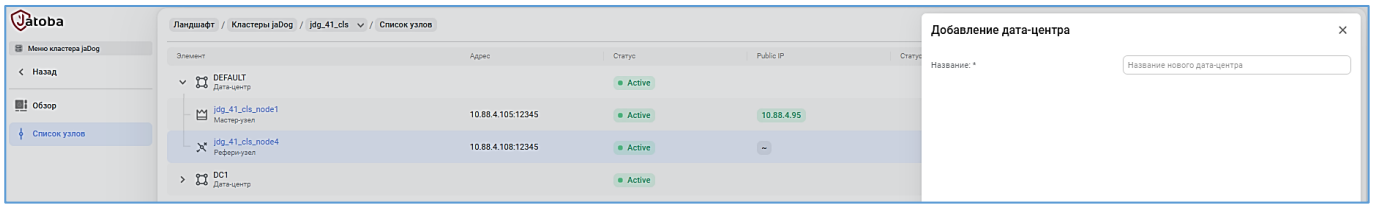

Рисунок 19.22 – Окно «Создание дата-центра»

В поле «Имя дата-центра» вносится требуемое название.

Это соответствует команде в утилите «jadog_ctl»:

```
datacenter create 'name'
```

Для рассматриваемого примера создаются дата-центры:

— «dc1»;

— «dc2».

В контекстном меню Дата-центра находится пункт меню «Удалить».

Удалить возможно только пустой Дата-центр, т.е. Дата- центр, не содержащий в себе узлов кластера.

Невозможно удалить Дата-центр по умолчанию «DEFAULT».

19.8.3. Присоединение узлов кластера к Дата-центру

К созданным дата-центрам присоединим узлы кластера:

— Node1 IP-10.116.102.54/24 и Node2 IP- 10.116.102.55/24 к «dc1»;

— Node5 IP-10.116.103.57/24 и Node6 IP-10.116.103.58/24 к «dc2».

Присоединение к Дата-центрам узлов кластера выполняется в подразделе «Jadog кластеры».

Присоединение к Дата-центрам узлов кластера выполняется во вкладке «Список узлов», в строке узла, через контекстное меню выбрав опцию «Присоединить к дата-центру».

Каждый узел присоединяется отдельно.

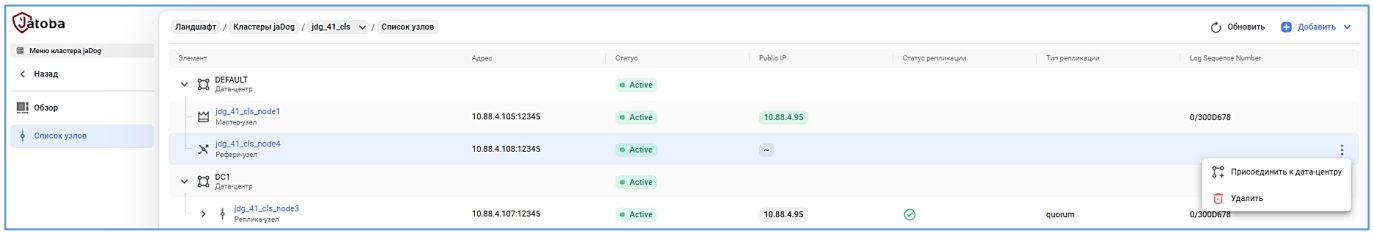

Рисунок 19.23 – Контекстное меню «Присоединить к дата-центру»

Нажатие на меню вызовет одноименное окно.

Поле «Выберите дата-центр» выполнено в виде выпадающего списка, в котором отражаются созданные Дата-центры (см. п. 19.8.2).

Это соответствует команде в утилите «jadog_ctl»:

```
datacenter 'dc1' attach node 10.116.102.54 12345
datacenter 'dc1' attach node 10.116.102.55 12345
datacenter 'dc2' attach node 10.116.103.57 12345
datacenter 'dc2' attach node 10.116.103.58 12345
```

В результате узлы кластера распределены по Дата-центрам. Один узел выполняет роль «Master», остальные узлы работают с ролью «Slave».

В подсети «102» кластер работает с Public IP – 10.116.102.81/24. Второй публичный адрес 10.116.103.82/24 в подсети «103» не используется. Полученная конфигурация кластера представлена в таблице 19.3 и показана на рисунке 19.24.

Таблица 19.3 – Сетевая адресация серверов стенда кластера «jaDog», работающих в Дата-центрах

№	Имя сервера	IP-адрес	Маска подсети	Public IP	Роль/ состояние	Дата-центр
1	**JDS**	10.116.102.40	255.255.255.0			
	Подсеть 102					
2	**Node1**	10.116.102.54/24	255.255.255.0	10.116.102.81/24	Slave	dc1
3	**Node2**	10.116.102.55/24	255.255.255.0	10.116.102.81/24	Master	dc1
4	**Node3**	10.116.102.57/24	255.255.255.0			
5	**Node4**	10.116.102.58/24	255.255.255.0			
	Подсеть 103					
6	**Node5**	10.116.103.57/24	255.255.255.0	10.116.103.82/24	Slave	dc2
7	**Node6**	10.116.103.58/24	255.255.255.0	10.116.103.82/24	Slave	dc2

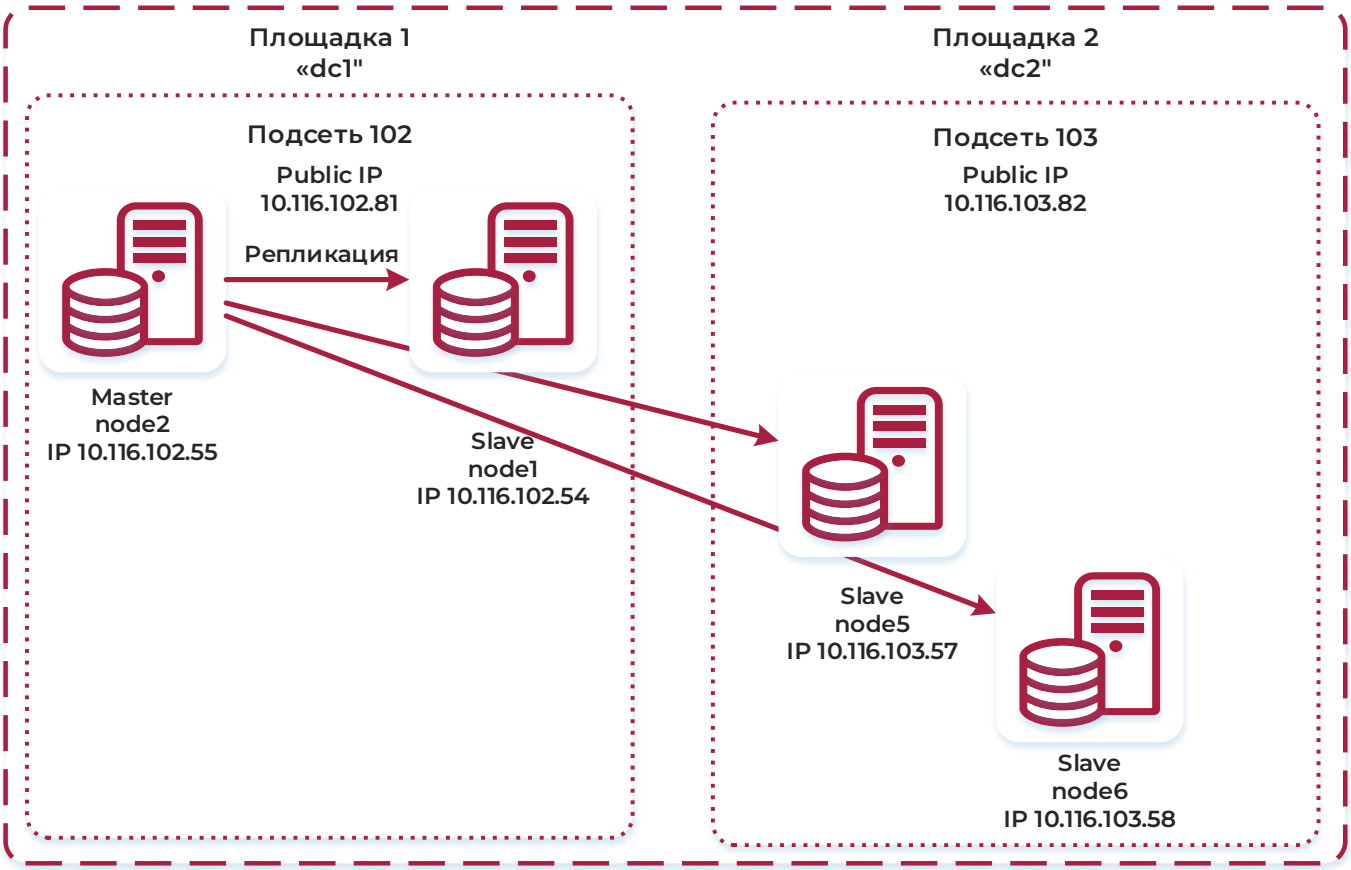

Рисунок 19.24 – Схема кластера в Дата-центрах

19.9. Отключение кластера от JDS

Отключение кластера выполняется через кнопку «Отключить» в правом верхнем углу во вкладке «Обзор» на уровне «Кластеры jaDog».

Данная операция подразумевает отключение кластера от инфраструктуры JDS. При этом он продолжить функционировать, но не будет отражаться во вкладке «Кластеры jaDog».

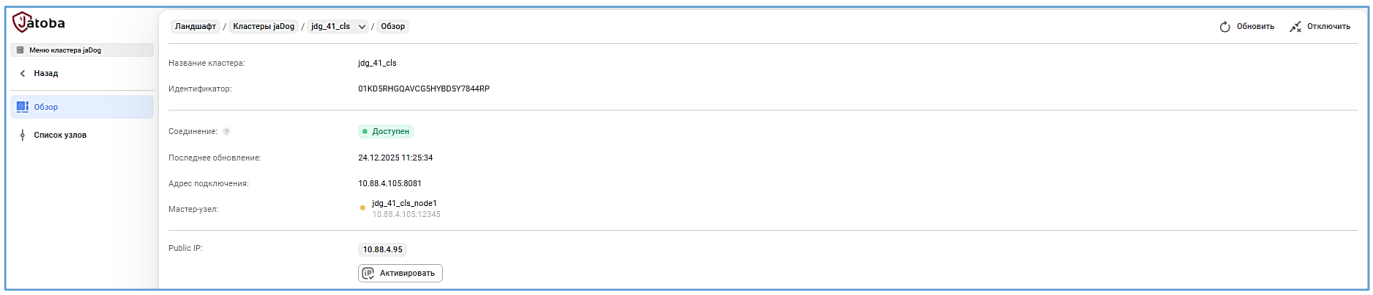

Рисунок 19.25 – Контекстное меню кластера.

После выбора опции «Отключить» компонент выведет окно подтверждения действия.

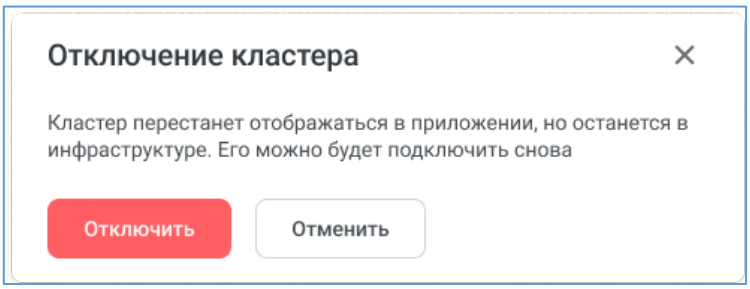

Рисунок 19.26 – Окно «отключение кластера»

Отключенный кластер можно вновь подключить способом, описанным в документе «Руководство по безопасности».

20. РАЗДЕЛ «МОНИТОРИНГ» (MONITORING)

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

Настройка подключения описана в п. 2.3 «Вкладка «Источники данных» настоящего документа.

Информация собирается с компонент:

— «node_exporter» – предназначен для мониторинга и сбора метрик с различных компонентов в системе на основе ОС Linux;

— «postgres_exporter» – предназначен для сбора и экспорта метрик СУБД, таких как статистика по базе данных, нагрузка на сервер, количество запросов и т. д.;

— «sql_exporter» – предназначен для экспорта данных из SQL-запросов в формат, удобный для анализа и визуализации.

Информацию аккумулирует система «PROMETHEUS» и передаёт ее в подраздел «Панель» JDS. Утилита «Alertmanager» обеспечивает контроль над пороговыми значениями и рассылку уведомлений.

Схема взаимодействия компонент представлена на рисунке 20.1.

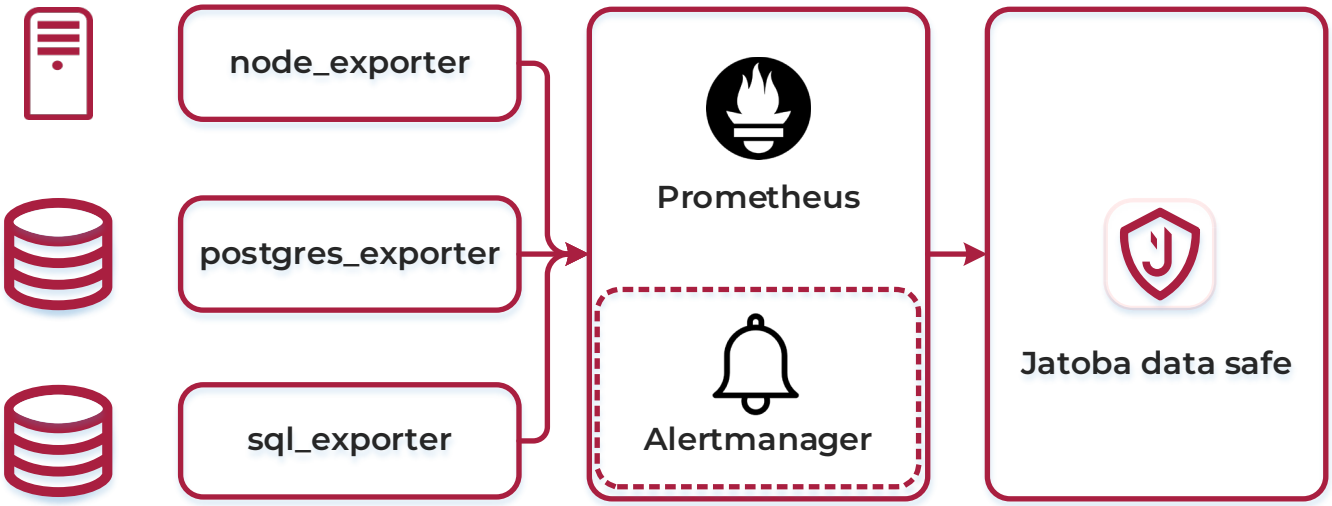

Рисунок 20.1 – Схема взаимодействия компонент для сбора метрик

Настройка вышеуказанных компонент описана в документе «Руководство по настройке. Часть 28. Поддержка мониторинга СУБД».

Во вкладке «Мониторинг» отображаются предустановленный набор виджетов.

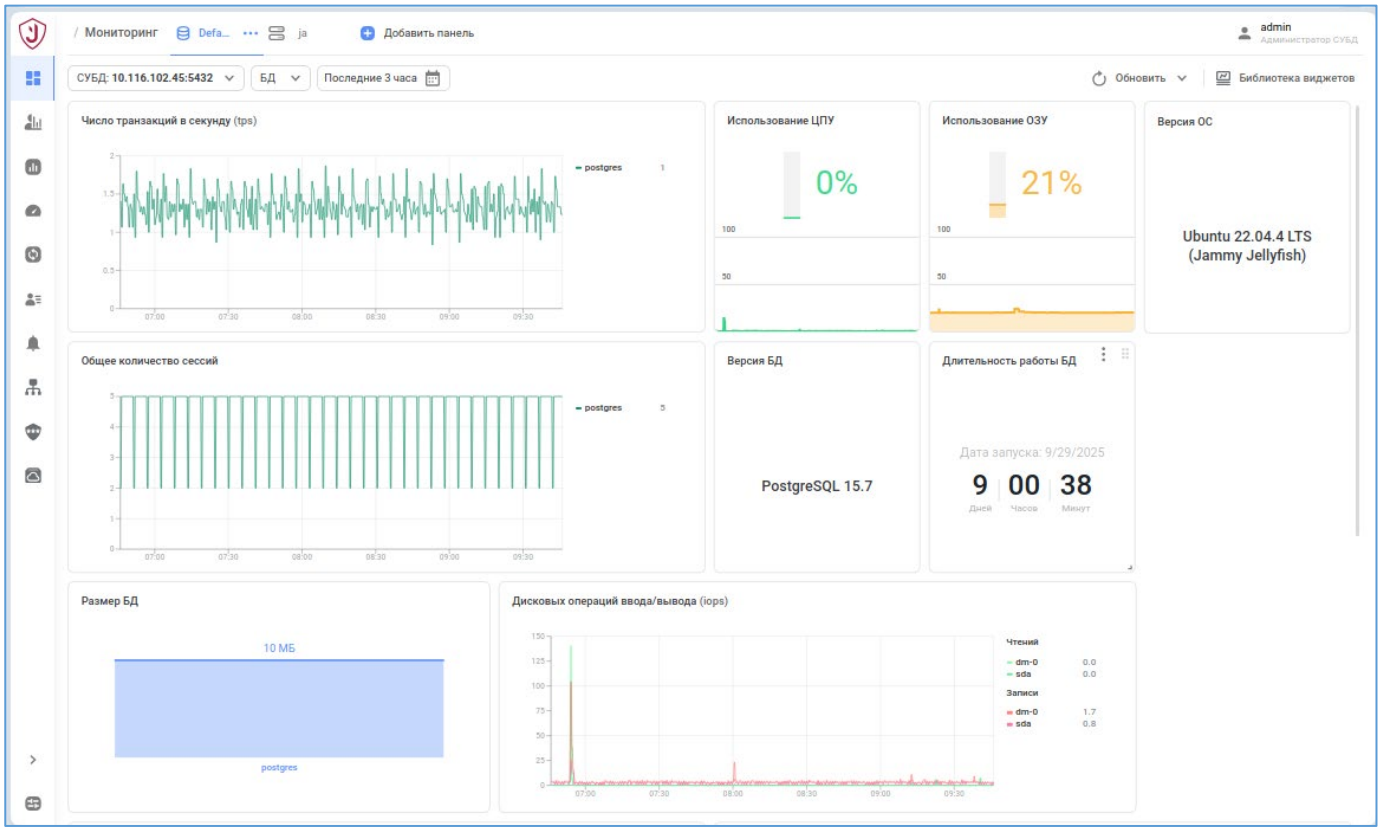

Рисунок 20.2 – Предустановленные виджеты

В верхней строке доступен выбор:

— контролируемой СУБД;

— всех баз данных или единственной БД;

— периода контроля;

— периодичности обновления вкладки;

— библиотека виджетов.

Рабочее пространство возможно организовать созданием вкладок с виджетами или простым выбором виджетов.

20.1. Библиотека виджетов

Библиотека виджетов структурирована по двум вкладкам. На вкладке «Сервер» располагаются виджеты, относящиеся к используемой ОС. На вкладке «БД» располагаются виджеты, относящиеся к работе баз данных.

Перечень используемых виджетов, находящихся в библиотеке виджетов, приведенных в таблице 20.1.

Таблица 20.1 – Перечень виджетов в библиотеке виджетов

Вкладка библиотеки виджетов	**Виджет**	**Метрика**
Сервер	Использование ЦПУ	ЦПУ, нагрузка
Сервер	Дисковый ввод/вывод	диск, чтение, запись
Сервер	Дисковых операций ввода/вывода	диск, чтение, запись, нагрузка
Сервер	Версия ОС	версия
Сервер	Использование ОЗУ	ОЗУ, нагрузка
Сервер	Дисковый ввод/вывод	диск, чтение, запись, нагрузка
Сервер	Использование диска	диск, чтение, запись, нагрузка
Сервер	Свободное пространство	диск, размер
Сервер	Сетевой ввод/вывод	сеть, чтение, запись, нагрузка
Сервер	Загрузка системы (load average 1/5/15 min)	ЦПУ, нагрузка
БД	Версия БД	версия (PostgreSQL/Jatoba)
БД	Количество сессий по состояниям	сессии, нагрузка
БД	Число транзакций в секунду	нагрузка
БД	Длительность работы БД	длительность
БД	Размер БД	размер
БД	Количество заблокированных и ожидающих сессий	сессии, конфликты
БД	Изменение размеров БД	Размер, запись
БД	Общее количество сессий	Сессии, нагрузка
БД	Блокировки	конфликты
БД	Взаимоблокировки, конфликты	конфликты
БД	Максимальный возраст незамороженных транзакций	длительность
БД	Работа со строками данных	Строки, чтение, запись
БД	Максимальная продолжительность запросов/ожиданий	Сессии, конфликты, длительность
БД	Автовакуумы и их длительность	Сессии, длительность
БД	Интенсивность контрольных точек	WAL, контрольные точки, нагрузка
БД	Объем WAL	WAL, запись размер
БД	Интенсивность работы с буферами	WAL, чтение, запись
БД	Длительность обработки контрольных точек	WAL, контрольные точки, длительность
БД	Доля чтения из кэша	чтение
БД	Запись во временные файлы	размер, чтение
БД	Количество транзакций и их откатов	нагрузка

На панель виджеты добавляются нажатием кнопки «Библиотека виджетов». В окне «Библиотека виджетов» выбираются требуемые виджеты, которые будут выстраиваться в окне вертикально.

Выбор требуемых виджетов возможно выполнить через поле «поиск» и/или используя фильтр по метрикам приведенных в таблице 20.1. В фильтре метрик виджетов доступен множественный выбор.

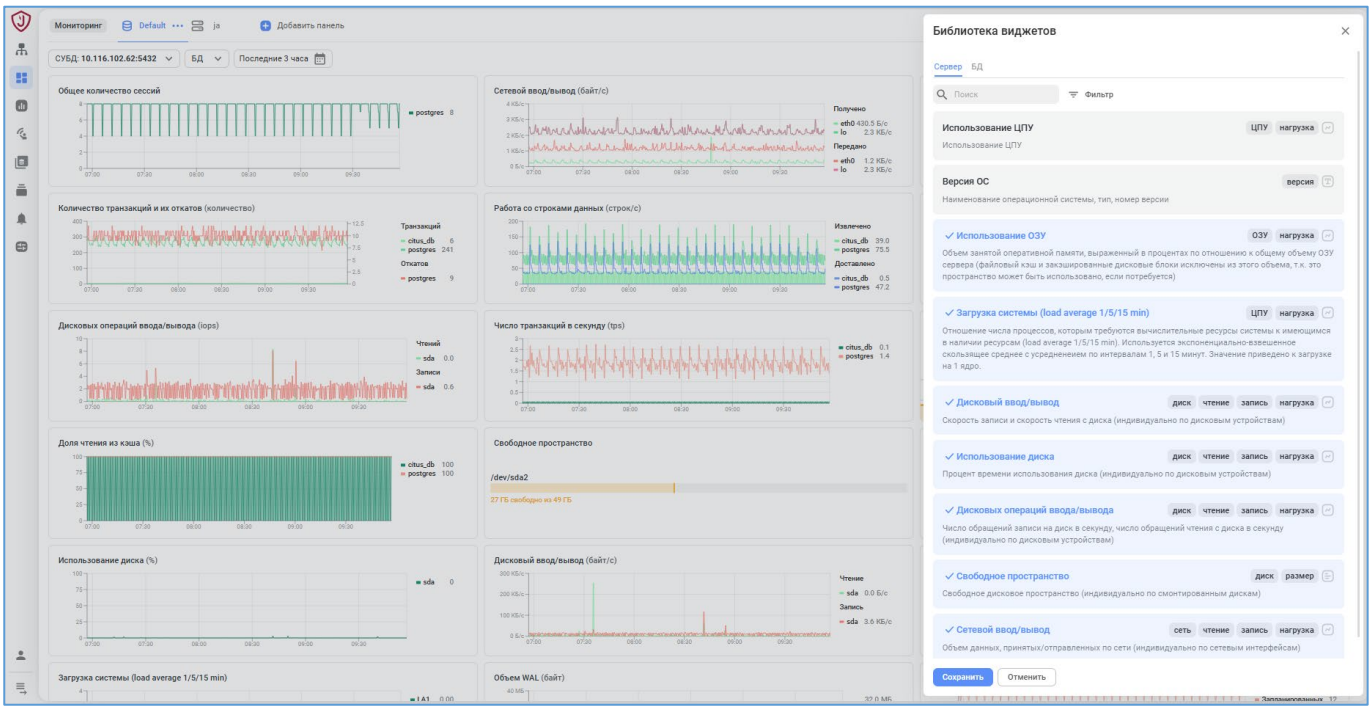

Рисунок 20.3 – Окно «Библиотека виджетов»

После сохранения выбора, виджеты можно:

- изменять размер и адаптировать размер виджета на нестандартный;
- перемещать по пространству окна.

Компонент запомнит и сохранит их расположение и размер.

Виджет автоматически загрузит данные метрик. В случае их отсутствия на виджете выводится информация о причине отсутствия данных.

выдавать пользователю следующие сообщения:

- Prometheus не вернул данных, так как СУБД не существует в заданном периоде или не настроен ни один экспортёр (Prometheus did not return data because the DBMS does not exist in the specified period or no exporter is configured)

Такое может произойти, если пользователь выбрал СУБД, а затем сменил период наблюдения на тот, в котором этой СУБД ещё/уже не существовало; при выборе периода список СУБД инициализируется заново, но выбор пользователя в отношении СУБД остается)

– В заданном периоде БД <datname> не существует (The database <datname> does not exist in the specified period)

Такое может произойти, если пользователь выбрал БД, а затем сменил период наблюдения на тот, в котором этой БД ещё/уже не существовало; при выборе периода список БД инициализируется заново, но выбор пользователя в отношении БД остается.

– Для указанных параметров Prometheus не вернул данных, возможно, не настроен <exporter_type>-экспортёр (Prometheus did not return data for the specified parameters, perhaps the <exporter_type>-exporter is not configured properly)

Нужный для виджета экспортёр может быть не подключен, не сконфигурирован, не отвечать по каким-то причинам, из-за чего в Прометей не сохраняются нужные данные; так же может быть, что не удается выполнить сопоставление адреса экспортера и адреса СУБД, отсутствуют метрики pg_static, pg_server, node_os_info.

– В заданном периоде показатели равны нулю (There are only zero values in the specified period)

Все временные ряды были отброшены при подготовке данных, поскольку содержали только нулевые значения.

20.2. Добавление панели виджетов

Помимо имеющейся панели виджетов «Default», существует функциональная возможность добавления новых панелей через кнопку «Добавить панель».

Панели имеют градацию на:

– СУБД;

– Кластеры.

Визуально отличаются значками.

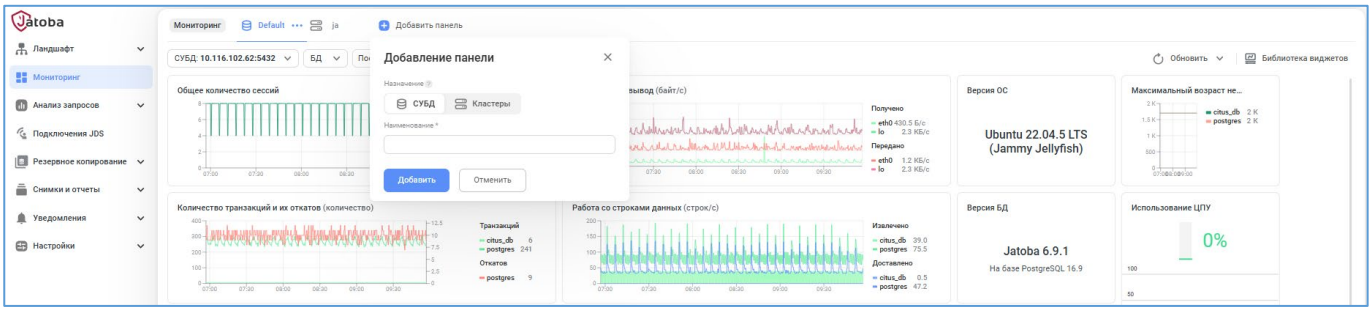

Рисунок 20.4 – Окно добавления панели виджетов

20.3. Панель виджетов для кластера ja_Hipe_Cluster

Воспользоваться панелью виджетов для кластера на основе компонента ja_Hipe_Cluster возможно, когда экспортеры и система «Prometheus» настроена. Описание настройки приведено в документе «Руководство по настройке. Часть 28. Поддержка мониторинга СУБД».

Набор виджетов для кластера ограничен и приведен в таблице 20.2

Таблица 20.2 – Перечень виджетов для ja_Hipe_Cluster

Тип виджета	Виджет	Метрика	Описание
	Использование сессий узлами	Сессии, нагрузка	общее кол-во сессий на каждом узле кластере с учетом ретроспективы
Сервер	Использование диска	диск, нагрузка	
	Объём шардированных таблиц	размер	
Сервер	Использование ЦПУ	ЦПУ, нагрузка	
Сервер	Использование ОЗУ	ОЗУ, нагрузка	
БД	Число транзакций в секунду	нагрузка	
Сервер	Сетевой ввод/вывод	сеть, нагрузка	
	Количество узлов	Доступность	
	Максимальная продолжительность запросов/ожиданий	Сессии, конфликты, длительность	
	Состояние узлов	Доступность	
	Общее количество сессий	Сессии, нагрузка	количество сессий к СУБД

На виджетах отображаются графы для каждого узла кластера.

Легенда вижетов является активной. При нажатии на легенду узла кластера в виджете контрастно отразится граф только выбранного узла. Остальные графы изменят контрастность.

Рисунок 20.5 – Виджеты кластера

20.4. Уведомления. Информирование о заданном значении показателя

Виджеты отражающие динамические значения оснащены механизмом уведомлений. Этот механизм активируется через контекстное меню виджета, выбором опции «Уведомления».

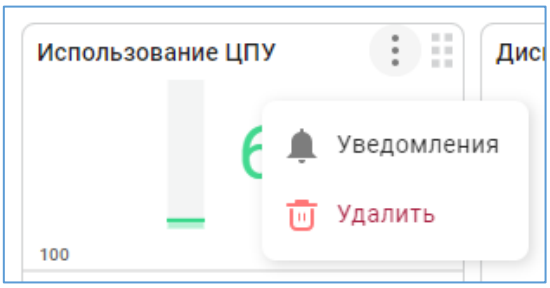

Рисунок 20.6 – Контекстное меню виджета

Выбор данной опции вызовет окно настройки уведомлений.

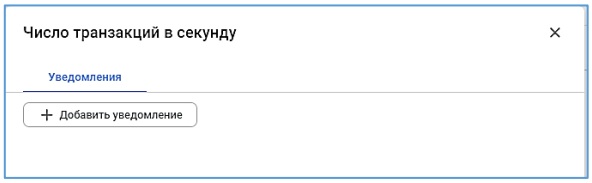

Рисунок 20.7 – Окно уведомления

Добавление уведомления доступно нажатием на кнопку «+ Добавить уведомление».

Каждый виджет может быть настроен на несколько уведомлений, для нескольких объектов контроля и имеет собственные настройки в которых устанавливаются пороговые значения по типам условий.

Такая конструкция уведомлений позволяет:

— устанавливать объекты контроля;

— создавать условие на любой объект;

— отслеживать выход метрики за пределы заданного диапазона и наоборот;

— следить за метриками, которые:

- в нормальном состоянии колеблются в определенном "коридоре" величин;
- в ненормальном состоянии выходят из «коридора» величин, как в большую, так и в меньшую сторону.

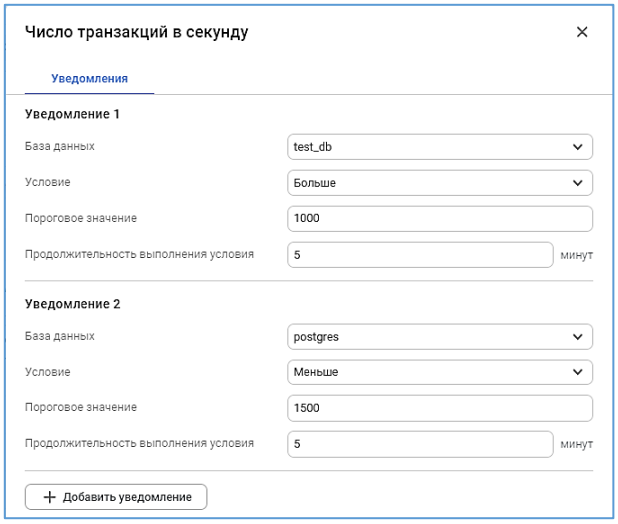

Рисунок 20.8 – Настройка уведомлений для виджета

Уведомления настраиваются пользователями самостоятельно и будут отправляться на E-mail указанный в карточке пользователя (см. п 2.1.3). Также уведомления приходят в Telegram и Zulip. Изменить созданные уведомления может только создавший их пользователь.

Создать «Уведомления» от имени и с правами пользователя JDS «admin» невозможно, т.к. у данной учетной записи отсутствует E-mail и не может быть добавлен.

21. РАЗДЕЛ «АНАЛИЗ ЗАПРОСОВ» (QUERY ANALYSIS)

Подраздел «Анализ запросов» предоставляет:

— отображение визуализации плана запроса средствами Pg-explain;

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

— возможность ручного ввод плана запроса.

Настройка требуемых компонентов и подключение к JDS описано в документе «Руководство по настройке. Часть 24. Поддержка мониторинга СУБД в части анализа запросов».

Подраздел «Анализ запросов» (Query analysis) не поддерживается с версией ядра «4» СУБД «Jatoba»

21.1. Вкладка «Запросы»

Вкладка «Запросы» отображает планы запросов с некоей большой длительностью выполнения.

Отображаются поля:

- Host – IP-адрес хоста;
- Наименование хоста – условное наименование хоста;
- Всего – количество отобранных планов запросов из лога pg-monitor;
- Шаблонов – значение количества шаблонов и ссылка для перехода к списку планов запросов выбранной СУБД;
- Timeline – графическое представление распределения запросов по времени суток.

По умолчанию отображаются запросы на текущую дату.

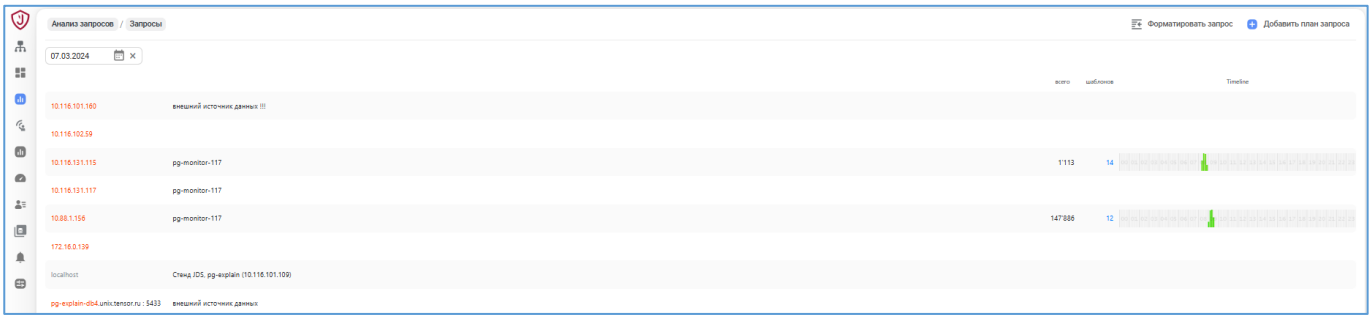

Рисунок 21.1 – Вид вкладки «Запросы»

При нажатии на гиперссылку количества шаблонов вкладка «Запросы» перестроится и отобразит вкладку «по шаблонам».

На вкладке «по шаблонам» отображаются поля:

— шаблон – план уникального запроса без учета повторов его выполнения;

— метод;

— app – приложение, отправившее запрос;

— кол-во – всего повторов выполнения этого запроса;

— sum, мс – суммарное время выполнения всех запросов одного шаблона;

— avg, мс – среднее время выполнения запроса;

— buf:mem – требуемая оперативная память для выполнения запроса;

— buf:dsk – требуемое дисковое пространство для выполнения запроса;

— % – доля дисковых ресурсов для выполнения запроса;

— last – последнее по времени выполнение запроса – ссылка для перехода к визуализации плана запроса;

— Timeline – графическое представление распределения запросов по времени суток.

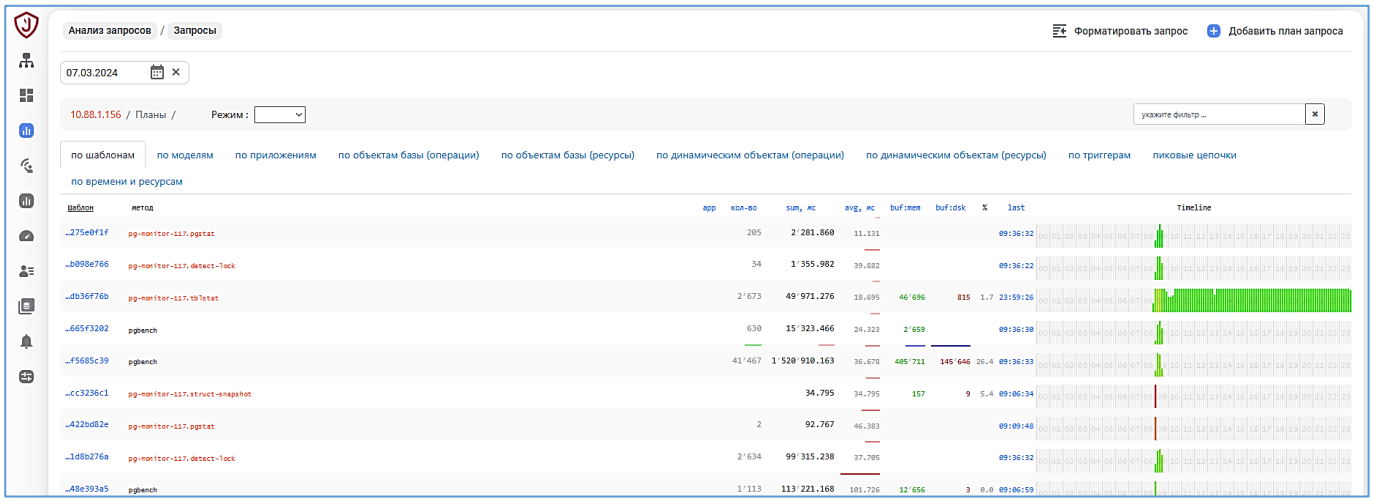

Рисунок 21.2 – Вкладка «по шаблонам»

Визуализация плана запроса

При клике по конкретному шаблону открывается список запусков запроса по времени.

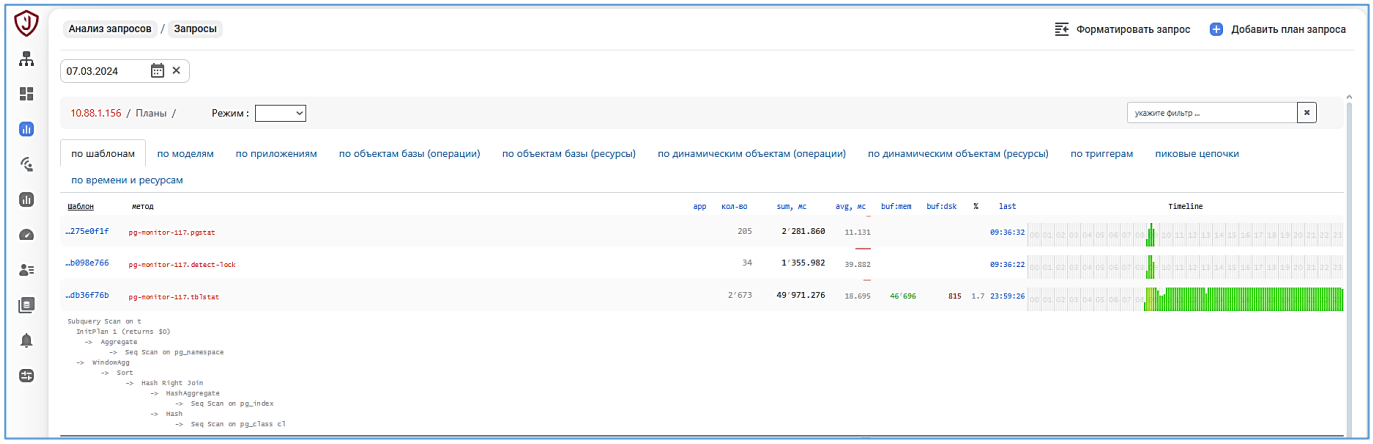

Рисунок 21.3 - Список запусков запроса по времени

При выборе конкретного запроса из списка планов запросов и нажатию по значению в поле «last» открываются вкладки визуализации запроса:

— вкладка «explain»;

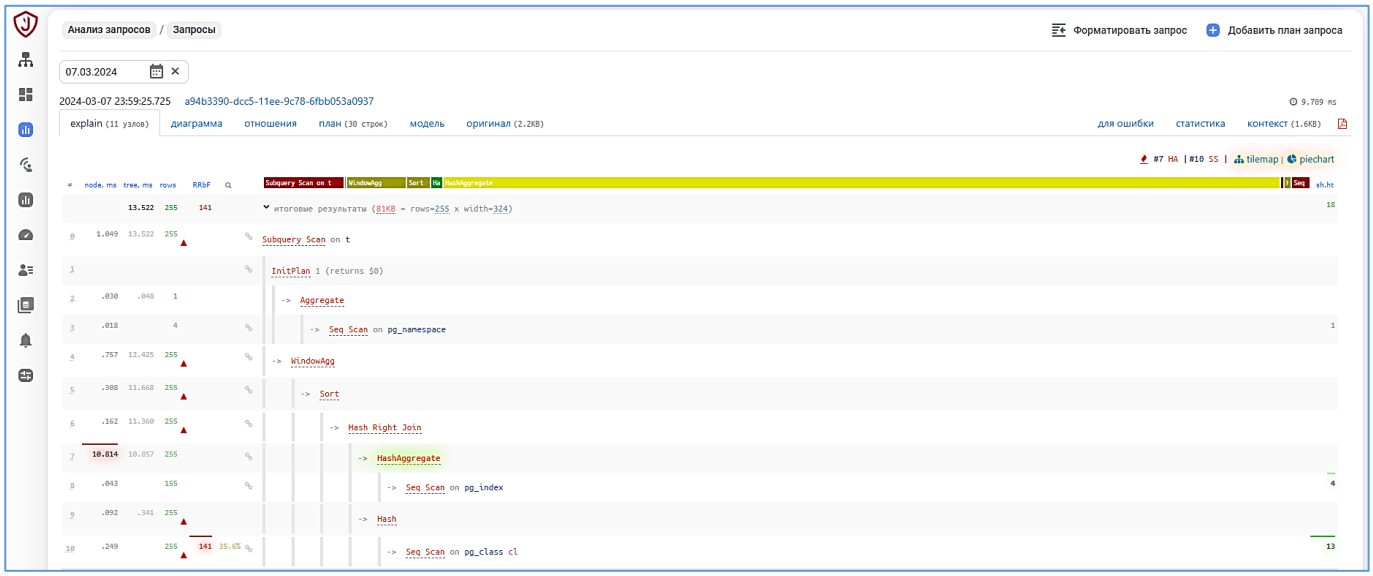

Рисунок 21.4 – Визуализация explain по узлам

Визуализированный план запроса возможно экспортировать в PDF-файл через пиктограмму «Adobe Acrobat».

— вкладка «диаграмма»;

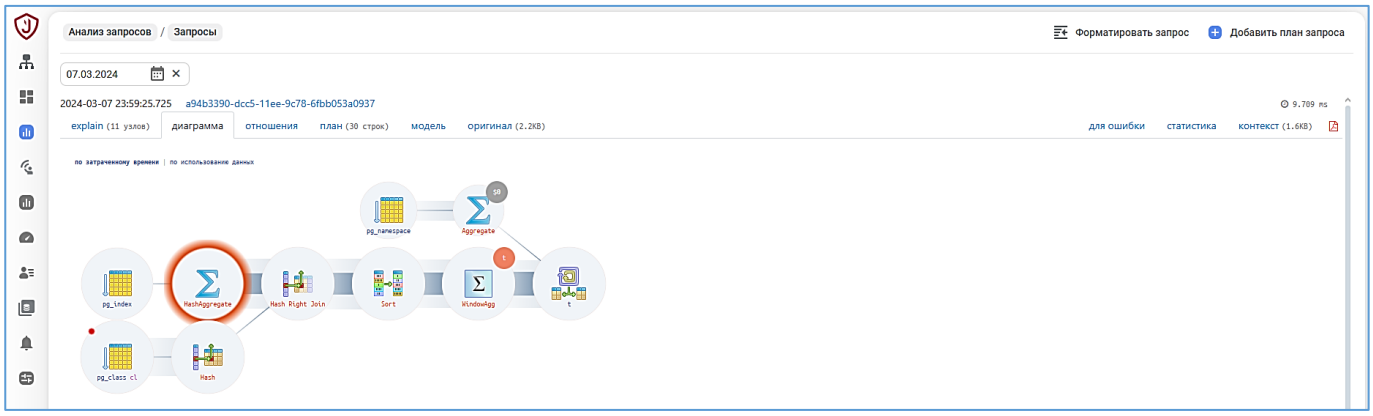

Рисунок 21.5 – Визуализация на вкладке «диаграмма»

— вкладка «отношения»;

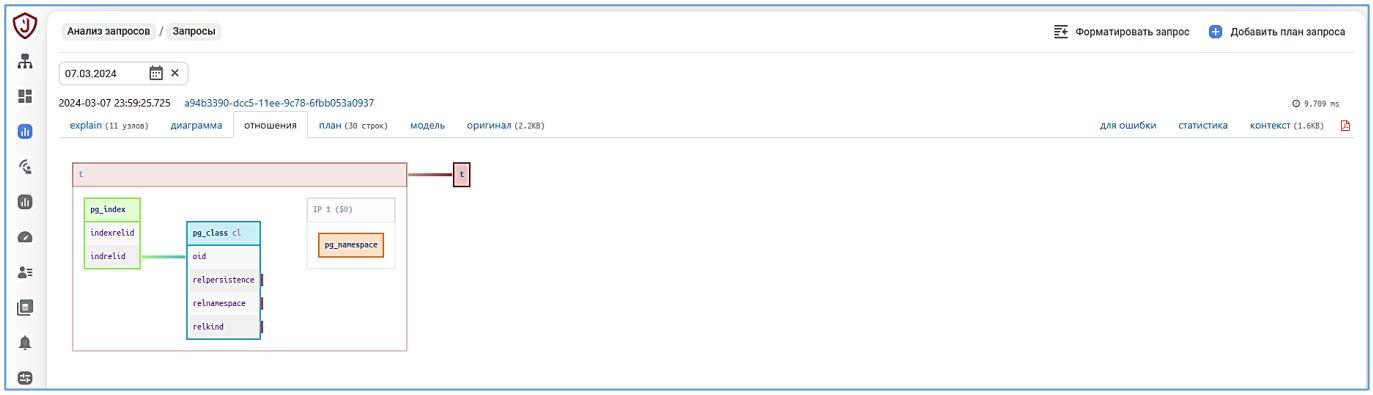

Рисунок 21.6 – Визуализация на вкладке «отношения»

— вкладка «план»;

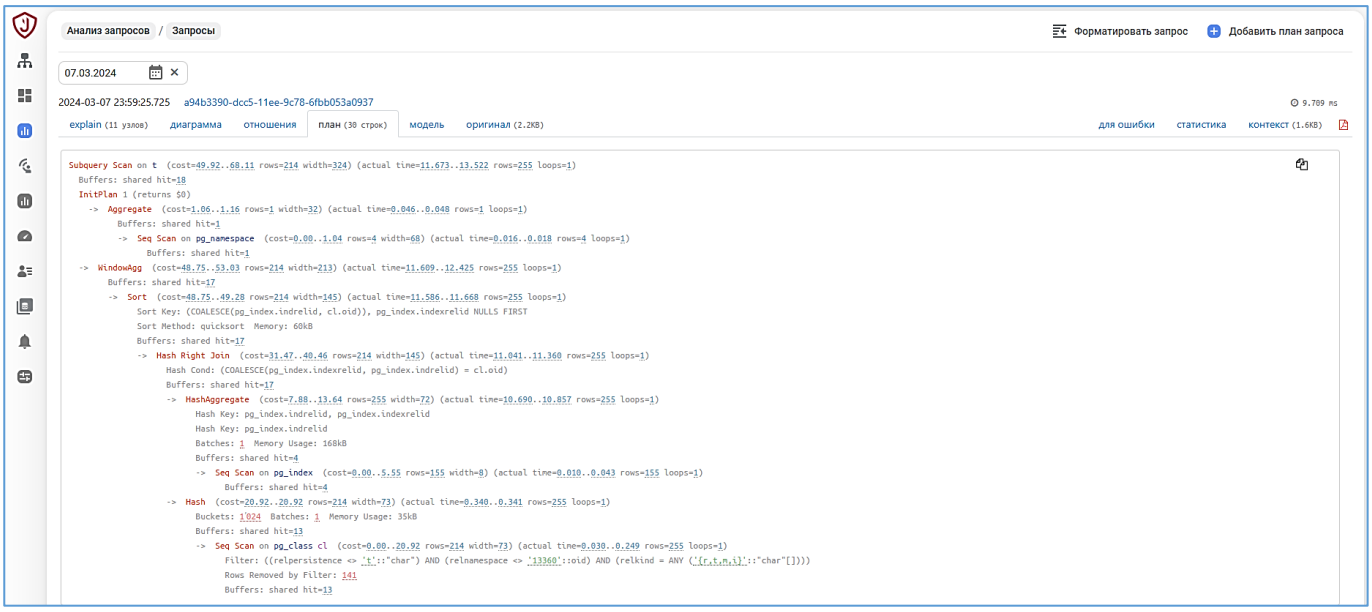

Рисунок 21.7 – Визуализация на вкладке «план»

— вкладка «модель»;

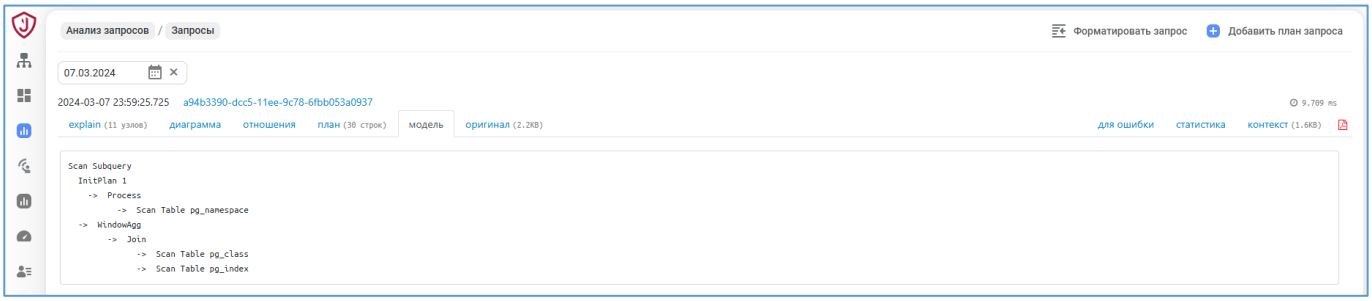

Рисунок 21.8 – Визуализация на вкладке «модель»

— вкладка «оригинал».

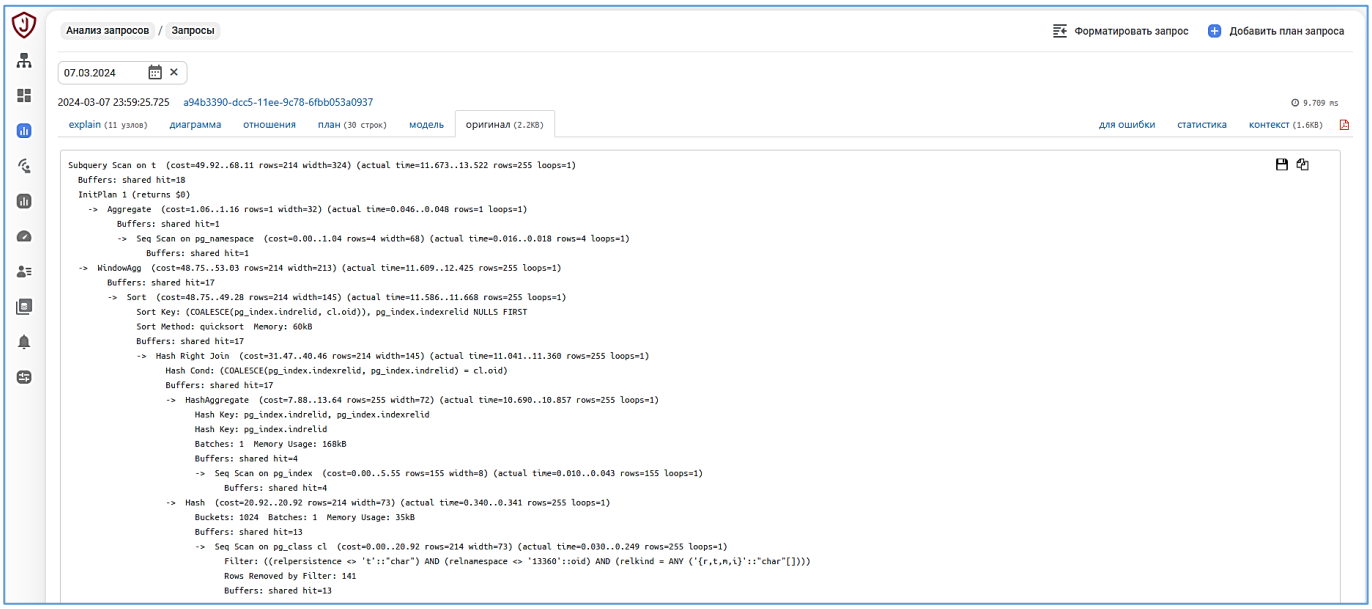

Рисунок 21.9 – Визуализация на вкладке «оригинал»

21.2. Вкладка «Мегазапросы»

Вкладка «Мегазапросы» отображает планы запросов, имеющие хотя бы одну из особенностей:

— большой объем возвращаемой выборки;

— большое количество используемых в запросе параметров;

— большой размер запроса;

— большая длительность передачи результатов запроса от сервера.

Рисунок 21.10 – Вид вкладки «Мегазапросы»

При выборе вкладки отображается список подключенных СУБД и следующие поля:

— «Host» – IP-адрес хоста;

— «Наименование хоста» – условное наименование хоста;

— «Resultset» – количество по признаку большого объема возвращаемой выборки – ссылка к списку планов запросов, отфильтрованных по выбранному параметру;

— «Params» – количество, большое число используемых параметров в запросе – ссылка;

— «Query» – количество, большой размер текста запроса – ссылка;

— «Diff» – количество, большая длительность передачи результатов запроса от сервера – ссылка;

— «Timeline» – график времени, когда выполнялись запросы.

При нажатии на гиперссылки «Resultset» или «Diff» вкладка «Мегазапросы» перестроится и отобразит вкладку «по приложениям».

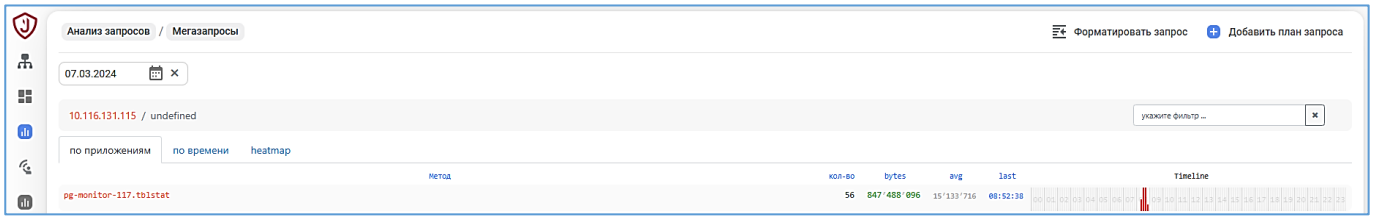

Рисунок 21.11 – Вкладка «по приложениям»

Вкладка «по приложениям» отображает поля:

— «Приложение» – приложение отправившее запрос;

— «Метод» – метод, используемый в плане для выполнения определенной операции;

— «Кол-во» – число выполнения запросов;

— «Duration» – суммарное время выполнения запросов с учетом передачи их результатов от сервера – фактическое время;

— «Exectime» – суммарное время выполнения запросов – ожидаемое время;

— «Diff» – разность суммарных фактического и ожидаемого времени - суммарное время передачи результата запроса;

— «+%» – отношение времени передачи результата запроса к времени выполнения запроса, в процентах;

— «Last» – время последнего выполнения запроса;

— «Timeline» – график времени, когда выполнялись запросы.

Нажатие по значению времени в поле «Last» откроет визуализацию плана запроса.

В теле вывода визуализации плана запроса присутствует гиперссылка «перейти к анализу». Нажав на которую, вкладка перестроится и отразит вкладки визуализации, как было описано выше:

— вкладка «explain»;

— вкладка «диаграмма»;

— вкладка «отношения»;

— вкладка «план»;

— вкладка «модель»;

— вкладка «оригинал».

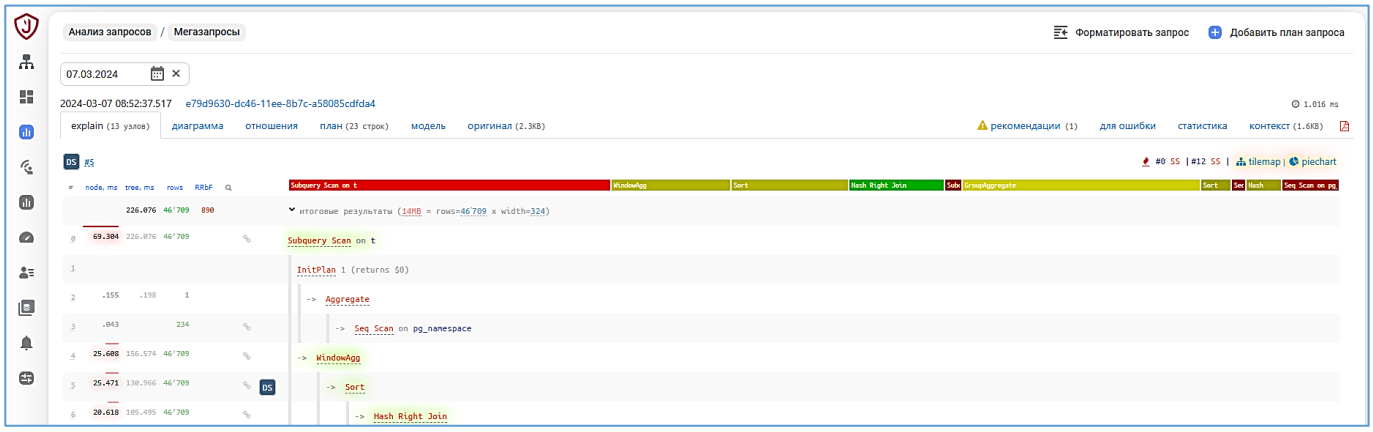

Рисунок 21.12 – Вкладки визуализации запроса.

21.3. Вкладка «Блокировки»

Вкладка «Блокировки» отображает планы запросов, в результате которых потребовалось блокировать ресурсы данных. Отображаются поля:

— «Host» – IP-адрес хоста;

— «Наименование хоста» – условное наименование хоста;

— «deadlock» – взаимные блокировки ресурсов, требуемых для двух запросов;

— «lock» – обычная блокировка ресурсов данных требуемая для выполнения конкретного запроса;

— «Timeline» – графическое представление распределения запросов по времени суток.

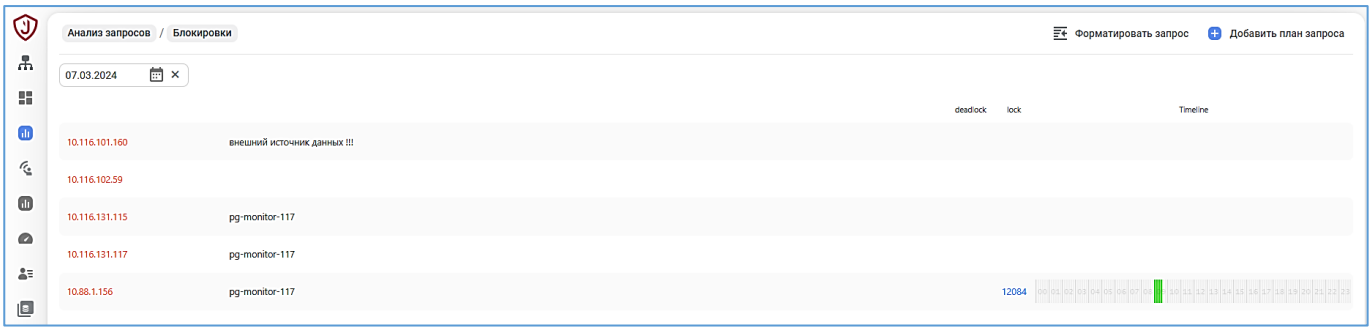

Рисунок 21.13 – Вид вкладки «Блокировки»

Нажатие по значению в поле «lock» открывает агрегированный список запросов на вкладке «по типам», сгруппированный по типам блокировок, по приложениям, по времени.

Отображаются поля:

— «mode» – тип блокировки ресурса;

— «type» – область действия блокировки;

— «приложение» – при клике разворачивается список, где дополнительно отображается PID и приложение;

— «объект блокировки» – объект блокировки;

— «sum, мс» – суммарное время выполнения запросов;

— «кол-во» – количество запросов в агрегированной строке группы;

— «last» – время начала выполнения последнего запроса – ссылка;

— «Timeline» – графическое представление распределения запросов по времени суток.

Рисунок 21.14 – Вкладка «по типам»

Кликнув по значению в поле «last» пользователь должен увидеть страницу анализа плана выполнения запроса, выполнявшегося последним, где можно найти данные по блокировке.

Далее, выбрав ссылку «Перейти к анализу», можно перейти к блоку визуализации плана запроса, рядом с которым расположена ссылка.

Рисунок 21.15 – Вывод анализа плана запроса

На данной странице анализа планов запросов, входящих в шаблон, можно увидеть информацию о блокировке.

21.4. Вкладка «Ошибки»

Во вкладке «Ошибки» отражаются ошибки на целевых СУБД сортированные по датам:

— по хостам (см. п. 21.4.2);

— по ошибкам (см. п. 21.4.2);

отображаемых в одноименных ссылках (вкладках).

21.4.1. Вкладка «по хостам»

Вкладка отображает количество ошибок, с делением по критичности, на всех хостах.

Во вкладке «по хостам» отображаются столбы:

— Host - наименование хоста СУБД;

— Fatal - высокая критичность ошибки выполнения запроса;

— Error - обычная критичность ошибки выполнения запроса;

— Warning - предупреждение о проблеме выполнения запроса;

— Timeline - графическое представление распределения запросов по времени суток

Нажатие на количество ошибок в строке хоста вызовет переход страницу списка классов ошибок для выбранного хоста.

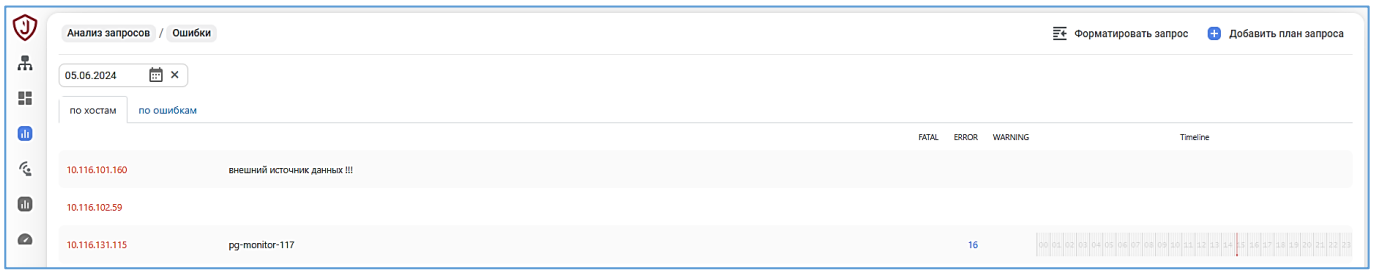

Рисунок 21.16 – Вкладка «по хостам»

Страница списка классов ошибок для выбранного хоста

Страница отображает список наименований классов ошибок выполнения запросов с отображением числа приложений, где встречаются ошибки, количества случаев каждого класса ошибок и распределением по времени за выбранные сутки.

На странице отображаются столбы, описанные в таблице 21.1.

Таблица 21.1 – Столбцы страницы списка классов ошибок для выбранного хоста

Поля	Описание
Класс ошибки	наименование класса ошибок, зарегистрированных на конкретном хосте
Методы	наименования приложений и методов вызывавших запросы с ошибками (если более 1 приложения, то список наименований приложений скрыты в свернутую строку)
app/arg	количество приложений
Кол-во	количество случаев ошибок конкретного класса
last	последнее время выполнения запроса

Поля	Описание
Timeline	графическое представление распределения запросов по времени суток

Рисунок 21.17 - Страница списка классов ошибок для выбранного хоста

Выбрав класс ошибки и нажав на ее строку развернется список ошибок, разграниченных по времени.

Страница описания запроса, выполненного с ошибкой

Выбрав время выполнение запроса, открывается Страница описания запроса, выполненного с ошибкой, которая содержит строку краткого описания ошибки, с указанием критичности ошибки.

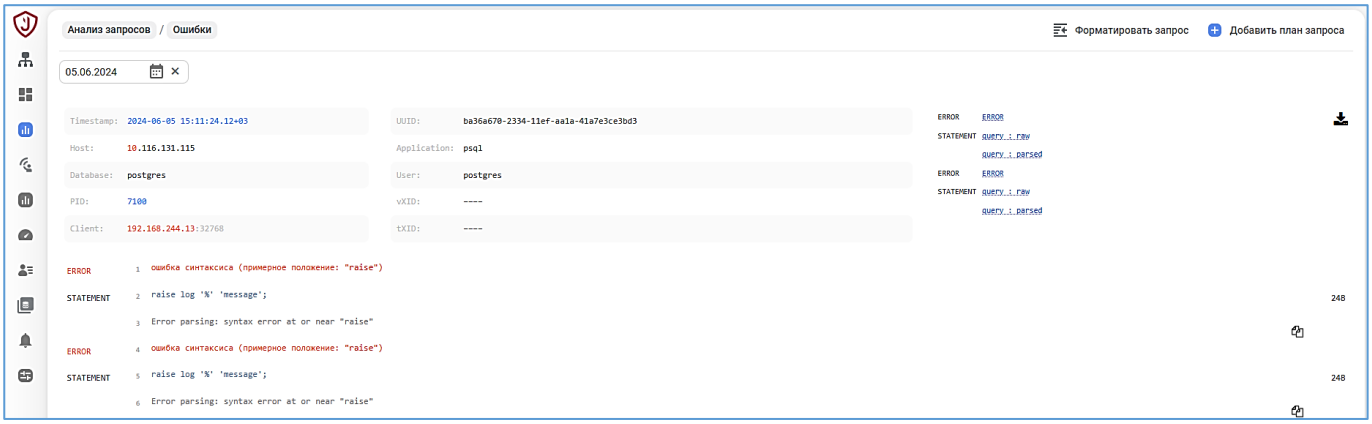

Рисунок 21.18 - Страница описания запроса, выполненного с ошибкой

Полное описание ошибки показывается при нажатии на ее строку.

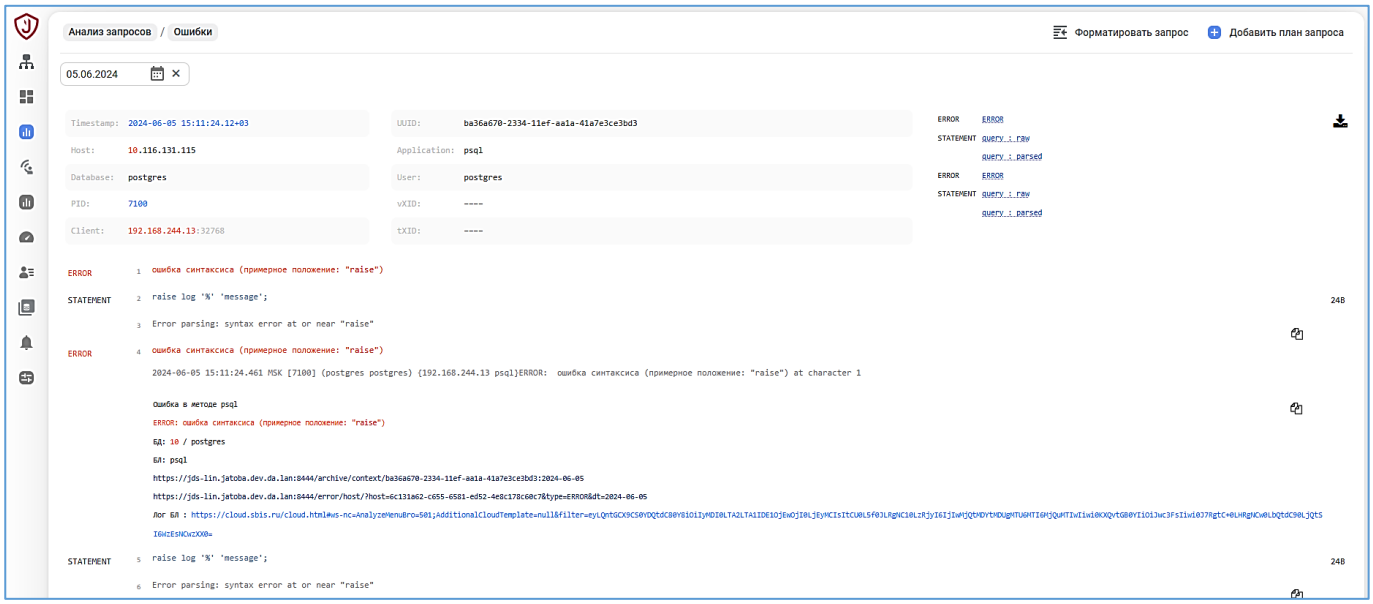

Рисунок 21.19 – Полное описание ошибки

Пиктограмма «Скопировать» копирует в буфер обмена полное описание ошибки.

21.4.2. Вкладка «по ошибкам»

Вкладка отображает количество ошибок, без деления по критичности, на всех хостах.

Во вкладке «по ошибкам» отображаются столбы:

— Ошибка - наименование класса ошибки;

— Количество - количество ошибок конкретного класса;

— hosts - число хостов, где зарегистрированы ошибки данного класса;

— last - время последнего выполнения запроса с ошибкой данного класса;

— Timeline - графическое представление распределения запросов по времени суток.

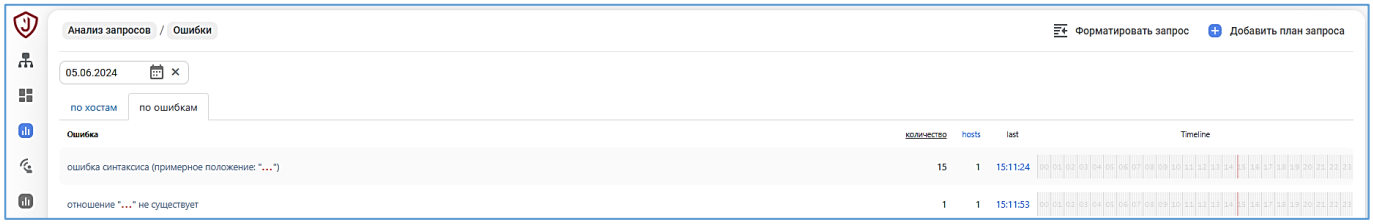

Рисунок 21.20 - Вкладка «по ошибкам»

Выбрав и развернув строку выбранного класса ошибки, отобразится список хостов, где выполнялись запросы с ошибками выбранного класса.

В случае последующего выбора хоста из развернутого списка, компонент выполнит переход на страницу "Страница списка классов ошибок для выбранного хоста", описанную ранее.

В случае выбора времени последнего выполнения запроса, система выполнит переход на страницу "Страница описания запроса, выполненного с ошибкой", описанную ранее.

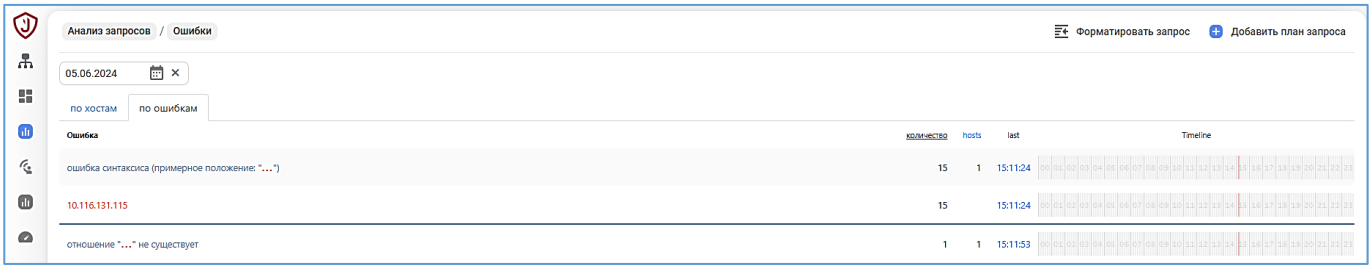

Рисунок 21.21 – Список хостов на которых проявилась ошибка

21.5. Вкладка «Статистика»

Во вкладке отображается статистическая и аналитическая информация об объекте мониторинга на основе журнала аудита СУБД. Для чего во вкладке «Настройки» (см. п. 21.6) устанавливаются дополнительные параметры журнала аудита СУБД.

Установленная дата календаря отображает статистическую информацию по полям:

— Relations - снепшоты состояния таблиц;

— RU/SA - статистика использования ресурсов;

— Stats - снепшоты статистики по таблицам;

— Analyze - события применения команды;

— Vacuum - события применения команды;

— Checkpoint - события применения команды;

— Timelime – линия времени.

При переходе по кликабельным пиктограммам и значениям открываются страницы с данными статистики.

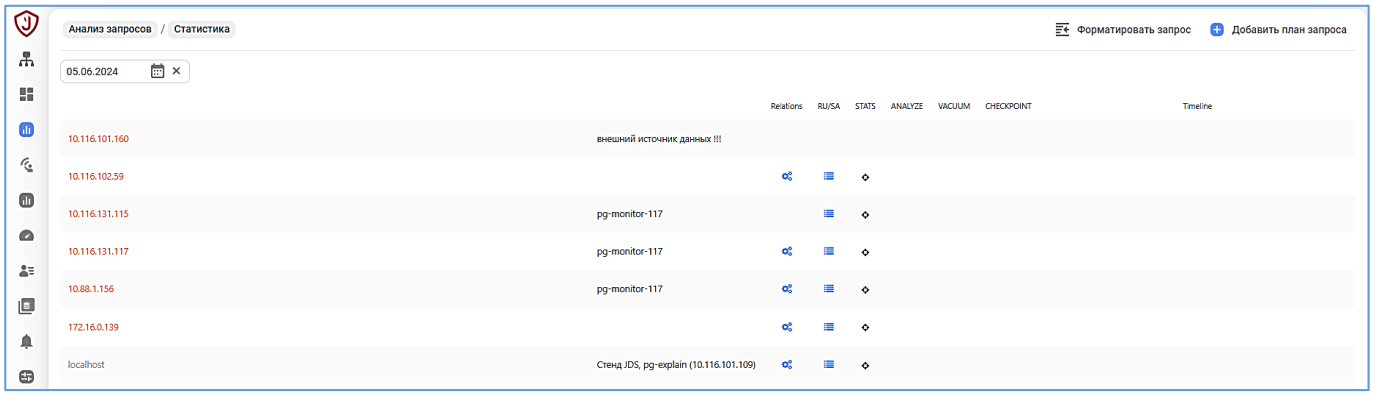

Рисунок 21.22 – Вкладка «Статистика»

21.6. Вкладка «Настройки»

Настройка подключений описана в документе «Руководство по настройке. Часть 24. Поддержка мониторинга СУБД в части анализа запросов», в пунктах:

— 5.1.4. Конфигурирование компонента JDS на отдельном узле;

— 5.2.5. Редактирование параметров компонента JDS.

При настроенном подключении для наблюдаемой СУБД дополнительно устанавливаются параметры журнала аудита СУБД.

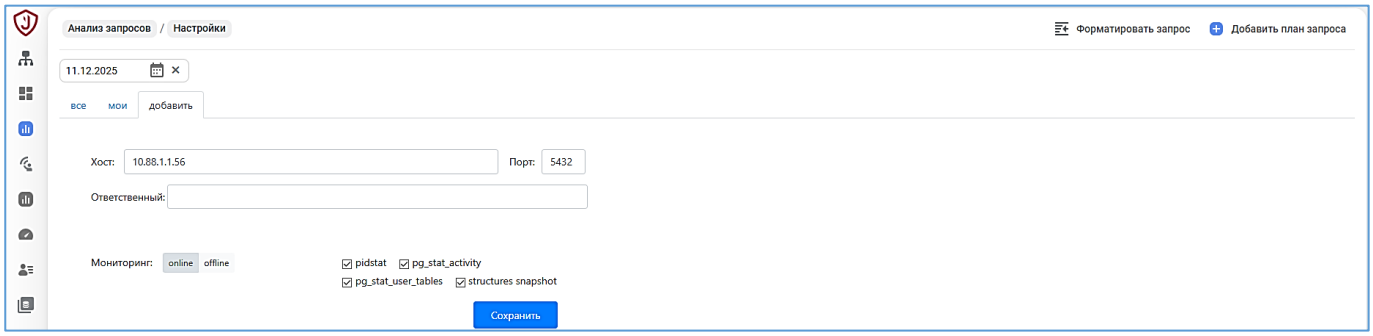

Рисунок 21.23 – Дополнительные настройки журнала аудита СУБД

21.7. Форматирование запроса

Подраздел «Анализ запросов» имеет функциональную возможность форматирования SQL-запросов.

Нажатие кнопки «Форматировать запрос» вызывает окно с двумя основными полями «Исходный запрос» и «Форматированный запрос». SQL-запрос вставляется через буфер обмена. После нажатия кнопки «Форматировать» система выполняет автоматизированную проверку синтаксиса, форматирование и раскраску SQL-запроса.

Например

Исходный запрос

```
INSERT INTO orders (customer_id, product, price)
     SELECT (random() * 3 + 1)::integer, 'product', (random() *
1000 + 1)::integer
     FROM generate_series(1, 1000);
```

Форматированный запрос

```
INSERT INTO orders(
  customer_id
, product
, price
)
SELECT
  (random() * 3 + 1)::integer
, 'product'
, (random() * 1000 + 1)::integer
FROM
  generate_series(1, 1000);
```

Полученный результат форматирования запроса возможно сохранить через буфер обмена.

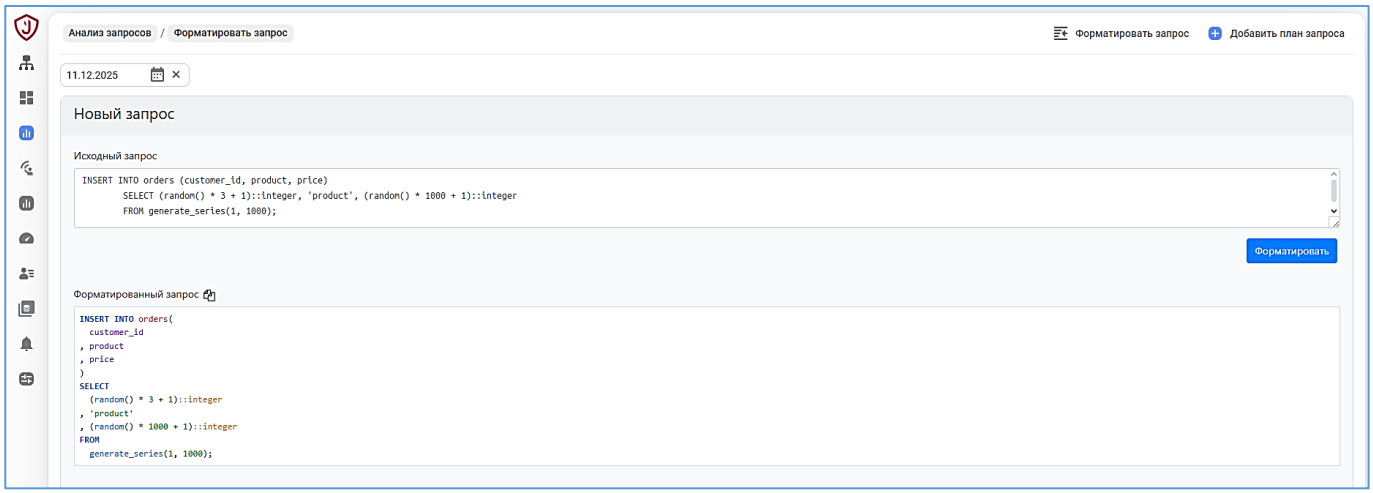

Рисунок 21.24 – Окно «Форматировать запрос»

21.8. Добавление плана запроса

Для визуализации плана выполнения запроса, загружаемого вручную, необходимо скопировать в буфер обмена текст плана, затем открыть в боковом меню раздел «Анализ запросов» и нажать кнопку «Добавить план запроса».

В открытом окне «План запроса для анализа» необходимо вставить текст плана запроса из буфера в поле ввода, как показано на рисунке 21.25. Корректный план запроса автоматически получит подсветку синтаксиса.

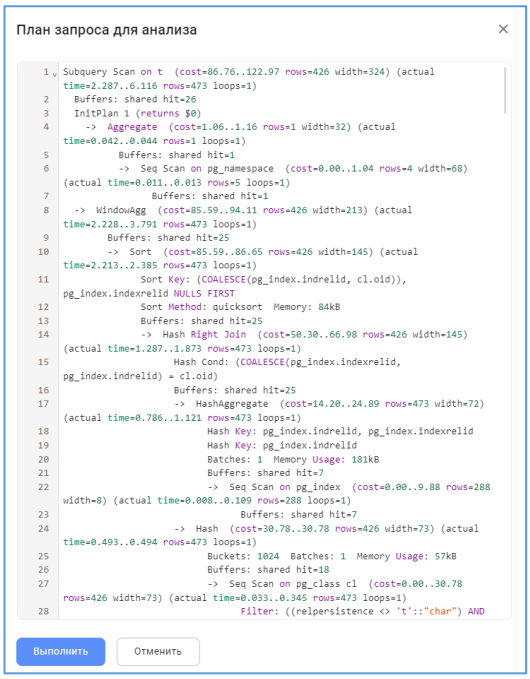

Рисунок 21.25 - Окно «План запроса для анализа»

Для выполнения визуализации вставленного текста плана запроса требуется нажать кнопку «Выполнить».

После начала обработки текста плана запроса, если был вставлен некорректный (неполный) текст плана запроса или, по ошибке, был вставлен текст SQL-запроса, то будет отображаться сообщение об ошибке:

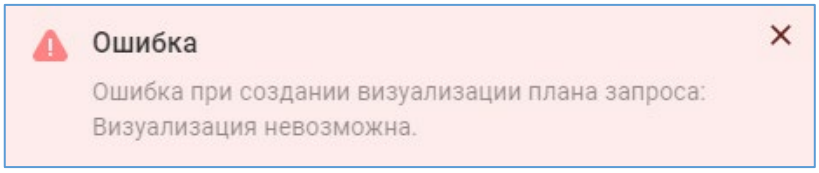

Рисунок 21.26 – Ошибка визуализации плана запроса

Если при обработке текста плана запроса ошибки нет, то одновременно с открытием страницы визуализации плана выполнения запроса будет отображаться сообщение:

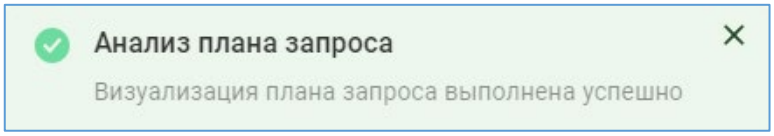

Рисунок 21.27 – Сообщение об успешной визуализации плана запроса

Страница визуализации плана запроса состоит из нескольких вкладок, состав которых зависит от информации, полученной из плана, а также контекстной информации, относящейся ко времени выполнения запроса, если такая информация доступна.

Вкладки страницы визуализации плана запроса:

— Explain – отображение форматированного плана выполнения запроса и данных по узлам плана;

— Диаграмма – диаграмма этапов выполнения плана запроса с выделением проблемных узлов;

— Отношения – схема отношений таблиц, используемых в запросе, в том числе временных;

— План – отображение плана запроса с подсветкой синтаксиса;

— Модель – упрощенный вид плана запроса, без детализации для узлов плана;

— Оригинал – исходный вид загруженного плана запроса;

— Таблицы – описание используемых таблиц и созданных индексов;

— Рекомендации – рекомендация по исправлению проблемы в узле;

— Для ошибки - готовый текст сообщения для вставки в баг-трекер;

— Статистика – список наименований узлов плана выполнения запроса с расширенными данными по узлам;

— Контекст – сводная информация о запросе и плане его выполнения.

21.8.1. Форматированное текстовое представление плана запроса

Страница визуализации плана запроса открывается на вкладке «Explain» - первой из нескольких доступных вкладок. На странице визуализации всегда отображаются дата/время загрузки плана и UUID запроса.

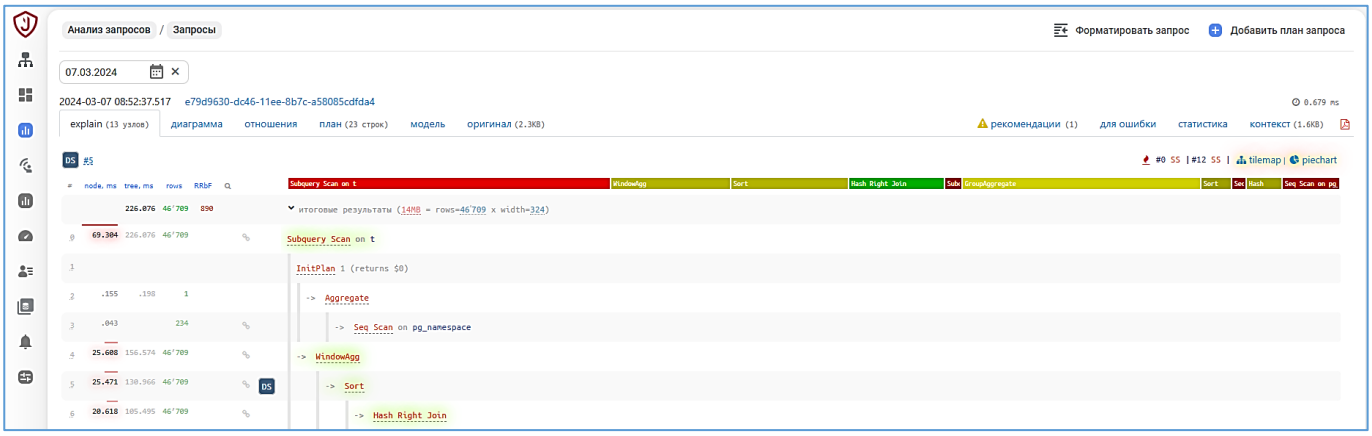

Рисунок 21.28 – Текстовое представление плана запроса

Отображение даты и времени в верхнем левом углу зависят от способа его загрузки. Для плана запроса, загруженного автоматически из журнала контролируемой СУБД – это время выполнения запроса в БД. Для плана запроса, загруженного вручную – это время загрузки плана запроса пользователем.

Вкладка «Explain» может быть полезна для анализа последовательности выполнения этапов запроса, представленных в виде дерева пронумерованных узлов. План запроса отображается в отформатированном виде с отдельными колонками времени выполнения узлов плана и числом обрабатываемых строк:

— node, ms – время исполнения узла, без учета дочерних узлов;

— tree, ms – время исполнения узла, включая дочерние узлы;

— rows – количество строк, обработанных узлом;

— RRbF – количество строк, отброшенных фильтром в запросе.

Просмотр подробных данных каждого узла в развернутом виде возможен при клике по строке узла, как показано на рисунке 21.29.

Рисунок 21.29 - Просмотр подробных данных узла в развернутом виде

Для более оперативного ознакомления с данными отдельного узла плана во всплывающем окне, можно воспользоваться строкой-диаграммой, выбрав один из узлов.

21.8.2. Сравнительные диаграммы плана запроса

Если недостаточно текстового представления данных по узлам, то на этой же вкладке «Explain», можно взвесить узлы плана отдельно по стоимости, времени выполнения и возвращаемым строкам в графическом виде, нажав кнопки, «Tilemap» или «Piechart».

Кнопка «Tilemap» – диаграмма в виде последовательности шестигранников - тайлов, с выбором всех трех параметров, выделенных на следующем рисунке стрелкой. Цветом и толщиной линий на диаграмме указан весовой вклад узла в общую оценку по каждому параметру. Всплывающее окно показывает тот же набор данных для узла, что и в текстовом представлении плана запроса. Нажав на тайл можно подсветить узел в текстовом представлении, видимом в соседнем окне.

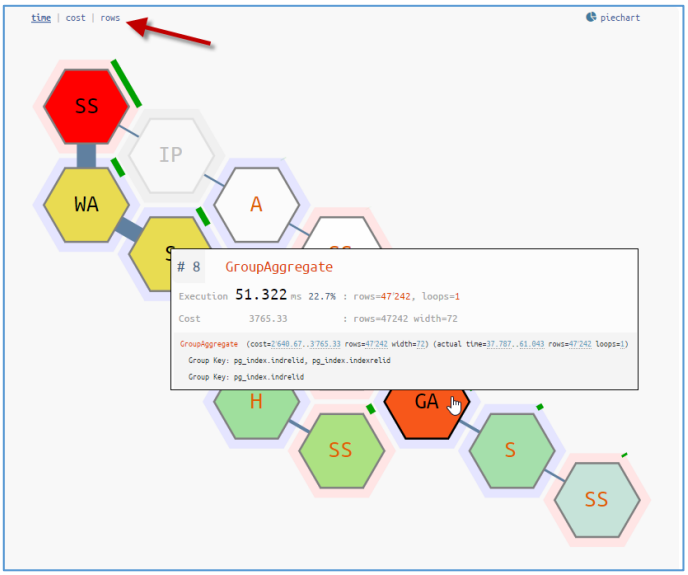

Рисунок 21.30 – Диаграмма тайтлов

Кнопка «Piechart» – круговая диаграмма, только для отображения долями веса времени каждого из узлов плана в общем времени выполнения запроса. Здесь последовательность выполнения узлов обозначена слоем (от внешнего к центральному), а цвета долей совпадают с цветами на строке-диаграмме в текстовом представлении плана запроса. Всплывающее окно показывает тот же набор данных для узла, что и в текстовом представлении. Нажав на долю в диаграмме можно подсветить узел в текстовом представлении, видимом в соседнем окне.

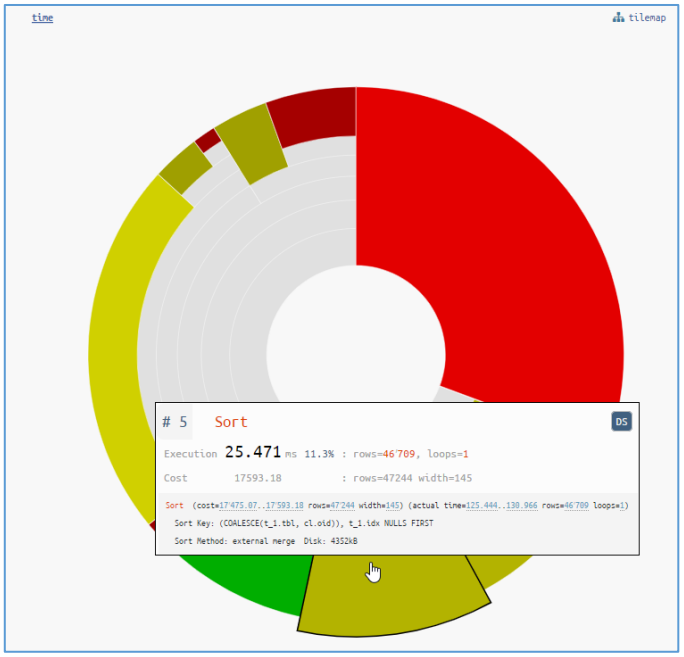

Рисунок 21.31 – Круговая диаграмма

Независимо от вида представления узла в составе плана запроса, всплывающая подсказка к узлу содержит в удобном для чтения виде детальную информацию:

— # - номер и наименование узла;

— Execution – фактическое время выполнения узла (в ms, без учета вложенных узлов), для одного повтора (loops);

— Loops – фактическое количество повторных выполнений узла;

— Процент – процентное значение фактического времени выполнения узла от общего фактического времени выполнения, без учетов всех повторов;

— Rows (красное значение) – количество строк, фактически возвращенное узлом;

— Cost – оценочная стоимость узла в установленных единицах;

— Rows (серое значение) – оценочное количество строк, возвращаемых узлом;

— Width – средний оценочный объем прочитанной строки (в байтах).

21.8.3. Функциональная диаграмма плана запроса

Если необходимо изучить план запроса целиком, но он сложен и нет желания вчитываться во всплывающие подсказки на диаграммах, то можно на вкладке «Диаграмма» посмотреть представление плана запроса в виде последовательности функциональных пиктограмм – миниатюрных обозначений узлов каждого типа.

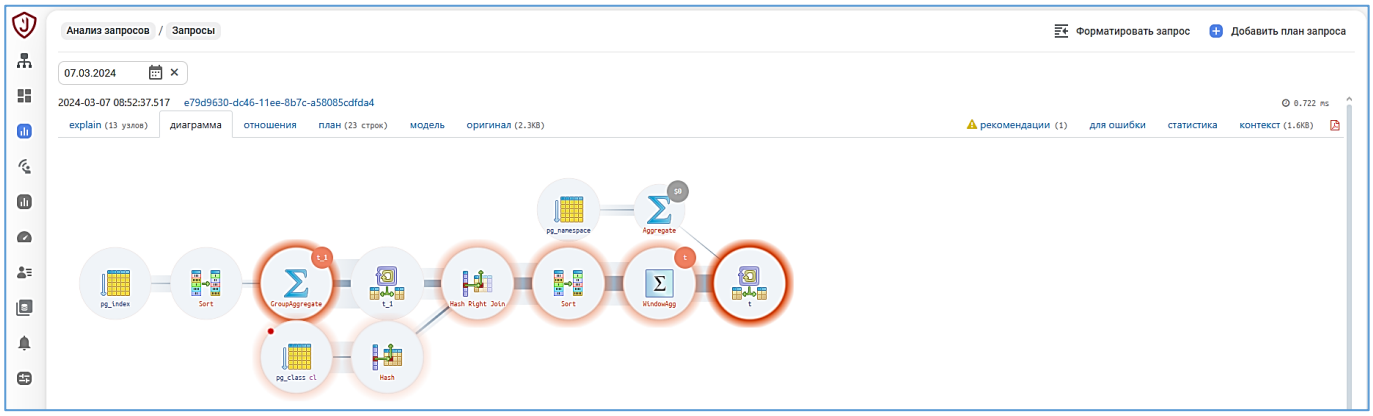

Рисунок 21.32 – Функциональная диаграмма

Расположение узлов на этой диаграмме, если смотреть по порядку их номеров, идет справа налево. «Читать» план запроса нужно по отдельным ветвям -сверху-вверх и слева-

направо. «Прочитав» дочернюю ветвь, нужно опуститься на следующий уровень и «читать» начиная слева, с начала ветви.

Нажатие на пиктограмму выбранного узла выполняет переход к этому же узлу, обозначенному на вкладке «Explain», в форматированном текстовом представлении.

21.8.4. Модель плана запроса

Для агрегирования информации о планах запросов, выполняемых многократно, но с разными временем и объемами выбираемых данных, используют очищенную форму плана запроса - шаблон плана запроса. О шаблонах планов запросов будет рассказано в разделе «Анализ длительности выполнения запроса к БД».

На вкладке «Модель» можно увидеть еще более очищенную форму плана запроса, называемую моделью плана запроса.

Модель плана запроса – это агрегированная форма для объединения нескольких планов запросов, выполнявшихся над одними и теми же объектами БД, но разными способами. В модели плана запроса обобщенная структура агрегированных планов: объединены разные операции над таблицами, операция объединения данных из таблиц представлена один раз с указанием всех используемых таблиц, все узлы сортировки, группировки и уникализации данных собраны в один узел.

Рисунок 21.33 – Модель плана запроса

Таким образом получаем компактный алгоритм использования объектов БД в запросе.

21.8.5. Диаграмма отношений таблиц

Для лучшего понимания состава используемых запросом объектов БД, можно посмотреть диаграмму отношений таблиц, расположенную на вкладке «Отношения». Цвета блоков совпадают с цветами на строке-диаграмме в текстовом представлении плана запроса.

Всплывающее окно показывает тот же набор данных для узла, что и в текстовом представлении. Нажатие на блок узла обеспечивает контекстный переход к этому узлу в текстовом форматированном представлении, на вкладке «Explain».

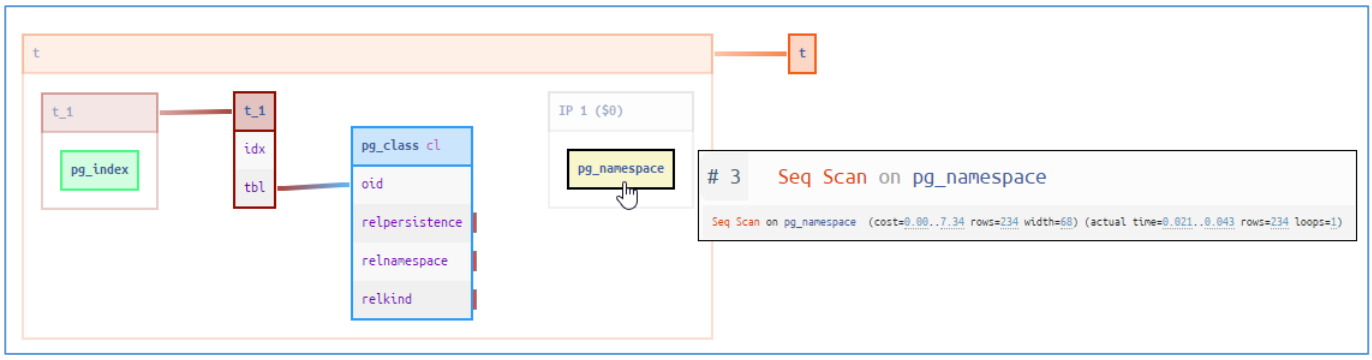

Рисунок 21.34 – Диаграмма отношения таблиц

Использование таблиц в узлах плана запроса, в виде списка, можно посмотреть на вкладке «Статистика»

21.8.6. Автоматические рекомендации по повышению качества запросов

В некоторых типовых случаях, при достаточном наборе данных, компонент JDS может предложить рекомендацию, для повышения производительности запроса в конкретном узле плана выполнения запроса. Такие рекомендации не являются обязательными. Они обозначаются особыми пиктограммами на диаграммах и в списках узлов, как например рекомендация на рисунке 21.35 - увеличить выделение оперативной памяти для обработки большого количества записей, с целью снижения нагрузки на дисковое хранилище.

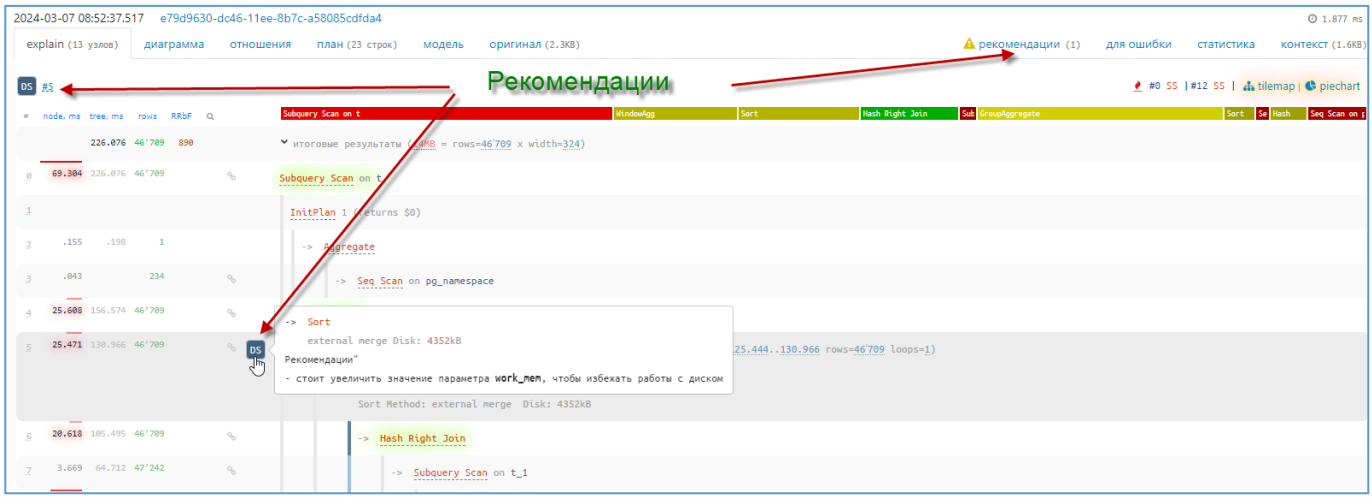

Рисунок 21.35 – Рекомендации по плану запроса

Рекомендации JDS могут содержать предложения:

— Выполнить ANALYZE, в случае если запросы, попавшие в журнал, не содержат планы выполнения;

— Выполнить VACUUM, если таблицы, используемые в запросах слишком разрежены;

— Создать индекс, если сортировка в запросе занимает много времени;

— Расширить используемый индекс, например, полями сортировки, если при выборке единственной записи перебирается много строк;

— Добавить составной индекс, если выполняется последовательное сканирование по нескольким индексам;

— Уточнить условие отбора по WHERE, если фильтр отбрасывает слишком много строк, из прочитанного.

В случае если план запроса содержит несколько рекомендаций, то все рекомендации удобнее просмотреть на вкладке «Рекомендации», как было показано на рисунке выше. Число рядом с наименованием вкладки – число рекомендаций. На странице списка рекомендаций, нажатие на номер узла обеспечивает контекстный переход к этому узлу в форматированном текстовом представлении, на вкладке «Explain».

22. ПОДРАЗДЕЛ «ПОДКЛЮЧЕНИЯ JDS» (JDS CONNECTIONS)

Вкладка «Подключения JDS» отображает количество подключений к компоненту пользовательского веб-интерфейса для администраторов «Jatoba data safe», позволяя выполнить меру безопасности, установленную Приказом № 17 ФСТЭК России:

Мера защиты УПД.9 (3) в части следующих требований:

— контроль и отображение администратору числа активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей.

После выбора цели отображаются столбцы:

— «Пользователь»;

— «Тип»:

  - JDS (подключение к компоненту);
  - БД (подключение к служебной БД компонента);

— «Количество подключений»;

— «Лимит подключений».

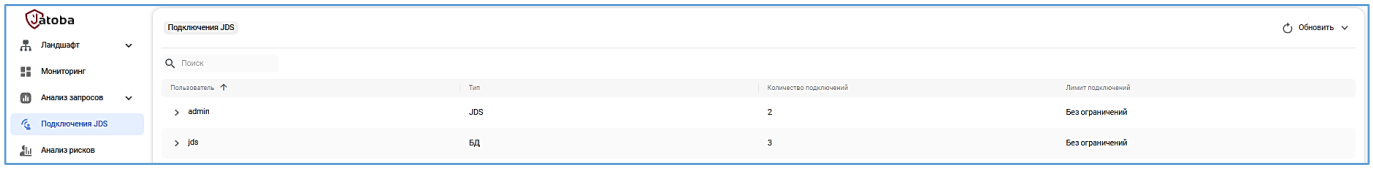

Рисунок 22.1 – Подраздел «Подключения JDS»

Лимит подключений для пользователей JDS устанавливается в карточке пользователя (см. п. 2.1.3).

Подключения от имени пользователя выполнено в виде раскрывающего списка, в котором отображаются:

— «Адрес подключения»;

— «Приложение» – версия приложения JDS, версия интернет браузера и версия ОС;

— «Время до отключения, чч:мм».

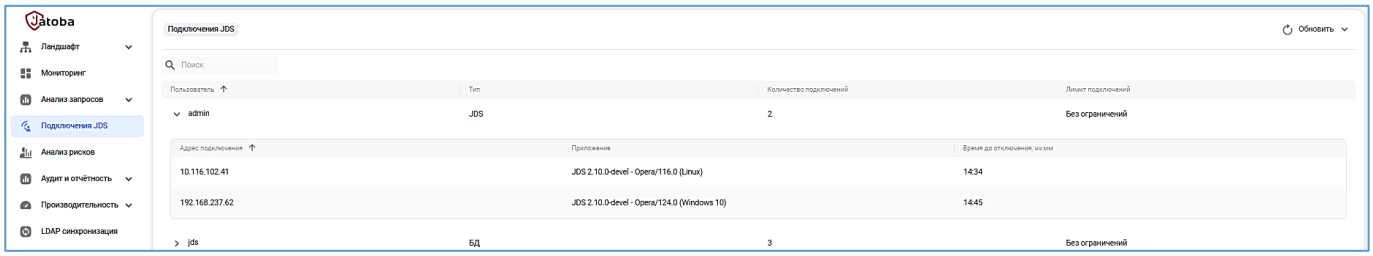

Рисунок 22.2 – Отображение дополнительной информации о подключении пользователя JDS

23. РАЗДЕЛ «РЕЗЕРВНОЕ КОПИРОВАНИЕ» (BACKUP)

Раздел «Резервное копирование» не доступен целевой СУБД «Jatoba» с версией ядра «18», т.к. компонент «pg_ProBackup» в данной версии не поддерживается.

Функционирование раздела обеспечивается следующими условиями:

— Настройка целевого хоста и непосредственно SSH-соединения (см. документ «Руководство по безопасности»);

— Установлены пакеты компонента pg_ProBackup (см. документ «Руководство по установке»):

- jatoba<ver>-pg-probackup;
- jatoba<ver>-ptrack.

Для активации компонента ptrack в СУБД «Jatoba» на целевом хосте, в разделе «Ландшафт» через «Параметры СУБД» изменить конфигурационный файл «postgresql.conf», прописав следующие строки:

```
shared_preload_libraries='ptrack'
```

Расширение ptrack устанавливается в порядке описанном в разделе 16.

Должен быть создан каталог хранения резервных копий, а также для внешнего каталога (по необходимости) и на него установлены права командой:

```
chown -R postgres /backup_dir(директория резервного
копирования)
```

23.1. Настройки для ProBackUp

Первоначальная настройка целевой СУБД выполняется в разделе «Резервные копии».

В разделе устанавливаются параметры, приведенные в таблице 23.1.

Таблица 23.1 – Требуемые параметры для настройки для probackup

Параметр	Значение	Примечание
Хост	IP	Значение присвоится автоматически
Порт	5433	Значение по умолчанию
СУБД	jatoba-<ver>	Значение присвоится автоматически
Роль для резервного копирования	postgres	Значение по умолчанию

Параметр	Значение	Примечание
БД для подключения	Имя БД	Значение устанавливается из выпадающего списка
Архивный режим	on/always	
Уровень WAL	logical/replication	
Количество подключений	1	Значение по умолчанию «1». При работе СУБД в кластере параметр «max_wal_senders» рекомендуется увеличить в диапазоне от 2 до 10.
Проверка контрольных сумм	чек бокс	
PTRACK	тумблер	

23.2. Вкладка «Хранилища»

Во вкладке «Хранилища» раздела «Ландшафт» настраивается хранилища, в котором и будут храниться резервные копии СУБД.

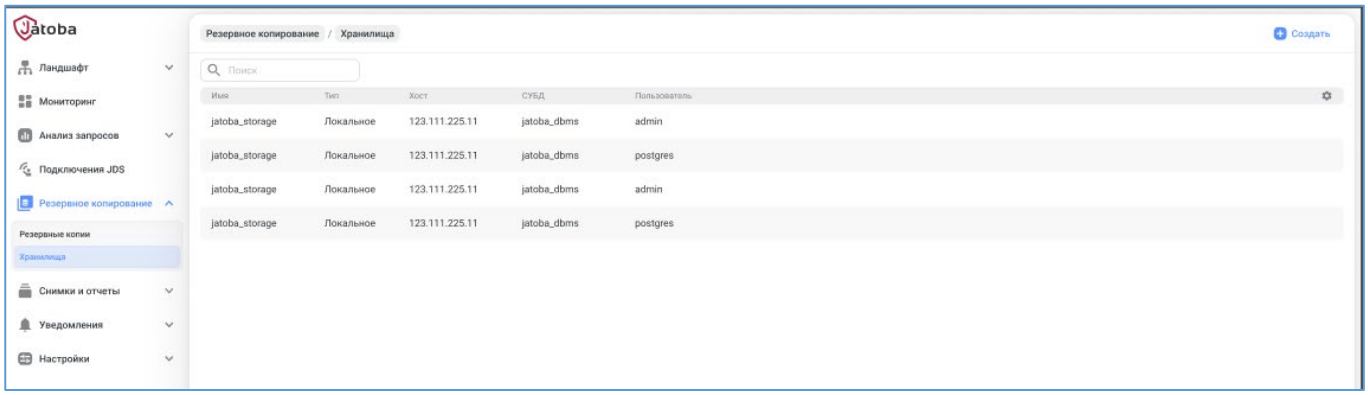

Рисунок 23.1 – Хранилища

Во вкладке устанавливаются параметры, приведенные в таблице 23.2.

Таблица 23.2 – Требуемые параметры для хранилища резервных копий

Параметр	Значение	Примечание
Тип	Локальное	
Имя	-	Имя хранилища
Путь к папке для резервных копий	-	Каталог в котором инициализируется хранилище
		Каталог будет создан автоматически, но требуется проверка установленных прав
Хост	IP	Имя или IP хоста. Значение выбирается из выпадающего списка из раздела «Ландшафт»
СУБД	-	Имя резервируемой СУБД. Значение выбирается из выпадающего списка из раздела «Ландшафт»
Путь к папке data	/var/lib/jatoba/<ver>/data	Целевой каталог СУБД
Пользователь	postgres	Имя администратора СУБД

Параметр	Значение	Примечание
Пользователь backup	postgres	Имя учетной записи для подключения к утилите
Внешний каталог	-	Путь к каталогу хранения резервных копий
Полных резервных копий	0-10 По умолчанию – 0	Параметр определяет политику хранения полных резервных копий.
Срок хранения	0-30	Срок актуальности резервных копий в хранилище. Максимальное значение - 30 дней
Копий для восстановления	Максимальное	Параметр определяет политику хранения (актуальности) копий для восстановления СУБД на момент времени в хранилище.
Тайм-аут архивации (сек)	300	Параметр определяет переключение сервера на новы сегмент WAL по истечении указанного периода времени Максимальное значение – 3600 сек.
Сжатие	Тумблер	zlib, pglz
Уровень сжатия	1	Максимальное значение -9
Каталог журналов	-	Директория хранения журналов. По умолчанию <директория хранилища>/log
Имя журнала	pg_probackup.log	
Размер журнал	Числовое значение в КБ/ МБ/ ГБ	Максимальный размер журнала - 1 ГБ
Время хранения	Числовое значение в Миллисекунды/ Секунды/ Минуты / Часы/ Дни	Параметр определяет срок актуальности файла журнала

Параметр «Внешний каталог» должен отличаться от «Путь к папке для резервных копий», т.к. при восстановлении произойдет конфликт обработки и СУБД не сможет быть восстановлена.

Учетная запись postgres должна иметь права доступа к директории, которая является параметром «Внешний каталог».

Поддерживается несколько хранилищ резервных копий, параметры которых возможно редактировать.

23.3. Вкладка «Резервные копии»

После вышеописанных действий возможно перейти к созданию резервных копий.

Первая резервная копия СУБД должна быть выполнена по типу резервирования «FULL» в режиме резервирования «ARCHIVE».

Перед первой полной архивацией СУБД в обязательном порядке требуется перезагрузка СУБД перезагрузка

Нажатие кнопки «Создать» вызывает вкладку «Создание резервной копии».

Во вкладке устанавливаются параметры, приведенные в таблице 23.3.

Таблица 23.3 – Требуемые параметры для создания резервной копии

Параметр	Значение	Примечание
СУБД	jatoba-<ver>	Значение присвоится выбором из выпадающего списка.
Хранилище резервных копий	-	Хранилище выбирается из выпадающего списка
Тип резервирования	FULL/ DELTA /PAGE /PTRACK	
Режим резервирования	ARCHIVE /STREAM	
Пароль пользователя postgres	-	Пароль вводится в ручную и не храниться.
Внешний каталог		Не обязательный параметр
Сжатие	тумблер	Включение отключение сжатия резервных копий. Не обязательное значение

При создании резервной копии с указанием внешнего каталога, отличного от предустановленного при конфигурировании хранилища рекомендуется указать также параметры сжатия. В ином случае, в резервную копию попадет каталог, который был предустановлен ранее.

Созданные резервные копии отразятся в общем списке.

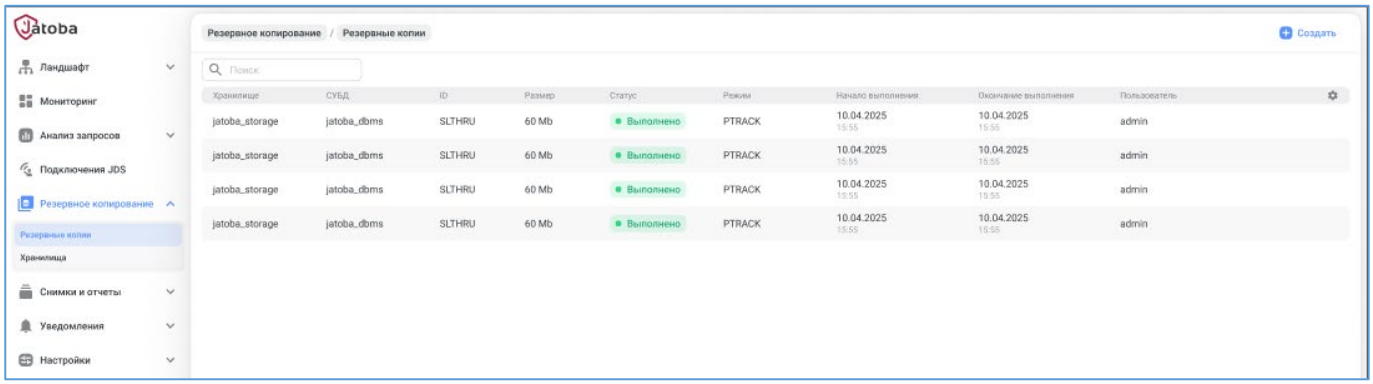

Рисунок 23.2 – Список резервных копий

В случае возникновения ошибки с созданием резервных копий, выполните действия описанные в п.п. 27.14, настоящего документа.

Для каждой созданной резервной копии в ее строке будет отражаться пиктограмма отчета о выполненном резервном копировании, вне зависимости от результатов.

23.4. Восстановление резервной копии

Имея список резервных копий, доступно выполнить восстановление СУБД. Пользователь компонента с правами администратора во вкладке «Резервные копии» выполняет следующие действия:

— Выбирает резервную копию;

— Вызывает контекстное меню и выбирает пункт "Восстановить".

Будет вызвано информационное окно восстановления.

В зависимости от типа резервной копии возможны два основных варианта восстановления:

1) Если выбрана копия типа «FULL»:

— СУБД останавливается;

— Целевая директория СУБД «data» - удаляется;

— После запускается процесс восстановления;

— По завершении восстановления СУБД запускается.

2) Если выбрана копия типа «DELTA», «PTRACK» или «PAGE»:

— СУБД останавливается;

— Запускается режим инкрементального восстановления;

— По завершении восстановления СУБД запускается.

В случае восстановления СУБД относительно копии, снятой с другой СУБД - восстановление по копиям в режиме «DELTA», «PTRACK» или «PAGE» завершится с ошибкой, т.к. не будут совпадать контрольные суммы файлов в копии и в целевой папке СУБД «data».

В таком случае, восстановление должно производиться из резервной копии типа «FULL», с зачисткой целевой папки СУБД «data».

24. РАЗДЕЛ «СНИМКИ И ОТЧЕТЫ» (SNAPSHOTS & REPORTS)

Раздел «Снимки и отчеты» предназначен для создания снимков состояния БД (Snapshots) и получения отчетов. Создавать снимки и получать отчеты возможно через иерархическую структуру виртуальных серверов. Полученные данные будут храниться в служебной БД компонента.

Перечень отчетов полностью описан в документе «Руководство по настройке. Часть 6. Руководство по настройке анализа производительности СУБД» Компонент «pg_Profile». 643.72410666.00067-07 98-01-06».

Расширение pg_profile установленное средствами раздела «Ландшафт» автоматически появится в разделе «Снимки и отчеты» (Snapshots & Reports) (см. п.п. 16 Раздел «Ландшафт». БД. Вкладка «Расширения»

В случае когда виртуальный сервер local был создан автоматически при установке расширения pg_stat_statements обязательно требуется в разделе «Ландшафт» через «Параметры СУБД» изменить конфигурационный файл postgresql.conf и добавить строку:

```
shared_preload_libraries = 'pg_stat_statements'
```

И применить внесенные изменения перезагрузкой СУБД.

Для нового сервера запись в конфигурационном файле делается автоматически.

24.1. Вкладка «Снимки» (Snapshots)

Во вкладке «Снимки» отображаются хранимые снимки состояния БД. Выбирается один, несколько или все сервера. Компонент автоматически предложит выбрать хосты на которых установлено расширение «pg_profile».

Новый снимок создаётся через кнопку «Создать». После чего откроется окно «Создание снимка», в котором выбирается виртуальный сервер и доступно установить чекбокс «Добавить данные о размерах». При нажатии кнопки «Сохранить» снимок будет создан.

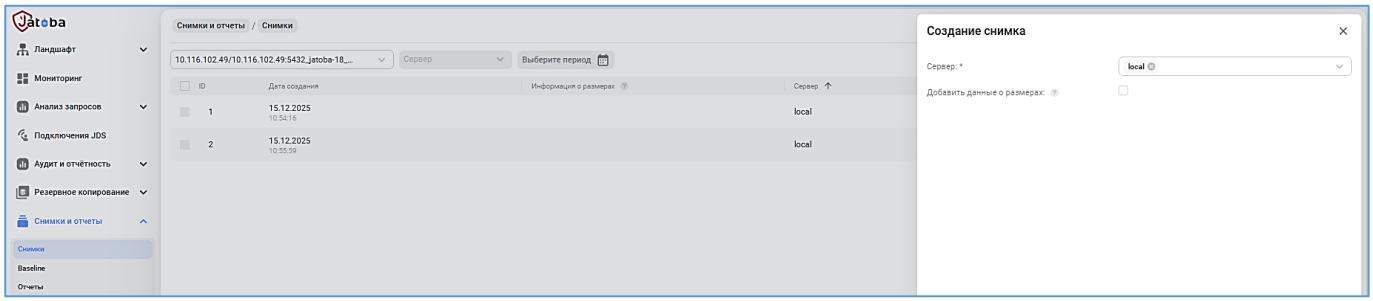

Рисунок 24.1 - Создание «Снимка»

Далее созданный снапшот (снимок) будет храниться в служебной БД.

Последний снимок с данными удалить невозможно.

Если снимок был создан не средствами подраздела, а вручную, то при открытии вкладка «Снимки» она синхронизируется под внесенные изменения.

Во вкладке по кнопке в форме троеточия, расположенной в правом верхнем углу доступны операции экспорта/импорта снимков. При нажатии кнопки «Экспортировать» открывается окно «Экспорт», в котором следует выбрать:

— Сервер;

— Начальный снимок;

— Конечный снимок.

После нажатия кнопки «Экспортировать» сформируется файл export.csv.

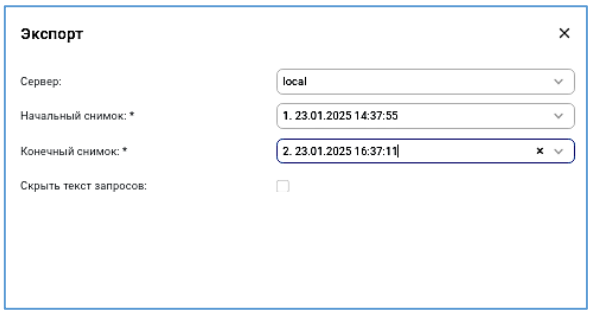

Рисунок 24.2 – Экспорт снимков

При нажатии кнопки «Импортировать» открывается окно «Импорт». Импортируются снимки в формате файлов *.csv максимального размера 28 МБ.

Импорт снимков выполняется, выбором файла либо перетаскиванием в поле «Файл».

24.2. Вкладка «Baseline»

Baseline – именованная последовательность снапшотов, которая имеет отдельную от настроенной политику хранения. Можно задать определенное время хранения в днях. Также можно создать последовательность снапшотов только для определенного периода времени.

Во вкладке доступно создание:

— Baseline по снимкам;

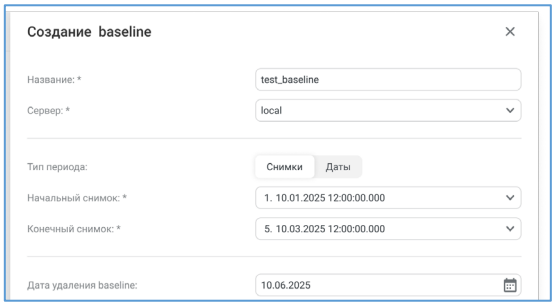

Рисунок 24.3 – Создание baseline по снимкам

— Baseline по датам.

Созданные Baseline отобразятся в списке и далее могут использоваться в формировании отчетов.

24.3. Вкладка «Отчеты» (Reports)

Во вкладке «Отчеты» доступно создавать или просматривать ранее созданные отчеты.

Нажатие кнопки «Создать» вызывает окно «Создание отчета», в котором устанавливаются параметры отчета.

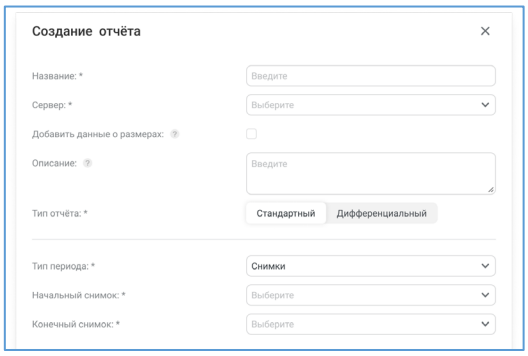

Рисунок 24.4 – Окно «Создание отчета»

Отчеты в компоненте бывают 2-х видов:

— стандартные отчеты;

— дифференциальные отчеты.

Стандартные отчеты содержат статистическую информацию для определенного периода времени.

Дифференциальные отчеты содержат статистическую информацию за два выбранных периода, позволяя легко сравнить показатели.

Параметры формируемых отчетов приведены в таблице 24.1

Таблица 24.1 – Параметры отчетов

Тип отчёта	**Тип периода**	**Первый параметр**	**Второй параметр**
Стандартный			
	Снимки	Начальный снимок: *	Конечный снимок: *
	Даты	Начальная дата *	Конечная дата *
	Baseline	Baseline: *	
Дифференциальный			
	Снимки - Снимки	**Интервал 1**	**Интервал 2**
		Начальный снимок: *	Начальный снимок: *
		Конечный снимок: *	Конечный снимок: *
	Даты - Даты	**Интервал 1**	**Интервал 2**
		Начальная дата *	Начальная дата *
		Конечная дата *	Конечная дата *
	Baseline - Baseline	**Интервал 1**	**Интервал 2**
		Baseline: *	Baseline: *
	Даты -Baseline	**Интервал 1**	**Интервал 2**
		Начальная дата *	Baseline: *
		Конечная дата *	
	Baseline - Даты	**Интервал 1**	**Интервал 2**
		Baseline: *	Начальная дата *
			Конечная дата *
	Baseline - Снимки	**Интервал 1**	**Интервал 2**
		Baseline: *	Начальный снимок: *
			Конечный снимок: *
	Снимки - Baseline	**Интервал 1**	**Интервал 2**
		Начальный снимок: *	Baseline: *
		Конечный снимок: *	

Сформированные отчеты отразятся списком во вкладке «Отчеты», которые возможно просмотреть, скачать или удалить.

Отчет скачивается в формате *.html

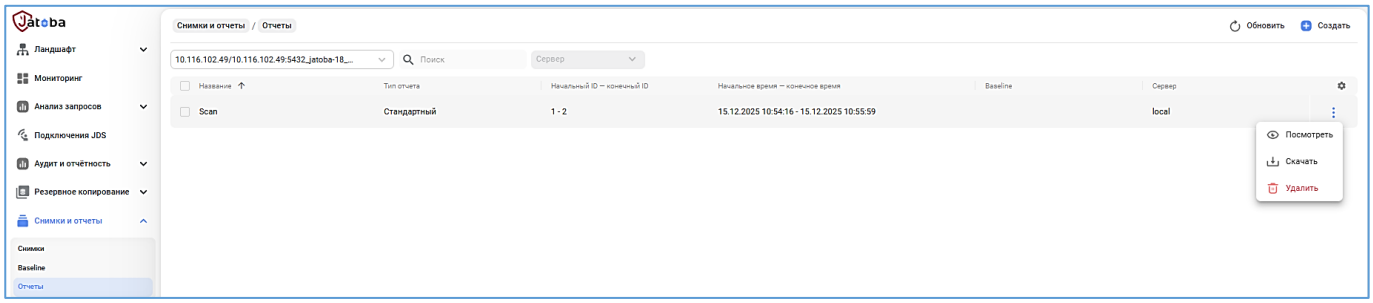

Рисунок 24.5 – Список отчетов

Просматриваемый отчет откроется в отдельной вкладке браузера.

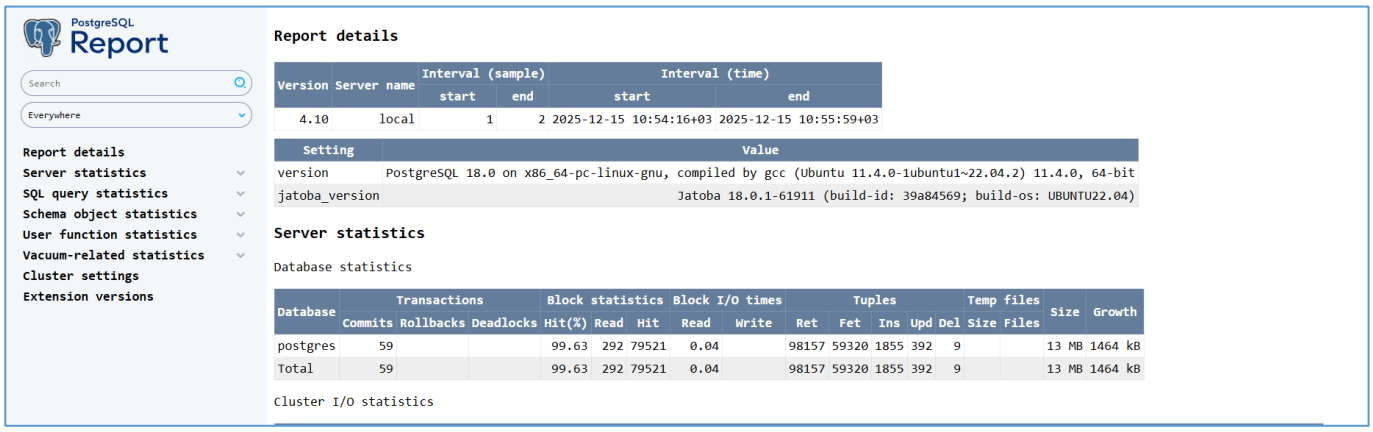

Рисунок 24.6 – Форма отчета «Snapshots & Reports»

25. 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» (см. п. 25.2.1);

Поиск выполняется по классу события или по коду события.

— «События учетных записей» (см. п. 25.2.2);

Поиск выполняется по ключевым фразам для выполнения мер безопасности УПД.1 (5) и УПД.9 (4) в соответствии с Приказом № 17 ФСТЭК России.

— «Произвольный текст» (см. п.25.2.3).

Поиск выполняется, по ключевым словам, задаваемым пользователем JDS.

Раздел «Уведомления» имеет функциональные возможности:

— настройки сервисов отправки сообщений (Zulip. см. п. 25.1.2) и писем (Email. см. п. 25.1.1);

— настройки периодичности отправки сообщений и писем (см. п. 25.1.3);

— формированию подписок на события безопасности пользователей JDS (см. п. 25.2);

— отправки сообщений и писем (см. п. 25.3.1);

— отправки писем с вложениями пользователей JDS подписанным на события безопасности (см. п. 25.3.1.1).

25.1. Подраздел «Настройки» (Settings)

25.1.1. Сервисы Email (Email services)

Компонент JDS обладает функциональной возможностью отправки уведомлений используя почтовые сервисы.

Предварительно должен быть создан почтовый ящик и полученные учетные данные для доступа к нему.

Для перехода к настройке Сервиса Email потребуется перейти по пути: «Настройки»→«Сервисы». Нажать пиктограмму «Добавить» в правом верхнем углу.

В открывшимся окне «Создание Email подключения» выполнить следующие действия:

— тумблер «Статус»;

Переключить тумблер если планируется, что подключение будет активным.

— «Наименование»*;

В поле можно указать произвольное название подключения.

— «Хост»*;

В поле вносится адрес хоста почтового сервера.

— «Порт»*;

В поле вносится порт хоста почтового сервера. При использовании SSL-соединения указывается порт – 465. Для SMTP протокола указывается порт TCP – 25.

— тумблер «Использование SSL»;

Переключить тумблер если планируется, что подключение будет использоваться SSL подключение. Параметры порта описаны выше.

— «Имя пользователя»*;

В поле вносится имя пользователя почтового ящика. Допускается внести полное наименование почтового ящика.

— «Пароль»*;

В поле указывается пароль для почтового ящика.

— «Имя отправителя»*;

В поле указывается имя отправителя.

— «Адрес отправителя»*;

В поле вносится адрес почтового ящика с почтовым доменом.

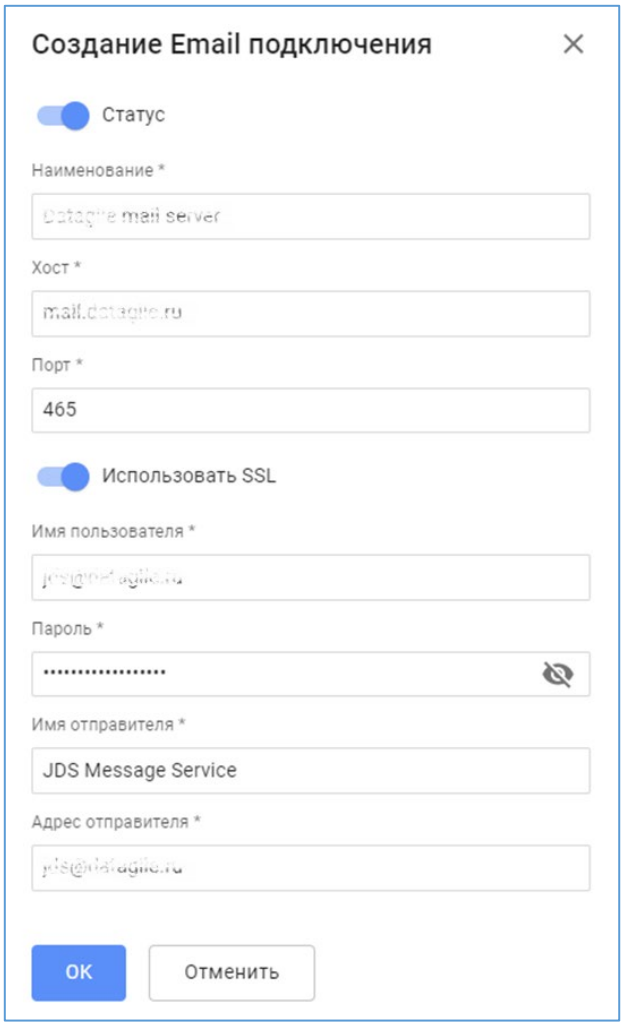

Рисунок 25.1 – Окно «Создание Email подключения»

Все поля в окне «Создание Email подключения» обязательны для заполнения

После сохранения настроек, созданное подключение появится в списке подключений.

25.1.2. Сервисы Zulip (Zulip services)

Использование сервиса мессенджера Zulip возможно только в случае, когда он используется в инфраструктуре. Предварительно настраивается бот Zulip и его параметры используются для последующей настройки сервиса Zulip.

25.1.2.1 Настройка бота Zulip

Настройка бота Zulip выполняется вне пространства компонента JDS. Настройка проводится на веб-странице чата Zulip.

Перейдя в чат потребуется:

— открыть личные настройки;

— выбрать вкладку «Боты».

В открывшейся вкладке «НАСТРОЙКИ/БОТЫ» заполнить поля:

— «Полное имя»;

В представленном примере указывается имя «JDS-agent».

— «Адрес электронной почты бота».

В поле вносится аналогичное имя «JDS-agent», а сервер Zulip автоматически подставит адрес E-mail. После имени до почтового домена будет подставлен префикс «-bot».

Проверив внесенный значения, создается бот нажатием на пиктограмму «Создать бот».

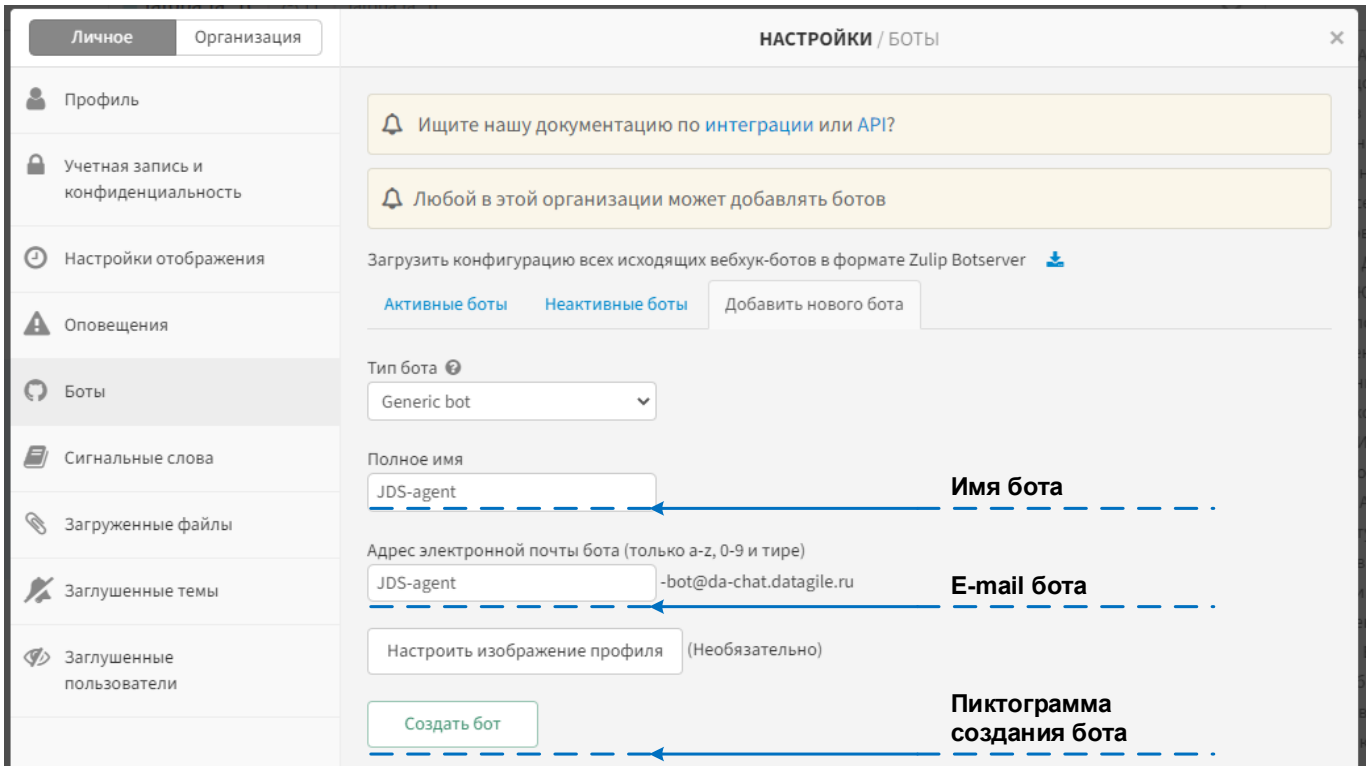

Рисунок 25.2 – Окно настройки Zulip бота

Автоматически откроется вкладка «Активные боты»

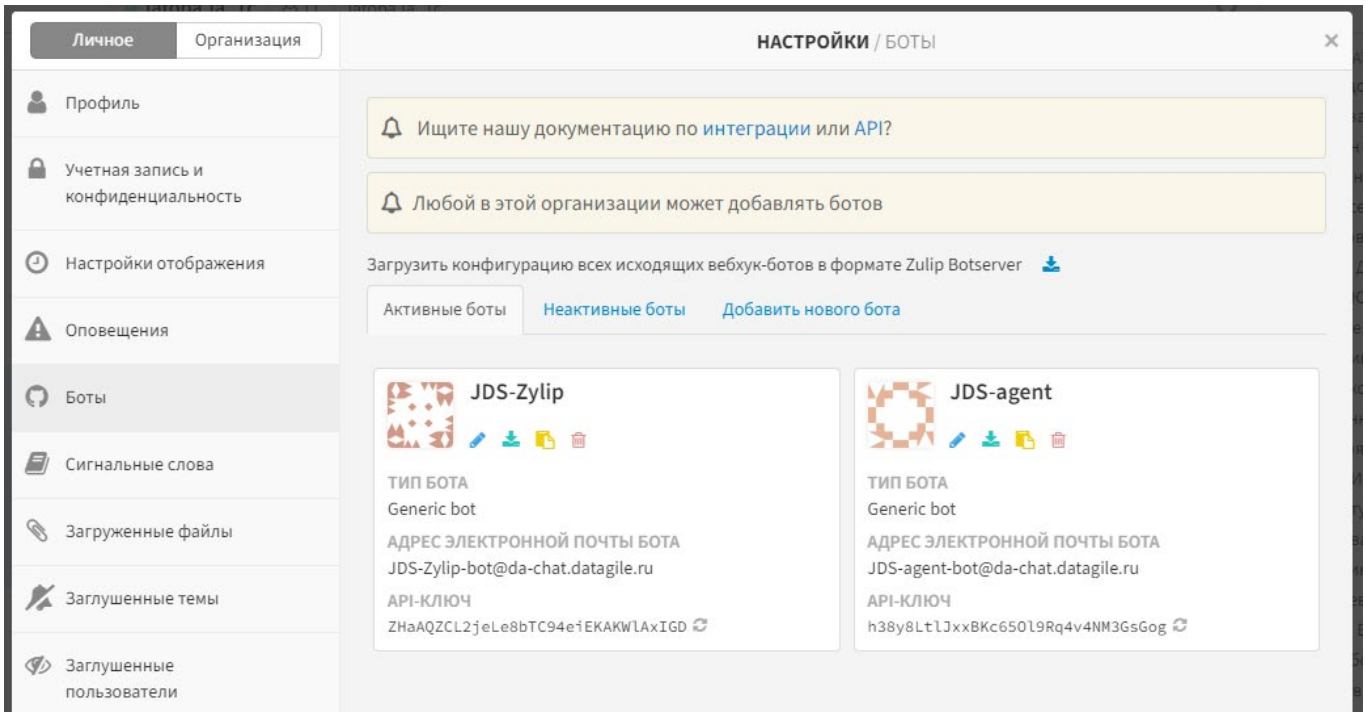

Рисунок 25.3 – Вкладка «Активные боты»

25.1.2.2 Создание Zulip подключения

Полученные параметры Zulip-бота используются в создании Zulip подключения.

Для перехода к настройке сервиса Zulip потребуется перейти по пути: «Настройки»→«Сервисы». Нажать пиктограмму «Добавить» в правом нижнем углу.

В открывшимся окне «Создание Zulip подключения» выполнить следующие действия:

— тумблер «Статус»;

Переключить тумблер если планируется, что подключение будет активным.

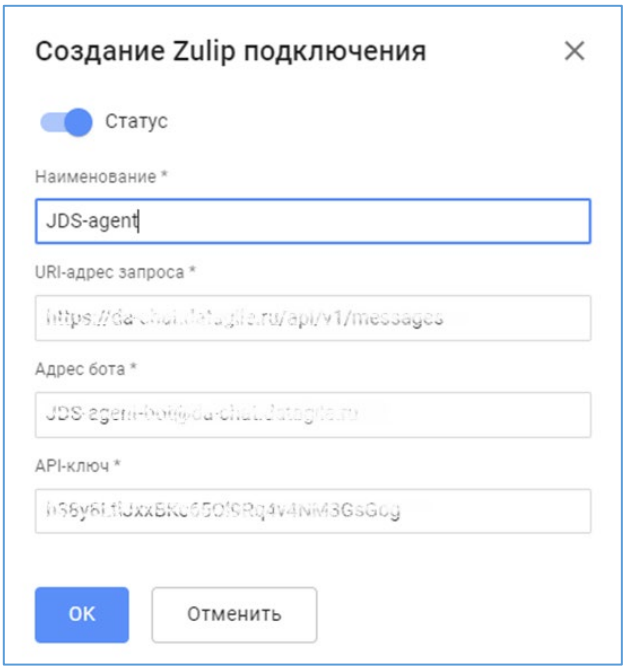

Рисунок 25.4 – Окно «Создание Zulip подключения»

— поле «Наименование»;

В поле можно внести произвольное название подключения.

— «URI-адрес запроса»;

Внести URI-адрес запроса. (URI-адрес возможно получить у администратора сервиса Zulip)

— «Адрес бота»;

В поле вносится E-mail бота (см. Рисунок 25.3).

— «API-ключ».

В поле вносится API-ключ бота (см. Рисунок 25.3).

Все поля в окне «Создание Zulip подключения» обязательны для заполнения

После сохранения подключение появится в общем списке.

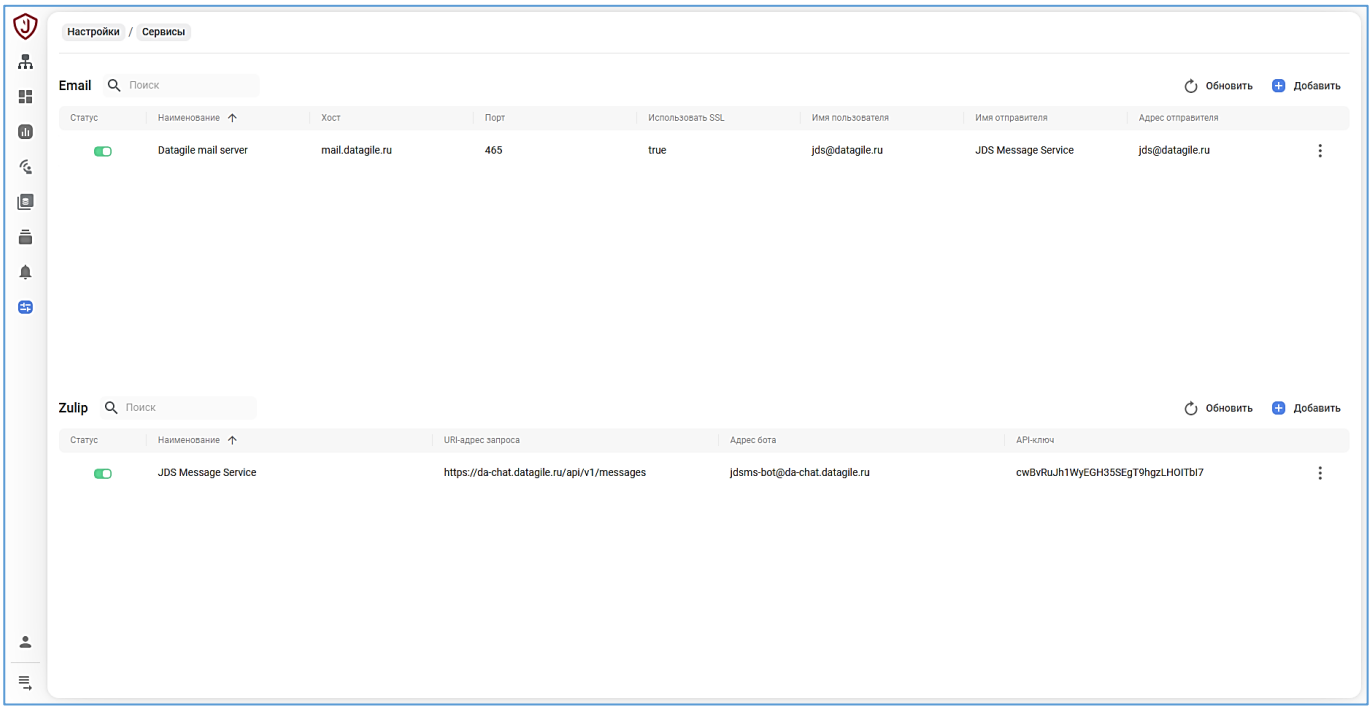

Рисунок 25.5 – Список подключений Zulip

25.1.3. Настройки обработки (Processing settings)

Подраздел «Обработчики» находится по пути: раздел «Уведомления» → подраздел «Сообщения». На вкладке «Обработчики» отражаются предустановленные параметры периодичности отправки сообщений.

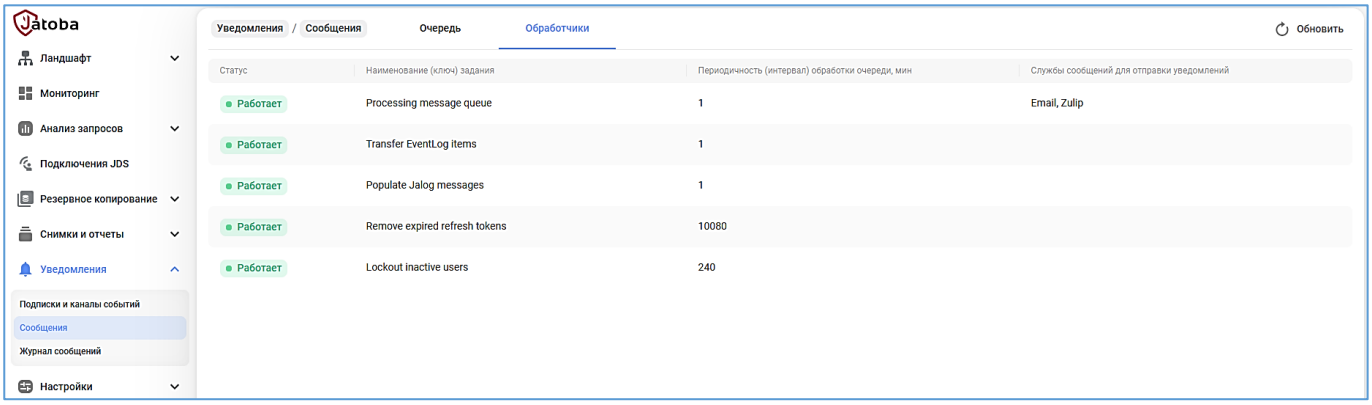

Рисунок 25.6 – Вкладка «Настройки обработки»

Изменить преднастроенные параметры можно от имени и с правами администратора компонента JDS, в каталоге веб-сайта в конфигурационном файле appsettings.json. В файле изменяется параметр «Interval» не целое число.

25.2. Подраздел «Подписки» (Subscriptions)

Подраздел служит для формирования каналов событий и подписок пользователей JDS на события безопасности СУБД и JDS. Формирование подписок следует осуществлять после основных настроек раздела описанных в разделе 25.1 настоящего документа.

Процесс формирования «Подписки и каналов событий» показан на рисунке 25.7.

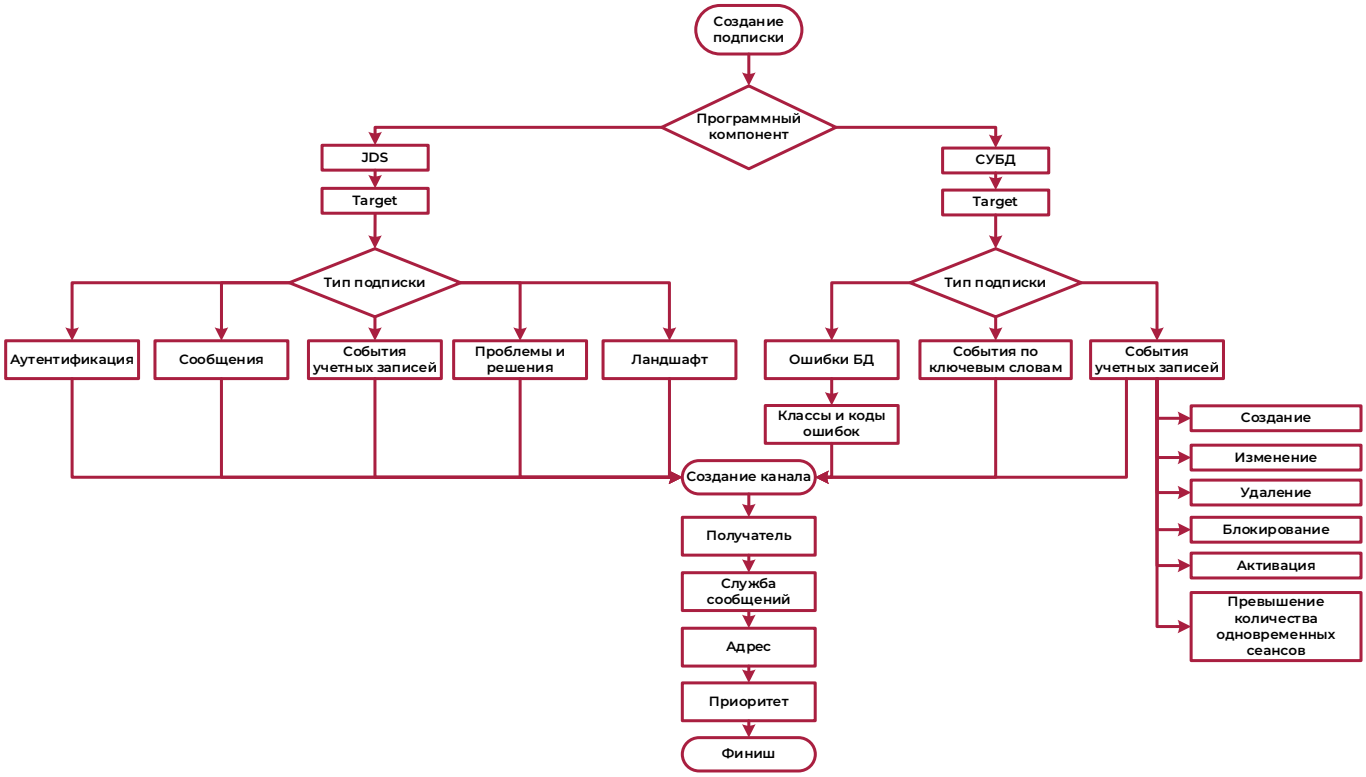

Рисунок 25.7 – Схема создания подписки

Условно процесс делится на этап создания канала событий и подписки на него пользователей.

Создание канала событий

Для перехода к формированию подписок потребуется перейти по пути: «Уведомления» → «Подписки». В окне «Подписки и каналы событий» нажать пиктограмму «Добавить» в правом верхнем углу.

В открывшимся окне «Создание канала событий» выполнить следующие действия:

— «Наименование»;

Поле является редактируемым и в него можно внести наименование подписки отражающую специфику (отличительную черту).

— «Программный компонент»;

Выпадающий список, в котором устанавливается единственный выбор компонента:

- JDS;
- СУБД.

— «Цель»;

Выпадающий список, в котором выбирается подключенная инсталляция СУБД, т.е. «Цель».

— «Тип подписки».

Поле выполнено в формате выпадающего списка, в котором возможно сделать единственный выбор и является зависимым от выбранного «Программного компонента».

Подробное описание механизма работы типа подписок приведено в пунктах настоящего документа:

- Ошибки БД (см. п. 25.2.1);
- События учетных записей (см. п. 25.2.2);
- Произвольный текст (см. п.25.2.3);

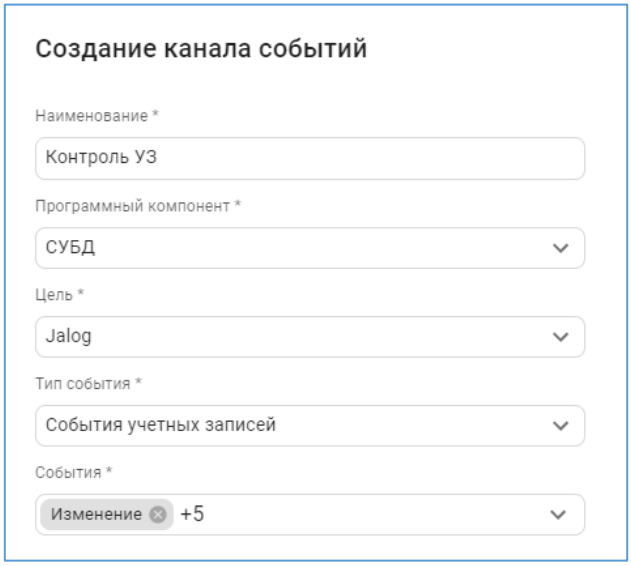

Рисунок 25.8 – Окно «Создание канала событий»

Созданный канал событий отразится в общем списке.

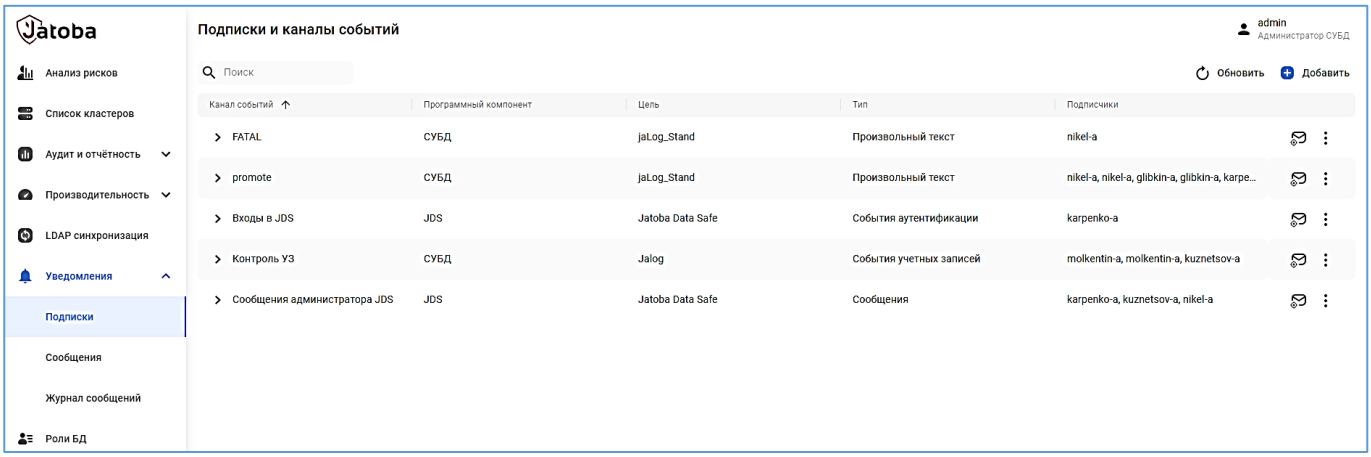

Рисунок 25.9 – Список каналов событий

Механизм создания канала событий проконтролирует созданный канал событий и не позволит сохранить новый канал если будут идентичны названия каналов событий, цель и тип поиска.

На данном этапе формирование канала событий закончено.

Канал событий возможно отредактировать или удалить через контекстное меню, вызываемое через пиктограмму в правой стороне строки канала.

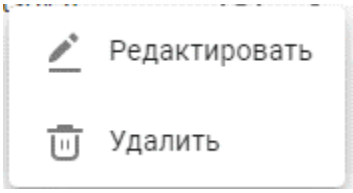

Рисунок 25.10 – Контекстное меню операций с каналом событий

Подписка пользователя

После того как создан канал событий, становится доступной функциональная возможность подписки пользователей.

Подписать пользователя на канал событий возможно через кнопку, расположенную в правой стороне строки канала.

Рисунок 25.11 – Кнопка добавления подписчика

Нажатие на кнопку вызовет окно «Создание подписки».

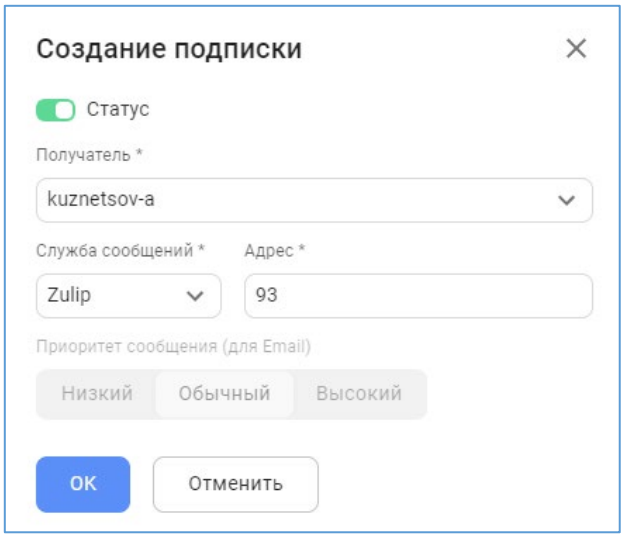

Рисунок 25.12 – Окно «Создание подписки»

В окне устанавливаются следующие параметры:

— «Статус»;

Тумблер означающий активность подписки пользователя.

— «Получатель»;

Поле выполнено в формате выпадающего списка, в котором возможно сделать единственный выбор. В списке получателей могут быть только пользователи компонента JDS. Описание создания пользователей JDS приведено в п. 2.1.3 настоящего документа.

— «Служба сообщений»;

Для установки «Службы сообщений» требуется в выпадающем списке выбрать:

- Email (25.1.1);
- Zulip (25.1.2).

— «Адрес»;

Поле «Адрес» редактируемое, можно заполнить вручную либо подставить адрес электронной почты из карточки пользователя JDS.

— «Приоритет сообщения*»:

- Низкий;
- Обычный;

- Высокий.

После сохранения, подписчик отразится в списке подписчиков канала событий.

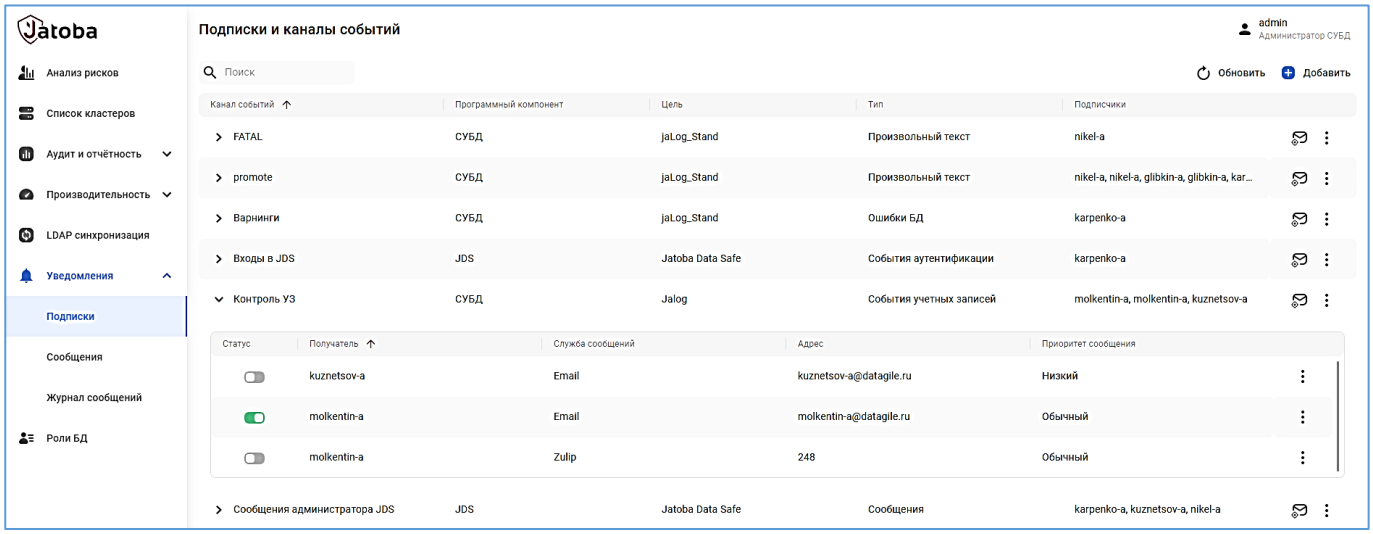

Рисунок 25.13 – Список подписчиков канала событий

Функциональные возможности механизма подписок позволяют добавлять:

— множество пользователей;

— одного и того же пользователя с разными службами сообщений.

Канал событий возможно отредактировать или удалить через контекстное меню, вызываемое через пиктограмму в правой стороне строки подписчика.

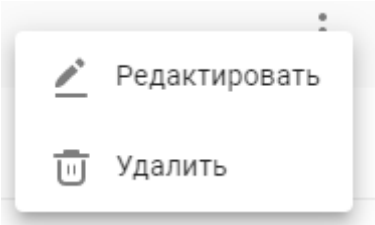

Рисунок 25.14 – Контекстное меню редактирования подписчика

25.2.1. Ошибки БД

Создать подписку на ошибки СУБД возможно с помощью:

— меню «Программный компонент» → «СУБД»;

— меню «Источник» выбрать одну из подключенных к JDS СУБД;

— меню «Тип события» → «Ошибки БД».

После чего станет доступной меню «Классы и коды ошибок».

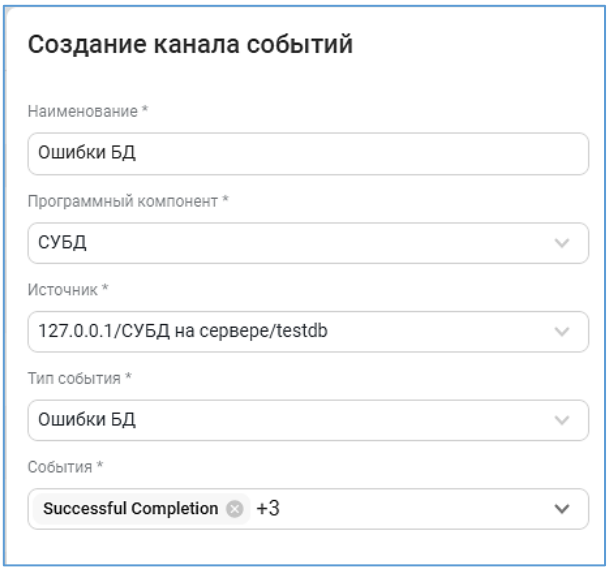

Рисунок 25.15 – Поле «Тип события»

Выбрав выпадающий список меню «Событий», отроется иерархический список. В списке доступен множественные выбор классов и/или кодов ошибок событий.

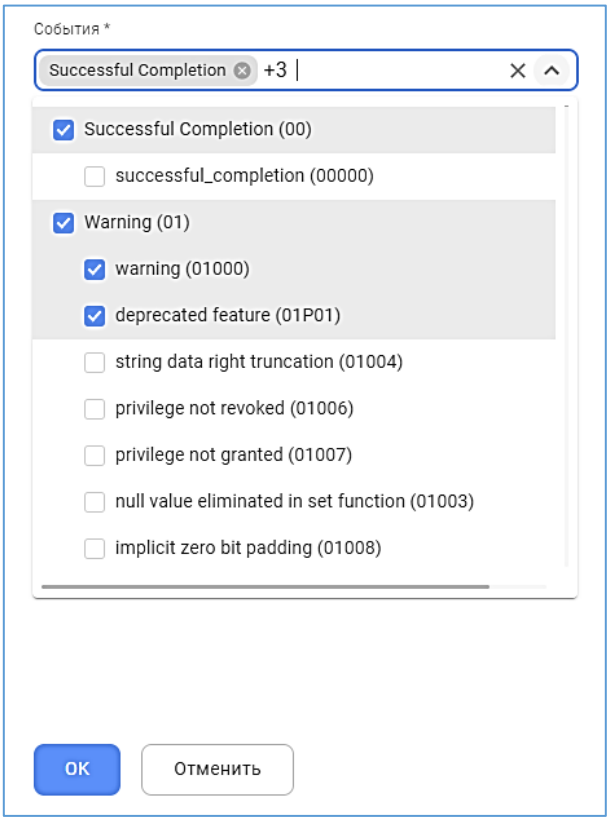

Рисунок 25.16 – Окно «Классы и коды ошибок»

В иерархическом списке доступно выбрать класс события или код подкласса события. Перечень классов событий приведен в Приложении 1.

25.2.2. События учетных записей

Использование типа подписки «События учетных записей» позволяет выполнить меры безопасности, установленные Приказом № 17 ФСТЭК России:

1) (УПД.1) «Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей».

Мера защиты УПД.1 в части следующего требования:

— оповещение администратора, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях.

Усиление меры защиты УПД.1(5) в части следующего требования:

— автоматический контроль заведения, активации, блокирования и уничтожения учетных записей пользователей и оповещение администраторов о результатах автоматического контроля.

2) (УПД.9) «Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы».

Усиление меры защиты УПД.9 (4) в части следующего требования:

— оповещение администратора о попытках превышения числа установленных допустимых активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи.

Создать подписку на «События учетных записей» СУБД возможно с помощью:

— меню «Программный компонент» → «СУБД»;

— меню «Цель» выбрать одну из подключенных к JDS СУБД;

— меню «Тип подписки» → «События учетных записей».

После чего станет доступной меню «События». Выбрав пункты:

— «Создание»;

— «Изменение»;

— «Удаление»;

— «Блокировка»;

— «Активация»;

будет выполняться поиск в служебной БД «ja_log» по набору ключевых фраз приведенных в таблице 25.1, для обеспечения меры безопасности УПД.1(5).

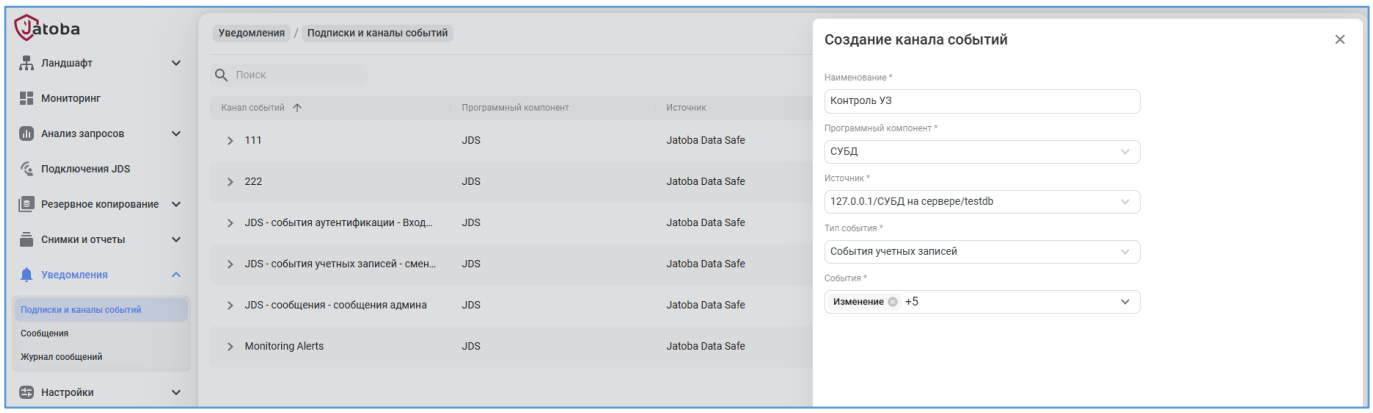

Рисунок 25.17 – Создание канала по типу события «События учетных записей»

Выбрав пункт «Превышение количества одновременных сеансов» будет выполняться поиск в служебной БД «ja_log» по ключевой фразе «too many connections», таким образом обеспечивается мера безопасности УПД.1(5).

Таблица 25.1 – Соответствие пунктов поля «События» с ключевыми фразами и мерами безопасности

Параметр в поле «События»	**Команда**	**Примечание**	**Мера безопасности**
Создание	CREATE ROLE CREATE USER CREATE GROUP	Заведение УЗ	УПД.1(5)
Изменение	ALTER GROUP ALTER ROLE ALTER USER ALTER.* OWNER TO ALTER DEFAULT PRIVILEGES GRANT REVOKE ALTER GROUP CREATE POLICY ALTER POLICY DROP POLICY SET ROLE RESET ROLE SET SESSION AUTHORIZATION RESET SESSION AUTHORIZATION	Изменение сведений, полномочий, ограничений УЗ	УПД.1(5)
Удаление	DROP ROLE DROP USER DROP GROUP	Уничтожение УЗ	УПД.1(5)

Параметр в поле «События»	Команда	Примечание	Мера безопасности
Блокировка	securityprofile.lock_account Account locked	Блокирование УЗ	УПД.1(5)
Активация (разблокировка)	securityprofile.unlock_account	Активация УЗ	УПД.1(5)
Превышение количества одновременных сеансов	too many connections	Количества сеансов УЗ	УПД.9 (4)

Далее, как описано выше, устанавливаются параметры адресата.

25.2.3. Произвольный текст

Подписка, по ключевым словам, предоставляет возможность пользователю компонента JDS самостоятельно устанавливать критерии поиска событий в целевой СУБД.

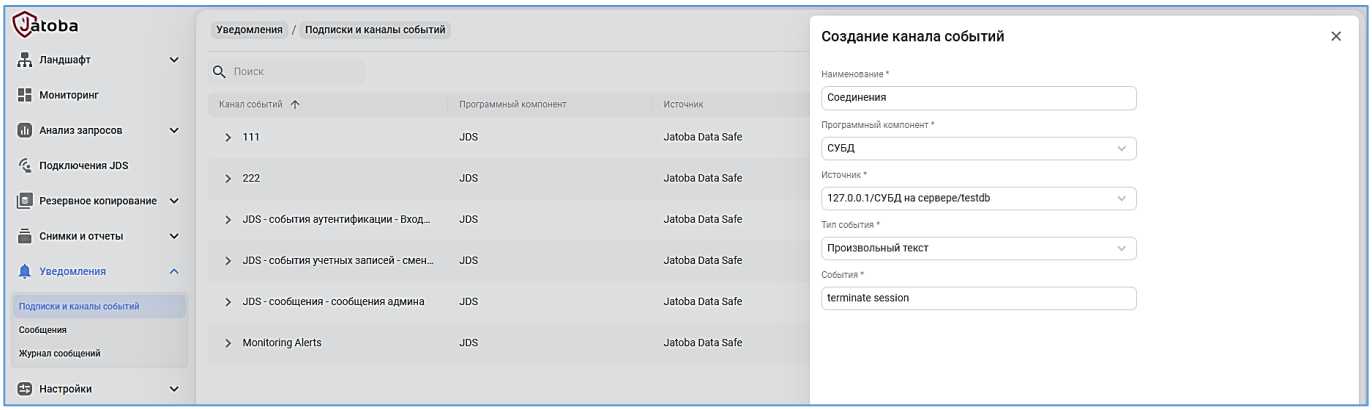

Рисунок 25.18 – «Тип события» «Произвольный текст»

25.2.4. Канал событий программного компонента JDS

Канал событий программного компонента JDS позволяет получать уведомления по событиям, приведенным в таблице 25.2.

Таблица 25.2 – Перечень типа событий и событий канала JDS

Тип события	События	Раздел документации
События аутентификации	Пользователь вошел в систему	
	Пользователь вышел из системы	
Сообщения	Сообщения администратора	
События учетных записей	Пароль изменен	2.2
Проблемы и решения	Задача запущена	11.3
	Задача завершена	
	Задача создана	

Тип события	События	Раздел документации
	Задача отредактирована	
	Задача удалена	
Ландшафт	Hba файл отредактирован	6
	Hba файл восстановлен	
	Конфигурация перезагружена	
	Создана резервная копия Hba файла	
	Список резервных копий Hba файла	
	Сервис СУБД запущен	
	Сервис СУБД остановлен	
	Сервис СУБД перезапущен	
	Автозапуск сервиса СУБД включён	
	Автозапуск сервиса СУБД выключен	

25.3. Подраздел «Сообщения» (Messages)

Подраздел «Сообщения» предназначен для:

— контроля отправленных сообщений (25.4);

— мониторинга сообщений, стоящих в очереди (25.3.1);

— отправки сообщений с вложениями подписчикам на определенные события (25.3.1.1).

Подраздел имеет две вкладки:

— «Очередь»;

— «Обработчики».

25.3.1. Очередь (queue)

В случае наступления события, на которое сформирована подписка, генерируется сообщение и попадает в «Очередь».

Через время, установленное на вкладе «Настройки обработки» (25.1.3), сообщение будет оправлено и отразится на вкладке «Журнал сообщений» (25.4).

25.3.1.1 Отправка сообщений

Вкладка «Очередь» имеет дополнительную функциональную возможность отправки сообщений с вложениями адресатам, подписанным на определенную категорию событий.

В качестве примера:

— сформировать в подразделе Матрица доступа (Access matrix) файл (17);

— создать сообщение;

— отправить.

На вкладе «Очередь» в правом верхнем углу нажать пиктограмму «Добавить». После чего откроется окно «Создания сообщения» (Create a message).

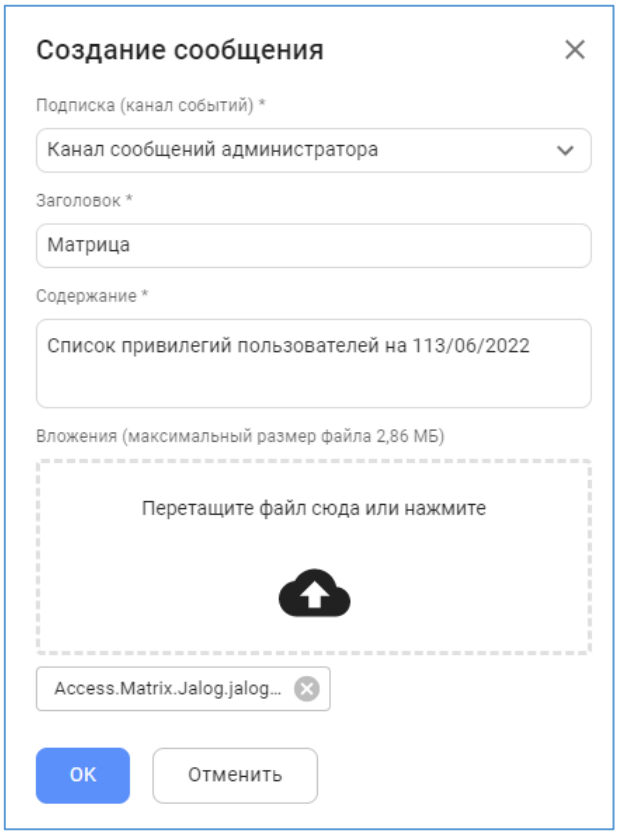

Рисунок 25.19 – Окно «Создания сообщения»

Установка параметров сообщений схожа с оформлением подписки пользователя JDS, для чего потребуется заполнить поля:

— «Подписка (канал события)*»;

Выбрать в выпадающем списке ранее сформированные подписки.

— «Заголовок *»;

Заполнить текстовую часть заголовка письма (темы).

— «Содержание *»;

Заполнить текстовую часть содержания письма.

— «Вложения».

При необходимости сформировать вложение кликнув на поле.

В приводимом примере ранее сформированную и экспортированную матрицу доступа вложить в сообщение.

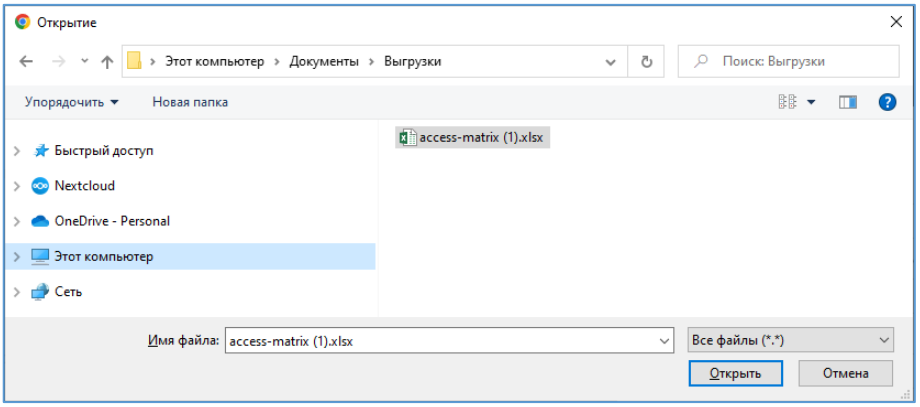

Рисунок 25.20 – Окно выбора вложения

Сохранить сформированное сообщение.

После чего сообщение отразится в списке сообщений в очереди.

Через время, установленное в «Настройке обработки» (25.1.3), сообщение отправится и попадет в «Журнал сообщений» (25.4).

Полученное адресатом сообщение будет иметь аналогичный вид, как представлено на рисунке 25.21.

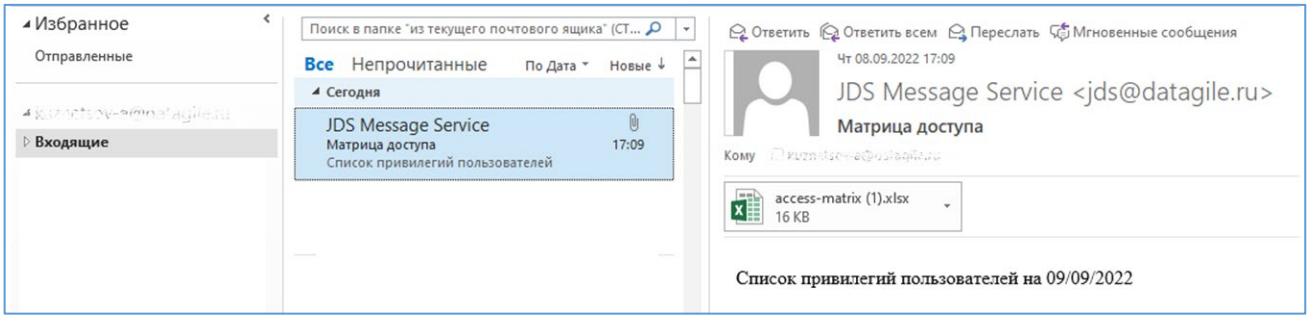

Рисунок 25.21 – Письмо сформированное на вкладе «Очередь сообщений» компонента JDS

Где:

— в адресе отправителя будут отражены «Имя отправителя» и «Адрес отправителя», которые были установлены в параметрах «Сервисы Email» (25.1.1);

— в теме письма будет указан «Заголовок», который указали в процессе формирования сообщения (см. Рисунок 25.19);

— в теле письма отражается «Содержание» (см. Рисунок 25.19);

— вложение соответствующее отправленному.

Отправка сообщений с вложениями возможно только для пользователей JDS, для которых установлена отправка писем через Email подключения

25.3.2. Обработчики (Handlers)

Вкладка «Обработчики» имеет информационный характер, в которой отображается информация:

— «Статус»;

— «Наименование (ключ) задания»;

— «Периодичность (интревал) обработки очереди, мин»;

— «Службы сообщений для отправки уведомлений».

Отображаемые параметры недоступны для редактирования.

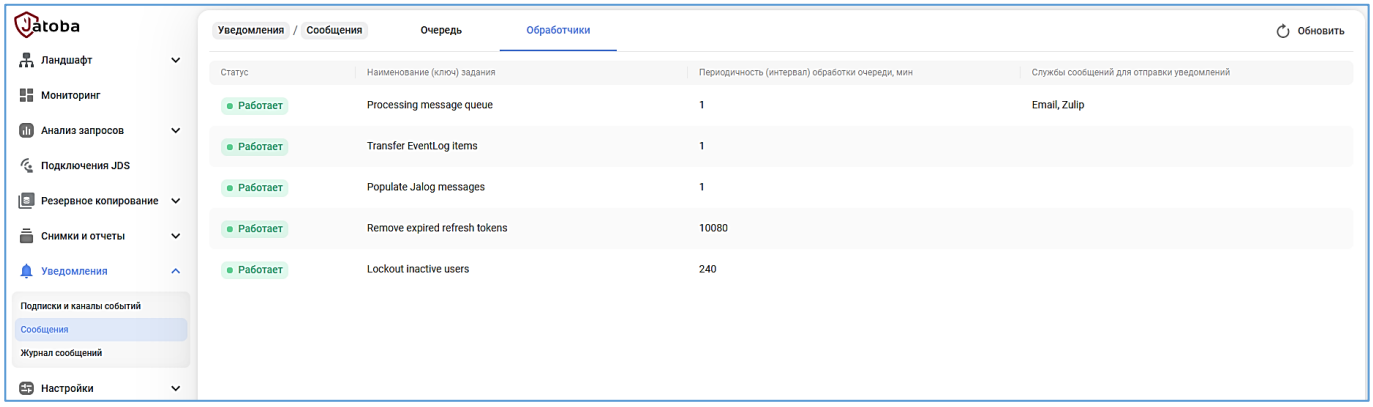

Рисунок 25.22 – Вкладка «Обработчики»

25.4. Журнал сообщений (Message log)

Вкладка «Журнал сообщений» выполняет контрольную функцию регистрации отправленных сообщений.

Список сообщений невозможно редактировать. Доступна сортировка по столбцам, а также полнотекстовый поиск.

При нажатии на вложение загрузится отправленный файл.

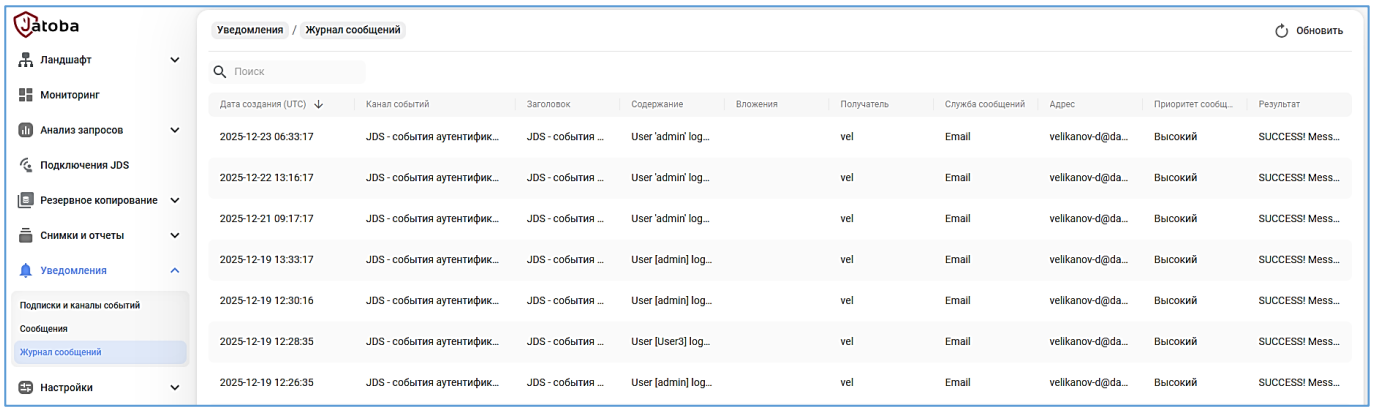

Рисунок 25.23 – Вкладка «Журнал сообщений»

26. ЖУРНАЛЫ СОБЫТИЙ JDS

Технический журнал - этот журнал предназначен для регистрации событий технического характера от момента запуска приложения и до его завершения. Также, в этот журнал записываются сообщения о технических ошибках любого уровня, которые возникают при выполнении функций приложения.

Технические журналы компонента JDS и службы jds-doctor, в текстовом формате находятся в каталоге:

— /var/log/jds для GNU Linux;

— %ProgramData%\jds для ОС семейства Windows.

Содержимое журналов доступно просматривать во внутреннем хранилище журналов «systemd» утилитой «journalctl».

Например

```
#journalctl -u jds-doctor
#journalctl -u jds
```

Файлы журналов формируются при запуске служб. Имя файла журнала имеет формат:

```
Service_name_ГГГГММДД.log
```

В конфигурационных файлах:

— /opt/jds/appsettings.json;

— /opt/jds-doctor/appsetting.json.

существует отдельный раздел «AppLogging» для управления техническим журналом.

```
  "AppLogging": {
    "Level": "Information",
    "SensitiveDataLogging": false,
    "FileCount": 90,
    "RotateInterval": "Day"
```

Этот раздел включает вложенные элементы не глубже одного уровня, которые отвечают за следующие параметры приведенные в таблице 26.1:

Таблица 26.1 – Параметры журналирования

Параметр	Описание параметра
"Level": "Information",	**«Level»** - уровень журналирования. Значение из набора (Debug, Information, Error) **DEBUG** - в журнал выводятся сообщения о начале, этапах и результатах выполнения действий, включая подробные сообщения об ошибках **INFORMATION** - в журнал выводятся сообщения о факте завершения выполнения крупных действий, а также краткие сообщения об ошибках **ERROR** - в журнал выводятся только сообщения об ошибках в процессе работы, с кратким текстом ошибки.
"SensitiveDataLogging":	**«SensitiveDataLogging»** - признак «Включать данные БД для отладки». Значение по умолчанию - «False».
"FileCount": 90,	**«FileCount»** - количество копий журнала. Значение по умолчанию - «90» (целое число).
"RotateInterval": "Day"	«RotateInterval» - периодичность создания нового журнала (периодичность ротации). Значение по умолчанию - «Day». Используются значения из набора hour, day, month.

Параметры журналирования в конфигурационных файлах /opt/jds/appsettings.json компонента JDS и /opt/jds-doctor/appsetting.json службы jds-doctor идентичны и применяются после перезагрузки одноименных служб.

27. СООБЩЕНИЯ ОБ ОШИБКАХ

27.1. Ошибка при проверке подключения к цели: 28P01

Ошибка при проверке подключения к цели:28P01 возникает в случае если указаны неверные аутентификационные параметры ассоциированного пользователя СУБД.

```
Error while checking target connection:28P01: password
authentication failed user [user_name]
```

Для устранения ошибки необходимо проверить аутентификационную информацию.

27.2. Ошибка при проверке подключения к цели

Ошибка при проверке подключения к цели, возникает в случае указания неверного IP-адреса, порта и т.д.

Сообщение переводится как: «Ошибка при проверке подключения к цели: Подключение пока исключено».

```
Error while checking target connection:Exception while
connection
```

Для устранения ошибки необходимо проверить данные для подключения.

27.3. Ошибка настройке конфигурационного файла: 28000

Ошибка возникает при некорректном формировании конфигурационного файла «pg_hba.conf».

```
Error while checking target connection:28000: no pg_hba.conf
entry for host [IP], user [user_name], database [db_name],SSL
off
```

Для устранения ошибки в конфигурационном файле «pg_hba.conf» необходимо внести строку разрешающую подключение к служебной СУБД, которую использует компонент JDS.

27.4. Ошибка при получении списка записей журнала ldapsync

Ошибка возникает если пользователь JDS, имеющий доступ к разделу «LDAP-синхронизация», выбрал целевую СУБД, на которой не установлено расширение «ja_sync_ldap».

```
Ошибка при получении списка записей журнала ldapsync: 3F000:
schema "ja_sync_ldap" does not exist POSITION: 15
```

27.5. Ошибка при получении списка профилей ldapsync

Ошибка возникает если у ассоциированного пользователя СУБД отсутствуют права на схему «ja_sync_ldap» и принадлежащие ей таблицы.

```
Ошибка при получении списка профилей ldapsync: 42501:
permission denied for table profile
```

Исправить ошибку возможно предоставлением прав ассоциированному пользователю СУБД на схему «ja_sync_ldap» и принадлежащие ей таблицы.

27.6. Ошибка при создании профиля ldapsync

Ошибка при создании профиля ldapsync возникает при отсутствии у пользователя СУБД прав на схему «ja_sync_ldap».

```
Ошибка при создании профиля ldapsync: Невозможно создать
профиль ldapsync для цели с Id = b14ac7ac-ff12-476f-afe6-
a4beef4ba802!
```

27.7. Ошибка при создании/обновления маппинга ldapsync

Ошибка возникает при попытке создания маппинга с указанием не уникальной групповой роли БД или имени группы в Microsoft Active Directory.

Компонент выведет следующие сообщения:

```
Ошибка при обновлении маппинга профиля ldapsync. Маппинг с
параметрами "Роль БД" = "значение_параметра" и/или "Группа AD"
= "значение_параметра" уже существует!

Ошибка при создании маппинга профиля ldapsync. Маппинг с
параметрами "Роль БД" = "значение_параметра" и/или "Группа AD"
= "значение_параметра" уже существует!
```

Для устранения ошибки требуется указать уникальные параметры, не используемые в других маппингах.

27.8. Ошибка при создании одноименного профиля ldapsync

Ошибка возникает при попытке указания неуникального имени профиля синхронизации.

Компонент выведет следующие сообщения:

```
Ошибка при создании профиля ldapsync: Профиль с именем
"Profile" уже существует!

Ошибка при обновлении профиля ldapsync: Профиль с именем
"Profile" уже существует!
```

Для устранения ошибки требуется указать уникальное имя профиля синхронизации.

27.9. Ошибка выполнения синхронизации

Ошибка о невозможности синхронизации профиля возникает в случае некорректно указанных параметров.

```
Невозможно выполнить синхронизацию профиля "profile_name" с id
= "profile_id"
```

Для устранения ошибки потребуется:

— провести анализ событий безопасности;

— перепроверить параметры профиля синхронизации;

— перепроверить параметры маппинга;

— сохранить внесенные изменения;

— выполнить повторную синхронизацию.

27.10. Сообщение «Синхронизация частично выполнена»

Сообщение «Синхронизация частично выполнена» возникает в случае, когда одна или несколько синхронизируемых учетных записей не соответствуют требованиям и были исключены из синхронизации.

Для полной синхронизации потребуется:

— провести анализ событий безопасности;

— исправить ошибку на источнике проблемы;

— выполнить повторную синхронизацию.

27.11. Ошибка при добавлении в кластер Master узла

В случае установки компонента JDS на один из узлов кластера может возникать ошибка добавления в кластер Master узла.

Компонент выведет одно из сообщений:

```
Ошибка при подключении списка узлов кластера: 57P01:
terminating connection due to administrator

Ошибка при подключении списка узлов кластера: An exception has
been raised that is likely due to transient
```

Для устранения ошибки необходимо внести изменения в строку:

```
"DefaultConnection": "User Id=jds; Password=P@assword;
Server=localhost; Database=jdsdb; Port=5432"
```

конфигурационного файла Appsettings.json компонента JDS значение:

```
Pooling=false;
```

После чего строка будет иметь следующий вид:

```
"DefaultConnection": "User Id=jds; Password=P@assword;
Server=localhost; Database=jdsdb; Port=5432; Pooling=false;"
```

Сохранить изменения в файле и выполнить перезагрузку службы веб-сервера.

Также ошибка может возникать и при выполнении функции «switchover».

27.12. Ошибка при создании канала событий

Ошибка создания канала событий возникает при идентичных параметрах с ранее созданным каналом событий.

Компонент выведет следующее сообщение:

```
Ошибка при создании канала событий: An error occurred while
saving the entity changes. See the inner exception for details.
```

Для устранения ошибки требуется изменить параметры канала событий.

27.13. Дублирование сообщений при рассылке уведомлений

Ошибка возникает при некорректной настройке клиента синхронизации времени.

Ошибка устраняется на уровне ОС командами:

```
sudo apt purge ntp
sudo apt purge chrony
sudo timedatectl set-ntp true
sudo systemctl start systemd-timesyncd
```

27.14. Резервное копирование

При ошибке создания резервной копии требуется выполнить следующие действия:

— удалить СУБД из раздела «Ландшафт»;

— повторно подключить СУБД в раздел «Ландшафт»;

— удалить в postgresql.conf последние команды архивации

— проверить права на директория бэкапа от ROOT для учетки postgres

— Удалить архивные копии из директории

— Удалить прежнее хранилище

— Настроить бэкап

— Создать хранилище

— Перед полной архивацией перезагрузка

— Выполнить FULL ARH

ПРИЛОЖЕНИЕ 1

Перечень «Классов событий» используемых в подразделе «Подписки»

Таблица П.1.1 – Перечень «Классов событий»

sql_state_code	Наименование
Class 00 — Successful Completion	
00000	successful_completion
Class 01 — Warning	
01000	warning
0100C	dynamic_result_sets_returned
01008	implicit_zero_bit_padding
01003	null_value_eliminated_in_set_function
01007	privilege_not_granted
01006	privilege_not_revoked
01004	string_data_right_truncation
01P01	deprecated_feature
Class 02 — No Data (this is also a warning class per the SQL standard)	
02000	no_data
02001	no_additional_dynamic_result_sets_returned
Class 03 — SQL Statement Not Yet Complete	
03000	sql_statement_not_yet_complete
Class 08 — Connection Exception	
08000	connection_exception
08003	connection_does_not_exist
08006	connection_failure
08001	sqlclient_unable_to_establish_sqlconnection
08004	sqlserver_rejected_establishment_of_sqlconnection
08007	transaction_resolution_unknown
08P01	protocol_violation
Class 09 — Triggered Action Exception	
09000	triggered_action_exception
Class 0A — Feature Not Supported	
0A000	feature_not_supported
Class 0B — Invalid Transaction Initiation	
0B000	invalid_transaction_initiation
Class 0F — Locator Exception	

sql_state_code	Наименование
0F000	locator_exception
0F001	invalid_locator_specification
Class 0L — Invalid Grantor	
0L000	invalid_grantor
0LP01	invalid_grant_operation
Class 0P — Invalid Role Specification	
0P000	invalid_role_specification
Class 0Z — Diagnostics Exception	
0Z000	diagnostics_exception
0Z002	stacked_diagnostics_accessed_without_active_handler
Class 20 — Case Not Found	
20000	case_not_found
Class 21 — Cardinality Violation	
21000	cardinality_violation
Class 22 — Data Exception	
22000	data_exception
2202E	array_subscript_error
22021	character_not_in_repertoire
22008	datetime_field_overflow
22012	division_by_zero
22005	error_in_assignment
2200B	escape_character_conflict
22022	indicator_overflow
22015	interval_field_overflow
2201E	invalid_argument_for_logarithm
22014	invalid_argument_for_ntile_function
22016	invalid_argument_for_nth_value_function
2201F	invalid_argument_for_power_function
2201G	invalid_argument_for_width_bucket_function
22018	invalid_character_value_for_cast
22007	invalid_datetime_format
22019	invalid_escape_character
2200D	invalid_escape_octet
22025	invalid_escape_sequence
22P06	nonstandard_use_of_escape_character

sql_state_code	Наименование
22010	invalid_indicator_parameter_value
22023	invalid_parameter_value
22013	invalid_preceding_or_following_size
2201B	invalid_regular_expression
2201W	invalid_row_count_in_limit_clause
2201X	invalid_row_count_in_result_offset_clause
2202H	invalid_tablesample_argument
2202G	invalid_tablesample_repeat
22009	invalid_time_zone_displacement_value
2200C	invalid_use_of_escape_character
2200G	most_specific_type_mismatch
22004	null_value_not_allowed
22002	null_value_no_indicator_parameter
22003	numeric_value_out_of_range
2200H	sequence_generator_limit_exceeded
22026	string_data_length_mismatch
22001	string_data_right_truncation
22011	substring_error
22027	trim_error
22024	unterminated_c_string
2200F	zero_length_character_string
22P01	floating_point_exception
22P02	invalid_text_representation
22P03	invalid_binary_representation
22P04	bad_copy_file_format
22P05	untranslatable_character
2200L	not_an_xml_document
2200M	invalid_xml_document
2200N	invalid_xml_content
2200S	invalid_xml_comment
2200T	invalid_xml_processing_instruction
22030	duplicate_json_object_key_value
22031	invalid_argument_for_sql_json_datetime_function
22032	invalid_json_text
22033	invalid_sql_json_subscript

sql_state_code	Наименование
22034	more_than_one_sql_json_item
22035	no_sql_json_item
22036	non_numeric_sql_json_item
22037	non_unique_keys_in_a_json_object
22038	singleton_sql_json_item_required
22039	sql_json_array_not_found
2203A	sql_json_member_not_found
2203B	sql_json_number_not_found
2203C	sql_json_object_not_found
2203D	too_many_json_array_elements
2203E	too_many_json_object_members
2203F	sql_json_scalar_required
2203G	sql_json_item_cannot_be_cast_to_target_type
Class 23 — Integrity Constraint Violation	
23000	integrity_constraint_violation
23001	restrict_violation
23502	not_null_violation
23503	foreign_key_violation
23505	unique_violation
23514	check_violation
23P01	exclusion_violation
Class 24 — Invalid Cursor State	
24000	invalid_cursor_state
Class 25 — Invalid Transaction State	
25000	invalid_transaction_state
25001	active_sql_transaction
25002	branch_transaction_already_active
25008	held_cursor_requires_same_isolation_level
25003	inappropriate_access_mode_for_branch_transaction
25004	inappropriate_isolation_level_for_branch_transaction
25005	no_active_sql_transaction_for_branch_transaction
25006	read_only_sql_transaction
25007	schema_and_data_statement_mixing_not_supported
25P01	no_active_sql_transaction
25P02	in_failed_sql_transaction

sql_state_code	Наименование
25P03	idle_in_transaction_session_timeout
Class 26 — Invalid SQL Statement Name	
26000	invalid_sql_statement_name
Class 27 — Triggered Data Change Violation	
27000	triggered_data_change_violation
Class 28 — Invalid Authorization Specification	
28000	invalid_authorization_specification
28P01	invalid_password
Class 2B — Dependent Privilege Descriptors Still Exist	
2B000	dependent_privilege_descriptors_still_exist
2BP01	dependent_objects_still_exist
Class 2D — Invalid Transaction Termination	
2D000	invalid_transaction_termination
Class 2F — SQL Routine Exception	
2F000	sql_routine_exception
2F005	function_executed_no_return_statement
2F002	modifying_sql_data_not_permitted
2F003	prohibited_sql_statement_attempted
2F004	reading_sql_data_not_permitted
Class 34 — Invalid Cursor Name	
34000	invalid_cursor_name
Class 38 — External Routine Exception	
38000	external_routine_exception
38001	containing_sql_not_permitted
38002	modifying_sql_data_not_permitted
38003	prohibited_sql_statement_attempted
38004	reading_sql_data_not_permitted
Class 39 — External Routine Invocation Exception	
39000	external_routine_invocation_exception
39001	invalid_sqlstate_returned
39004	null_value_not_allowed
39P01	trigger_protocol_violated
39P02	srf_protocol_violated
39P03	event_trigger_protocol_violated
Class 3B — Savepoint Exception	

sql_state_code	Наименование
3B000	savepoint_exception
3B001	invalid_savepoint_specification
Class 3D — Invalid Catalog Name	
3D000	invalid_catalog_name
Class 3F — Invalid Schema Name	
3F000	invalid_schema_name
Class 40 — Transaction Rollback	
40000	transaction_rollback
40002	transaction_integrity_constraint_violation
40001	serialization_failure
40003	statement_completion_unknown
40P01	deadlock_detected
Class 42 — Syntax Error or Access Rule Violation	
42000	syntax_error_or_access_rule_violation
42601	syntax_error
42501	insufficient_privilege
42846	cannot_coerce
42803	grouping_error
42P20	windowing_error
42P19	invalid_recursion
42830	invalid_foreign_key
42602	invalid_name
42622	name_too_long
42939	reserved_name
42804	datatype_mismatch
42P18	indeterminate_datatype
42P21	collation_mismatch
42P22	indeterminate_collation
42809	wrong_object_type
428C9	generated_always
42703	undefined_column
42883	undefined_function
42P01	undefined_table
42P02	undefined_parameter
42704	undefined_object

sql_state_code	Наименование
42701	duplicate_column
42P03	duplicate_cursor
42P04	duplicate_database
42723	duplicate_function
42P05	duplicate_prepared_statement
42P06	duplicate_schema
42P07	duplicate_table
42712	duplicate_alias
42710	duplicate_object
42702	ambiguous_column
42725	ambiguous_function
42P08	ambiguous_parameter
42P09	ambiguous_alias
42P10	invalid_column_reference
42611	invalid_column_definition
42P11	invalid_cursor_definition
42P12	invalid_database_definition
42P13	invalid_function_definition
42P14	invalid_prepared_statement_definition
42P15	invalid_schema_definition
42P16	invalid_table_definition
42P17	invalid_object_definition
Class 44 — WITH CHECK OPTION Violation	
44000	with_check_option_violation
Class 53 — Insufficient Resources	
53000	insufficient_resources
53100	disk_full
53200	out_of_memory
53300	too_many_connections
53400	configuration_limit_exceeded
Class 54 — Program Limit Exceeded	
54000	program_limit_exceeded
54001	statement_too_complex
54011	too_many_columns
54023	too_many_arguments

sql_state_code	Наименование
Class 55 — Object Not In Prerequisite State	
55000	object_not_in_prerequisite_state
55006	object_in_use
55P02	cant_change_runtime_param
55P03	lock_not_available
55P04	unsafe_new_enum_value_usage
Class 57 — Operator Intervention	
57000	operator_intervention
57014	query_canceled
57P01	admin_shutdown
57P02	crash_shutdown
57P03	cannot_connect_now
57P04	database_dropped
57P05	idle_session_timeout
Class 58 — System Error (errors external to PostgreSQL itself)	
58000	system_error
58030	io_error
58P01	undefined_file
58P02	duplicate_file
Class 72 — Snapshot Failure	
72000	snapshot_too_old
Class F0 — Configuration File Error	
F0000	config_file_error
F0001	lock_file_exists
Class HV — Foreign Data Wrapper Error (SQL/MED)	
HV000	fdw_error
HV005	fdw_column_name_not_found
HV002	fdw_dynamic_parameter_value_needed
HV010	fdw_function_sequence_error
HV021	fdw_inconsistent_descriptor_information
HV024	fdw_invalid_attribute_value
HV007	fdw_invalid_column_name
HV008	fdw_invalid_column_number
HV004	fdw_invalid_data_type
HV006	fdw_invalid_data_type_descriptors

sql_state_code	Наименование
HV091	fdw_invalid_descriptor_field_identifier
HV00B	fdw_invalid_handle
HV00C	fdw_invalid_option_index
HV00D	fdw_invalid_option_name
HV090	fdw_invalid_string_length_or_buffer_length
HV00A	fdw_invalid_string_format
HV009	fdw_invalid_use_of_null_pointer
HV014	fdw_too_many_handles
HV001	fdw_out_of_memory
HV00P	fdw_no_schemas
HV00J	fdw_option_name_not_found
HV00K	fdw_reply_handle
HV00Q	fdw_schema_not_found
HV00R	fdw_table_not_found
HV00L	fdw_unable_to_create_execution
HV00M	fdw_unable_to_create_reply
HV00N	fdw_unable_to_establish_connection
Class P0 — PL/pgSQL Error	
P0000	plpgsql_error
P0001	raise_exception
P0002	no_data_found
P0003	too_many_rows
P0004	assert_failure
Class XX — Internal Error	
XX000	internal_error
XX001	data_corrupted
XX002	index_corrupted

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Целевая СУБД – СУБД являющаяся целью мониторинга.

При использовании компонента пользовательского веб-интерфейса для администраторов «Jatoba data safe», компонент ведет мониторинг, обслуживание и прочие действия отдельно установленных СУБД «Jatoba». Такие СУБД для компонента «Jatoba data safe» являются целевыми.

Служебная СУБД – СУБД, обслуживающая компонент «Jatoba data safe», и выполняющая служебные функции

Флажок (от англ. check box) – элемент графического пользовательского интерфейса, позволяющий пользователю управлять параметром с двумя состояниями.

Бекапирование – резервное копирование (англ. backup copy) – процесс создания копии данных на носителе (жестком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Маппинг – маппинг, маппирование (англ. mapping) – в программировании определение соответствия данных между последовательностями элементов.

Instants – производная от слова инсталляция (англ. install). В контексте документа под данным термином подразумевается установленный на отдельном физическом или виртуальном сервере экземпляр СУБД «Jatoba».

Пиктограмма – значок, элемент графического интерфейса пользователя; небольшое изображение на мониторе, служащее для идентификации некоторого объекта: файла, программы и т. п. Выбор и активизация пиктограммы вызывает действие, связанное с выбранным объектом.

Extension – расширение в СУБД - это совокупность нескольких SQL объектов (типы данных, функции, операторы), объединенных в виде скрипта, динамически загружаемая библиотека (если она необходима) и управляющий файл, в котором указывается имя скрипта, путь к библиотеке, версия по умолчанию и прочие опции.

Снапшот (англ. Snapshots) – снимок состояния объекта.

Соответствие групп (mapping) – совокупность параметров, описывающих какие учетные записи AD будут синхронизированы с учетными записями СУБД.

SMTP (Simple Mail Transfer Protocol) – протокол, используемый для передачи электронной почты.

ZULIP – веб-сервис для обмена сообщениями и организации обсуждений с использованием технологии real-time.

Первичная идентификация - действия по формированию и регистрации информации о субъекте доступа или объекте доступа, а также действия по присвоению идентификатора доступа субъекту доступа или объекту доступа и его регистрации в перечне присвоенных идентификаторов доступа. (ГОСТ Р 58833-2020, пункт 3.41)

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

API	–	Application programming interface
HTTP	–	HyperText Transfer Protocol
HTTPS	–	HyperText Transfer Protocol Secure
IIS	–	Internet Information Services
IP	–	Internet Protocol
ISO	–	International Organization for Standardization
LDAP	–	Lightweight Directory Access Protocol
SQL	–	Structured Query Language
TCP	–	Transmission Control Protocol
UDP	–	User Datagram Protocol
UID	–	User Identifier
PID	–	Process ID. Идентификатор процесса
АРМ	–	Автоматизированное рабочее место
БД	–	База данных
ИБ	–	Информационная безопасность
ОЗУ	–	Оперативное запоминающее устройство
ОС	–	Операционная система
РСБ	–	Регистрация событий безопасности
СМИБ	–	Система менеджмента информационной безопасности
СУБД	–	Система управления базами данных
УПД	–	Управление доступом
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 документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

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