

Отчёт экспресс-чека инфраструктуры Directum RX

Контур «Документооборот» · ООО «Пример» · проверка 03.09.2026 · один рабочий день · доступ на чтение · rxdoctor 0.2.1

1. Что проверяли и что нашли за день

48

Автоматических проверок
rxdoctor

8

Ручных пунктов, которых
утилита не видит

6

Красных · чинить первыми

11

Жёлтых · в план

Состав контура. Directum RX 25.2 на Linux, 4 виртуальные машины: сервер приложений, СУБД PostgreSQL 16, брокер RabbitMQ вместе с Elasticsearch, файловое хранилище NFS. Около 420 пользователей, обновление до текущей версии выполнялось 14 месяцев назад. Тестового контура нет.

Как проверяли. Утром администратор заказчика запустил rxdoctor на сервере приложений под имеющимися учётками, отчёт пришёл до созвона. Остаток дня ушёл на то, что утилита не проверяет по своей природе: развернули вчерашний бэкап на отдельной машине, посмотрели состав задания копирования, доступы и секреты, интеграции и обновления ОС.

Главный вывод. Контур работает, но не восстановим: бэкап базы делается ежедневно, восстановление ни разу не проверялось, файловое хранилище не бэкапится вовсе, архив журналов транзакций не работает 11 дней и каталог pg_wal вырос до 38 ГБ при 52 ГБ свободных. При текущей динамике диск СУБД заполнится через 2–3 недели, и база остановится. Первые два факта нашёл rxdoctor за минуту, третий вскрылся только при учебном восстановлении.

2. Что показал rxdoctor

Источник	Проверок	Состояние	Коротко
PostgreSQL	15 ·  3  4	Красный	PG-12 архив WAL падает с 23.08; PG-13 pg_wal 38 ГБ при max_wal_size 2 ГБ; PG-05 три таблицы с мёртвыми строками больше 40 %; PG-06 autovacuum по умолчанию; PG-11 реплики нет
RabbitMQ	7 ·  2	Жёлтый	MQ-06 1 900 очередей, растёт между замерами; MQ-01 временные очереди без потребителей
Полнотекстовый поиск	6 ·  1	Жёлтый	ES-01 жёлтый на одном узле данных: реплики, которым негде разместиться
Веб-клиент и TLS	5 · 	Зелёный	Сертификат до 02.2027, цепочка полная, TLS 1.0 и 1.1 отключены
Хосты	5 ·  1  2	Красный	OS-05 обновления ОС не ставились 7 месяцев, три узла ждут перезагрузки; OS-02 своп 1,2 ГБ на сервере приложений; OS-01 диск СУБД 74 %
Kubernetes	7 · 	Не проверялось	Контур на виртуальных машинах

Источник	Проверок	Состояние	Коротко
Вопросы администратору	5 ·  2  1	Красный	Q-02 из копии не восстанавливали никогда; Q-04 мониторинга нет; Q-05 тестового контура нет

Полный отчёт rxdactor с фактурой (pid блокирующих сессий, имена очередей, узлы) приложен отдельным файлом. Здесь только то, что попало в приоритеты.

3. Что проверили руками

Пункт	Состояние	Что увидели
Учебное восстановление	Красный	База развернулась за 1 ч 40 мин, но карточки открываются без содержимого: файловое хранилище NFS не входит в задание копирования
Состав и место бэкапа	Красный	Бэкап лежит на диске СУБД; отказ диска забирает и данные, и копию
Доступы и секреты	Красный	Общая учётная запись root по паролю на всех машинах; пароли СУБД в почтовой переписке
Мониторинг и алерты	Красный	Только пинг хостов; возраст бэкапа и состояние архива никто не смотрит, об отказах узнают от пользователей
Интеграции и сеть	Жёлтый	Две интеграции (1С, почта) без документации; порты открыты «все ко всем» внутри сегмента
Обновления и откат	Жёлтый	Процедуры отката обновления RX нет, тестового контура нет
Централизованные логи	Жёлтый	Ротация есть, сбора нет; разбор инцидента это ssh на четыре машины
Владелец и регламенты	Зелёный	Владелец назван, окно обслуживания согласовано, есть кому принимать решения

4. Находки с приоритетом

#	Что найдено	Откуда	Чем заканчивается	Приоритет	Трудоёмкость
1	Архив журналов транзакций не работает с 23.08: путь архива недоступен после переноса NFS	Rxdoctor PG-12	Диск СУБД заполнится через 2–3 недели, база остановится; точки восстановления нет с 23.08	P1	2 часа
2	Файловое хранилище документов не входит в схему бэкапа	Руками	После восстановления откроются карточки без содержимого	P1	1 день
3	Восстановление из бэкапа никогда не проводилось; бэкап лежит на диске СУБД	Q-02 + руками	RTO неизвестен; отказ диска забирает и данные, и бэкап	P1	2 дня
4	Мониторинга сервисов и СУБД нет, только доступность хостов	Q-04 + руками	Деградация живёт часами до первой жалобы	P1	3 дня
5	Обновления безопасности ОС не ставились 7 месяцев, три узла ждут перезагрузки	Rxdoctor OS-05	Известные уязвимости открыты; обновление «разом» рискованнее регулярного	P1	Окно 2 часа
6	Общая учётная запись root с паролем на всех машинах; пароли СУБД в почтовой переписке	Руками	После инцидента не ответить, кто что делал; утечка одного пароля открывает всё	P2	1 день
7	1 900 очередей в брокере, число растёт между замерами	Rxdoctor MQ-06	Брокер начнёт тормозить без единой большой очереди	P2	2 часа
8	Три таблицы с мёртвыми строками больше 40 %, autovacuum по умолчанию	Rxdoctor PG-05, PG-06	Рост базы и замедление выборок; со временем «тормозит» без причины	P2	4 часа
9	Нет процедуры отката обновления RX и тестового контура	Q-05 + руками	Обновление это билет в один конец, поэтому версия стареет	P3	В аудит

5. Что делать в ближайшие две недели

На этой неделе · без изменения архитектуры

- Починить архив WAL и убедиться, что повторный запуск rxdoctor показывает PG-12 зелёным. Освободить место, не отключая архивацию.
- Добавить файловое хранилище в бэкап и вынести каталог бэкапов на отдельное хранилище, вне диска СУБД.

- **Повторить учебное восстановление** уже с хранилищем, с протоколом и замером времени. Это даст фактический RTO.
- **Поставить базовый мониторинг:** хосты, СУБД, брокер, сервисы RX, доступность веб-клиента, возраст бэкапа и состояние архива. Два алерта обязательны: «бэкап старше суток» и «архив не работает дольше часа».
- **Обновления безопасности ОС** в согласованное окно, начиная с сервера приложений.

На следующей неделе

- Именные учётные записи, вход по ключам, пароли СУБД в хранилище секретов, ротация утекших.
- Политика автоудаления временных очередей брокера; проверка шаблона на живом списке очередей.
- Настройка autovacuum под нагрузку RX, разовая обработка трёх таблиц в окне обслуживания.
- rxdoctor по расписанию раз в сутки с кодом возврата: чтобы красное не вернулось незаметно.

Что можно не трогать

Реплика СУБД, Kubernetes, переезд хранилища на S3, жёлтый Elasticsearch на одном узле. Всё это полезно, но не раньше, чем появятся проверенный бэкап и мониторинг. Свop на сервере приложений при текущей нагрузке не мешает.

6. Что не проверили за день

- Производительность под нагрузкой: нет истории метрик, разбор «тормозит» требует мониторинга хотя бы неделю.
- Полную карту сетевых потоков и состав интеграций: это предмет аудита, а не экспресс-чека.
- Сайзинг под рост: ресурсы под план на три года считаем отдельно, черновик можно прикинуть калькулятором на сайте.

Следующий шаг. Аудит на две недели: документ «как есть», карта сетевых потоков, реестр рисков с оценкой, план стабилизации. Или сразу стабилизация по пунктам выше, если картина понятна.