

Рекомендации по резервному копированию и восстановлению

Оглавление

- # Общие принципы
- # Слой прикладной логики
 - # Состав объектов
 - # Рекомендации по резервному копированию и восстановлению
- # Слой хранения сессий и токенов
 - # Состав объектов
 - # Рекомендации по резервному копированию и восстановлению
- # Слой хранения данных
 - # Состав объектов
 - # Рекомендации по резервному копированию и восстановлению

Документ предназначен для специалистов служб эксплуатации и содержит рекомендации по организации резервного копирования и восстановления RooX UIDM.

Рекомендации учитывают особенности архитектуры решения и предполагают использование стандартных инструментов и подходов, применяемых в инфраструктуре компании, эксплуатирующей RooX UIDM.

Документ не навязывает выбор конкретных технологий, средств резервного копирования или организационных политик.

Общие принципы

- Для всех слоёв рекомендуется применять стандартные инструменты резервного копирования, принятые в инфраструктуре компании.
- Для обеспечения готовности к аварийному восстановлению рекомендуется:
 - контролировать успешность выполнения резервного копирования (мониторинг/оповещения);
 - периодически выполнять тестовые восстановления (DR-тренировки), чтобы проверить применимость процедур и актуальность резервных копий.

Слой прикладной логики

Состав объектов

Слой включает:

- **код приложений**
 - На виртуальных машинах: пакеты, установленные с помощью пакетного менеджера;

- Kubernetes: Helm-чарты и контейнерные образы.
- **конфигурация приложения**
 - На виртуальных машинах: пакеты, возможно — локально применённая шаблонизация конфигурации;
 - Kubernetes: Helm-чарты и values.yaml.
- **логи приложения**
 - На виртуальных машинах: В файловой системе (/var/log/), а также в системах централизованного логирования;
 - Kubernetes: в системах централизованного логирования.

В отказоустойчивых конфигурациях:

- На виртуальных машинах: разворачивается несколько идентичных экземпляров виртуальных машин;
- В Kubernetes запускается несколько экземпляров подов соответствующих сервисов.

Рекомендации по резервному копированию и восстановлению

Основной подход

Рекомендуется использовать одинаковый подход как на виртуальных машинах, так и на Kubernetes-окружениях, при котором слой приложений запускается заново в случае сбоя:

- код приложения разворачивается заново из пакетов
- конфигурация восстанавливается из внешнего инструмента конфигурационного управления
- логи направляются в централизованное хранилище

При таком подходе резервное копирование слоя приложений не требуется.

Данный подход снижает риски, связанные с восстановлением серверов в некорректном состоянии (например, с некорректными изменениями в конфигурации) или с устаревшим состоянием серверов.

Дополнительный вариант

Данный вариант может использоваться при установке решения на виртуальные машины. В рамках него предлагается выполнять регулярный бэкап образа виртуальной машины в периоды низкой нагрузки

Преимущества: простота и потенциально более быстрое восстановление.

Недостаток: в случае резервирования некорректного состояния оно также будет восстановлено.

Слой хранения сессий и токенов

Состав объектов

Слой реализован на базе IMDB Tarantool.

В отказоустойчивых конфигурациях используются несколько экземпляров Tarantool с репликацией данных между ними.

Рекомендации по резервному копированию и восстановлению

Резервное копирование сессий и токенов не требуется, поскольку:

- данные имеют небольшое время жизни, сравнимое с временем восстановления: как правило - минуты, иногда -

часы

- потеря данных не критична для функционирования сервиса: в случае потери пользователям просто потребуется выполнить повторный вход в приложения

При восстановлении основная задача — запустить работоспособный экземпляр хранилища, пусть даже и с пустой базой.

Слой хранения данных

Состав объектов

Слой реализован на базе СУБД PostgreSQL (или аналогов).

В отказоустойчивых конфигурациях применяются схемы master-standby (тип репликации определяется принятыми в компании политиками работы с БД).

RooX UIDM использует следующие БД:

- `RX_SSO` — учётные записи пользователей и рабочие данные (OTP-коды, признаки блокировок и др.)
- `RX_FEDERATION` — данные для работы механизмов федеративной аутентификации (может объединяться с `RX_SSO` в некоторых инсталляциях)
- `RX_AUDIT` — аудит действий пользователей, событий жизненного цикла и событий безопасности
- `RX_IDM` — данные подсистемы управления пользователями (пользователи, группы, роли, полномочия)
- `RX_SCHEDULER` — оперативные данные задач, выполняемых по расписанию

Сохранность и консистентность этих данных является критичной для работы RooX UIDM.

Рекомендации по резервному копированию и восстановлению

Резервное копирование

Рекомендуется:

- Использовать стандартные механизмы резервного копирования PostgreSQL (`pg_dump`, физические бэкапы, репликация + архивирование WAL и др.),
- Частоту резервного копирования необходимо определять в соответствии с целевым показателем RPO (Recovery Point Objective, Целевая точка восстановления) компании.

Восстановление

Общая последовательность:

1. Восстановить данные всех схем, кроме `RX_AUDIT`. Данные аудита могут быть объёмными и их восстановление не критично для немедленной работы сервиса.
2. Запустить сервисы RooX UIDM и, тем самым, восстановить доступность системы и предоставление сервиса пользователям.
3. Продолжить восстановление данных схемы `RX_AUDIT` в фоновом режиме.

Управление данными аудита

Таблица `RX_AUDIT.OperationAudit` содержит накапливаемые данные. Чтобы исключить неограниченный рост таблицы, применяется следующий механизм:

- Таблица партиционируется по дням
- Необходимо настроить ежедневную задачу, которая:
 - выполняет экспорт самых старых партиций из БД и их перенос в "холодное" хранилище. Рекомендуется использовать высокопроизводительные форматы экспорта из-за возможно больших размеров партиций
 - удаляет сохраненные партиции из БД

Сроки хранения партиций в рабочей БД и в "холодном" хранилище определяются требованиями компании по оперативному доступу к данным, а также при необходимости исходя из регуляторных требований.

