# Avelana

Руководство по обслуживанию и поддержке системы

Версия 1.0

Содержание

# Аннотация

## ВНИМАНИЕ!

**Информация, необходимая для эксплуатации программного обеспечения Avelana, включает в себя большой набор документов.**

**Основные из них:**

1) **Руководство по установке и развертыванию**
2) **Руководство по обслуживанию и поддержке Продукта (данный документ)**
3) **Инструкция пользователя и документ с описанием работы с системой**
4) **Информация о технической поддержке и ресурсах, необходимых для эксплуатации**
5) **И другией.**

**Эти документы в ознакомительной версии доступны в интернет по адресу:**

**https://avelana.ru/documentation/**

**Полный комплект документации, адаптированный к инфраструктуре Заказчика и особенностями развертывания, предоставляется в рамках исполнения контракта, а также доступен для Заказчика на портале Технической Поддержки.**

**Данная версия документа носит ознакомительный характер и не содержит чувствительной информации, касающейся инфраструктуры клиента и ее особенностей.**

**При необходимости получения консультации по данному комплекту документов, если он не был вам предоставлен, вы всегда можете оставить запрос на сайте avelana.ru, либо направив письмо на электронный адрес info@avelana.ru в свободной форме.**

---

Для предотвращения и профилактики инцидентов при работе с системой, а также диагностики ее состояния и оперативной реакции на проблемы рекомендуется использование систем мониторинга.

В случае отсутствия у Заказчика корпоративной системы мониторинга рекомендуется использовать свободно распространяемое решение Zabbix, которое отвечает всем требованиям по обеспечению мониторинга Системы и своевременного оповещения о проблемах. Рекомендации по настройке Zabbix описаны в разделе Рекомендации по настройке системы мониторинга Zabbix.

В случае наличия у Заказчика действующей системы мониторинга либо в случае если она отличается от Zabbix, в разделе Мониторинг описаны ключевые объекты системы и программного окружения, для которых необходимо обеспечить мониторинг и своевременное оповещение ответственных за администрирование и поддержку ИТ-специалистов.

Помимо мониторинга необходимо обеспечить выполнение плана обслуживания узлов системы (раздел Обслуживание узлов системы).

В разделе Проблемы и их решение описаны основные проблемы, которые могут возникнуть в процессе работы с системой, и приведено описание способов их решения.

В разделе Порядок остановки и запуска серверов/сервисов при проведении технических работ описан порядок остановки и запуска серверов/сервисов при проведении технических работ.

Порядок действий в случае аварийных ситуаций с указанием предопределяющих факторов приведен в разделе Отработка аварийных ситуаций.

# История изменений

**Версия документа**: 1.0

**Версия продукта**: 2.0.x

**Дата изменения документа**: 30.07.2024

---

# Список терминов и сокращений

В технической документации к Продукту используются следующие термины и сокращения:

| Термин | Определение/расшифровка |
|---|---|
| **ТЗ** | Техническое задание |
| **АРМ** | Автоматизированное рабочее место |
| **КЧЧ** | Виджет клиентской части чата |
| **ПУР** | предварительные условия развёртывания |
| **Управляющий сервер** | ваш сервер, с установленным absible, с которого происходит настройка управляемых серверов |
| **Управляемые сервера** | сервера заказчика, где будут расположены компоненты продукта, согласно предварительным условиям развертывания и сайзингу |
| **Плейбук (файл сценариев)** | — это файл, в котором описываются действия, которые нужно выполнить для достижения поставленной цели (в нашем случае - подготовить сервера для установки Продукта) |
| **Плей** | набор тасок, выполняемых на какой-то группе серверов, направленных на какую-то единую цель (например, установить и настроить postgerqsl server) |
| **Таск** | отдельное действие плея (например, добавить PostgreSQL репозиторий в ОС) |
| **Система** | Система AVELANA |
| **Продукт** | Система AVELANA |

| Термин | Определение/расшифровка |
|---|---|
| **ASR** | (Automatic Speech Recognition) – автоматическое распознавание речи |
| **AWP** | Automated WorkPlace – автоматизированное рабочее место |
| **CRPM** | платформенный CRM-модуль |
| **KPI** | (Key Performance Indicators) – числовые показатели деятельности, которые помогают измерить степень достижения целей или оптимальности процесса |
| **HT** | (Handle Time) – время обработки обращения – общее время, когда обращение находилось в работе оператора |
| **ID** | идентификатор |
| **GUI/UI** | Graphical User Interface – графический интерфейс пользователя |
| **Режим HA** | Режим высокой доступности High Availability |
| **Логи (log, logs)** | Файл регистрации – файл с записями о событиях в хронологическом порядке, простейшее средство обеспечения журналирования |
| **ОС** | Операционная система |
| **Web-службы** | Идентифицируемая уникальным веб-адресом (URL-адресом) программная система со стандартизированными интерфейсами |

| Термин | Определение/расшифровка |
|---|---|
| **Worker-службы** | Приложение, автоматически (если настроено) исполняемое системой при запуске операционной системы |
| **ПО** | Программное обеспечение |
| **MS** | Сокращённое наименование компании Microsoft |
| **MSDTC** | Координатор распределённых транзакций |
| **WCF** | (Windows Communication Foundation) – программный фреймворк, используемый для обмена данными между приложениями, входящий в состав .NET Framework |
| **WFM** | (Workforce Management) – инструмент управления персоналом, который позволяет планировать потребность в трудовых ресурсах, а также загрузку и рабочее расписание сотрудников с учетом различных параметров |
| **HTML** | (HyperText Markup Language) – стандартизированный язык разметки документов в Интернете |
| **XML** | (eXtensible Markup Language) – расширяемый язык разметки |
| **SSH** | (Secure Shell) – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов) |
| **CPU** | (Central Processing Unit – процессор) – электронный блок либо интегральная |

| Термин | Определение/расшифровка |
|---|---|
| | схема, исполняющая машинные инструкции (код программ), главная часть аппаратного обеспечения компьютера или программируемого логического контроллера |
| **RAM** | (Random Access Memory) – один из видов памяти компьютера, позволяющий единовременно получить доступ к любой ячейке (всегда за одно и то же время, вне зависимости от расположения) по её адресу на чтение или запись |
| **HDD** | (Hard Disk Drive) жёсткий диск, винчестер – запоминающее устройство (устройство хранения информации, накопитель) произвольного доступа, основанное на принципе магнитной записи |
| **ПК** | Персональный компьютер |
| **ПКМ** | Правая кнопка мыши |
| **VM** | Virtual machine – виртуальная машина |
| **УЗ** | Учетная запись |
| **УД** | Учетные данные |
| **AD** | (Active Directory – «активный каталог») – службы каталогов корпорации Microsoft для операционных систем семейства Windows Server |
| **DMZ** | (Demilitarized Zone – демилитаризованная зона, ДМЗ) – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных |

| Термин | Определение/расшифровка |
|---|---|
| **DNS** | (Domain Name System «система доменных имён») – компьютерная распределённая система для получения информации о доменах |
| **SPN** | (Service Principal Name) – уникальный идентификатор экземпляра сервиса. |
| **HTTP** | (HyperText Transfer Protocol – «протокол передачи гипертекста») – протокол прикладного уровня передачи данных, изначально – в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных |
| **HTTPS** | (HyperText Transfer Protocol Secure) – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности |
| **IP** | (Internet Protocol Address «адрес Интернет-протокола») – уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP |
| **API** | (Application Programming Interface – программный интерфейс приложения) – описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой |
| **NTP** | (Network Time Protocol – протокол сетевого времени) – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью |

| Термин | Определение/расшифровка |
|---|---|
| **UTC** | (Coordinated Universal Time) – всемирное координатное время |
| **TCP** | (Transmission Control Protocol) – протокол, использующийся для обеспечения надёжной доставки данных на транспортном уровне |
| **Редирект** | Перенаправление пользователя с одной страницы на другую (с одного URL на другой) |
| **СУБД** | Система управления базами данных |
| **БД** | База данных |
| **SQL** | Structured Query Language («язык структурированных запросов») – декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных |
| **ESL** | (Event Socket Library – библиотека сокетов событий) – библиотека, предназначенная для взаимодействия с FreeSWITCH в различных языках программирования |
| **ACL** | Access Control List – список правил, запрещающих или разрешающих использование ресурсов сети |
| **PBX** | Private Branch Exchange – автоматическая телефонная станция, предназначенная для использования внутри организации |
| **АТС** | Автоматическая телефонная станция, предназначенная для использования внутри организации |

# Мониторинг

## Объекты мониторинга

### Мониторинг операционной системы

Под мониторингом состояния ОС подразумевается отслеживание общего состояния операционной системы серверов / виртуальных машин, на которых развернута система. Во многих системах мониторинга по умолчанию поставляются шаблоны для отслеживания основных параметров ОС.

В случае использования Zabbix, в качестве системы мониторинга, рекомендуется использовать стандартный шаблон **Template OS Linux by Zabbix agent**. Данные шаблоны поставляются в базовой установке Zabbix и не требуют отдельной установки и конфигурирования.

В случае использования иной системы мониторинга необходимо обеспечить мониторинг следующих параметров:

- **ICMP ping** с уведомлением об отсутствии ответа на ping более 2 минут (для проверки сетевой доступности хоста);
- **CPU utilization** с уведомлением о превышении порогов в 80 %, 90 % и 95 % более чем 5 минут;
- **CPU queue length** с уведомлением наличии необрабатываемых очередей более 5 минут;
- **CPU interrupt** с уведомлением о прерываниях в течение 5 минут;
- **RAM utilization** с уведомлением о превышении порогов в 80 %, 90 % и 95 % более чем 5 минут;
- **Free swap space** с уведомлением о превышении порогов в 80 %, 90 % и 95 % более чем 5 минут;
- Состояние файловой системы. **Свободное дисковое пространство** с уведомлением о превышении порогов в 80 %, 90 % и 95 %;

- Состояние файловой системы. **Очереди записи** с уведомлением о растущих очередях более чем 5 минут;
- Состояние файловой системы. **Операции I/O**; [1]
- **Состояние служб ОС** с уведомлением в случае, если служба не активна. Поддерживается по умолчанию большинством систем мониторинга;
- **Journalctl** с уведомлением о наличии ошибок в журналах системы.

### Мониторинг состояния Worker-служб (сервера приложений локального контура)

Необходимо обеспечить мониторинг следующих параметров:

- Состояние служб **Продукта** с уведомлением в случае, если служба не запущена[2] дольше чем 10 минут после uptime хоста и в течение 5 минут, если работа хоста не прерывалась.

Полный список Worker-служб, мониторинг которых необходимо обеспечить, доступен в разделе «Сервисы системы».

### Мониторинг состояния Web-служб (сервера приложений локального контура)

Необходимо обеспечить мониторинг следующих параметров:

[1] Пороговые значения для операций I/O рассчитываются для каждой отдельно взятой файловой системы. При расчёте учитывается тип дисков (hdd/ssd/sas), для hdd- и sas-дисков учитывается параметр скорости вращения (об/мин.), наличие и тип RAID массива. Расчёт производится на основе показателя IOPS файловой системы. Приблизительные значения iops по типам дисков приведены в таблице: https://ru.wikipedia.org/wiki/IOPS . Расчёт оптимального показателя операций I/O можно произвести при помощи калькулятора https://wintelguy.com/iops-mbs-gbday-calc.pl или https://wintelguy.com/raidperf.pl (для RAID массивов).

[2] Проверка может осуществляться штатными средствами системы или при помощи bash-команд. Например, systemctl status Svc.WorkExecution.service | grep -q running;echo $?.

- **Статус запуска Nginx**[3] и уведомление о проблеме, в случае если служба неактивна;
- **Лог-файлы Nginx** (по умолчанию /var/log/nginx) с уведомлением об ошибках;
- **Статус запуска web-служб**[4] и уведомление о проблеме, в случае если служба неактивна.

Полный список web-служб, мониторинг которых необходимо обеспечить, доступен в разделе «Сервисы системы».

### Мониторинг служб systemd Продукта и сервиса NGINX (сервер приложений DMZ-зоны)

Необходимо обеспечить мониторинг следующих параметров:

- **Статус запуска Nginx**[5] и уведомление о проблеме, в случае если служба неактивна;
- **Лог-файлы Nginx** (по умолчанию /var/log/nginx) с уведомлением об ошибках;
- **Статус доступности Nginx** «из вне»;[6]
- **Статус запуска служб Продукта**[7] и уведомление о проблеме, в случае если служба неактивна.

Полный список system-служб, мониторинг которых необходимо обеспечить, доступен в разделе «Сервисы системы».

---

[3] Проверка может осуществляться штатными средствами системы мониторинга или при помощи bash-команды systemctl status nginx.service | grep -q running;echo $?.

[4] Проверка может осуществляться штатными средствами системы мониторинга или при помощи bash-команды systemctl status Web.CN.Managing.service | grep -q running;echo $?.

[5] Проверка может осуществляться штатными средствами системы мониторинга или при помощи bash-команды systemctl status nginx.service | grep -q running;echo $?.

[6] Проверка может осуществляться штатными средствами системы мониторинга или при помощи bash-команды telnet your-app-server.com 443.

[7] Проверка может осуществляться штатными средствами системы мониторинга или при помощи bash-команды systemctl status Web.CN.Managing.service | grep -q running;echo $?.

## Мониторинг лог файлов Продукта

Лог-файлы Продукта по умолчанию расположены по пути /var/log/Product/.

Лог-файлы сервисов расположены в отдельных каталогах (по имени сервиса) в корне основной директории хранения логов и имеют имена вида log.txt и Log.txt.

Необходимо обеспечить мониторинг следующих параметров:

- Наличие в лог-файлах Продукта событий типа **ERROR/ERR, FATAL/FTL** с уведомлением в случае обнаружения такого события. Для событий вида **ERROR** или **ERR** – важность «Высокая», для событий вида **FATAL** или **FTL** – важность «Критическая».

## Мониторинг шины данных (RabbitMQ, Redis)

В случае использования Zabbix в качестве системы мониторинга рекомендуется использовать готовый шаблон для RabbtiMQ. Документация и шаблон доступны по ссылке https://www.zabbix.com/integrations/rabbitmq.

Официальная документация по организации мониторинга RabbitMQ с описанием мониторинга по API в том числе доступна по адресу: https://www.rabbitmq.com/monitoring.html.

В случае использования иной системы необходимо обеспечить мониторинг следующих параметров:

- **Состояние статуса службы rabbitmq**[8] с уведомлением в случае, если служба не запущена в случае более 5 минут;
- Наличие в **логах RabbitMQ** событий типа **ERROR** с уведомлением в случае обнаружения такого события (по умолчанию расположены в /var/log/rabbitmq);
- **Healthcheck node**;[9]

[8] Проверка может осуществляться штатными средствами системы мониторинга или при помощи bash-команды systemctl status rabbitmq-server | grep -q running;echo $?.

[9] Проверка может осуществляться штатными средствами системы мониторинга и или при помощи использовать http-запроса: http://RABBITMQ.USER:RABBITMQ.PASSWORD@RABBITMQ.HOST:RABBITMQ.PORT/api/healthchecks/node.

- **Состояние доступности портов**[10] сервиса (15672, 5672 и 6379 для redis) с уведомлением в случае, если порты не доступны более 5 минут;
- **Состояние кластера** [11] (в случае использование отказоустойчивой конфигурации), с уведомлением в случае наличия ошибок;
- Уведомление в случае достижения **пороговых значения использования памяти**[12]. Пороговые значения 80 %, 90 % и 95 % от общей доступной RAM хоста;
- Уведомление в случае достижения **порогового значения использования диска**;[13]
- **Состояние статуса службы Redis**[14] с уведомлением в случае, если служба не запущена более 5 минут.

[10] Проверка может осуществляться штатными средствами системы мониторинга или при помощи утилиты telnet, например: telnet your-rmq-ip 5672.

[11] Проверка может осуществляться штатными средствами системы мониторинга и или при помощи использовать http-запроса: http://RABBITMQ.USER:RABBITMQ.PASSWORD@RABBITMQ.HOST:RABBITMQ.PORT/api/health/checks/alarms

[12] Проверка осуществляется штатными средствами системы мониторинга или при помощи bash-команды free -h.

[13] Пороговые значения для операций I/O рассчитываются для каждой отдельно взятой файловой системы. При расчёте учитывается тип дисков (hdd/ssd/sas), для hdd- и sas-дисков учитывается параметр скорости вращения (об/мин.), наличие и тип RAID массива. Расчёт производится на основе показателя IOPS файловой системы. Приблизительные значения iops по типам дисков приведены в таблице: https://ru.wikipedia.org/wiki/IOPS . Расчёт оптимального показателя операций I/O можно произвести при помощи калькулятора https://wintelguy.com/iops-mbs-gbday-calc.pl или https://wintelguy.com/raidperf.pl (для RAID массивов).

[14] Проверка осуществляется штатными средствами системы мониторинга или при помощи bash-команды systemctl status redis | grep -q running;echo $?.

## Мониторинг СУБД

В случае использования Zabbix в качестве системы мониторинга рекомендуется использовать готовый шаблон для баз данных. Документация и шаблоны доступны по ссылке:

PostgreSQL – https://www.zabbix.com/ru/integrations/postgresql.

В случае использования иной системы необходимо обеспечить мониторинг следующих параметров:

- **Состояние служб postgresql и pgagent**[15] с уведомлением в случае, если служба не запущена в случае более 5 минут;
- **Состояние доступности порта**[16] **сервера**[17] с уведомлением в случае, если порты не доступны более 5 минут;
- **Состояние табличных пространств**;
- **Наличие и количество невалидных объектов**;
- **Наличие и количество блокировок**;
- **Наличие и количество prepared транзакций**;
- **Блоки сессий**;
- **Количество подключений** с уведомлением в случае приближения к пороговому значению, заданному конфигурацией сервера БД[18].

[15] Проверка осуществляется штатными средствами системы или при помощи bash-команд systemctl status postgresql-12 | grep -q running;echo $? и systemctl status pgagent_12 | grep -q running;echo $?.

[16] По умолчанию используется порт 5432.

[17] Проверка может осуществляться штатными средствами системы мониторинга или при помощи утилиты telnet, например, telnet your-rmq-ip 5432.

[18] Проверка может осуществляться штатными средствами системы мониторинга или путем выполнения SQL-запросов к СУБД (например, https://app.product.ru/files/monitoring/pgsql_monitoring.zip).

## Мониторинг серверов модуля аутентификации и авторизации пользователей

Необходимо обеспечить мониторинг следующих параметров состояния операционной системы:

- общее состояние операционной системы;
- утилизация ресурсов (RAM, CPU, Disk I/O);
- свободное дисковое пространство;
- свободное дисковое пространство точки монтирования для записи разговоров (сетевое хранилище).

Необходимо обеспечить мониторинг состояния службы docker.

Необходимо обеспечить мониторинг доступности сервера/кластера СУБД PostgreSQL (5432/TCP, в случае использования существующего инстанса или развёртывания в отказоустойчивой конфигурации).

Необходимо обеспечить мониторинг доступности порта 8080 (HTTP).

# Рекомендации по настройке системы мониторинга Zabbix

Обеспечения полноценного мониторинга системы можно добиться практически полностью с использованием стандартных шаблонов Zabbix.

## Мониторинг ОС узлов системы

Рекомендуется использовать следующие шаблоны

- **Template OS Linux by Zabbix agent** – для мониторинга состояния ОС;
- **Template Module ICMP Ping** – для мониторинга сетевой доступности узлов системы.

## Мониторинг СУБД

Рекомендации приведены по ссылке: https://www.zabbix.com/ru/integrations/postgresql.

## Мониторинг RabbitMQ

Рекомендации приведены по ссылке: https://www.zabbix.com/integrations/rabbitmq.

# Обслуживание узлов системы

## Общие положения

Обслуживание узлов системы подразумевает:

1. Обеспечение мониторинга состояния виртуальных машин на гипервизоре.
2. Обеспечение стандартного мониторинга операционной системы виртуальной машины.
3. Регулярное резервное копирование виртуальных машин средствами гипервизора или стороннего ПО. Рекомендуется создание полных резервных копий виртуальных машин не реже одного раза в месяц, а также перед установкой обновлений системы. Рекомендуется хранить не менее двух полных резервных копий.
4. Обеспечение регулярного создания моментальных снимков файловой системы (snapshots) виртуальных машин средствами гипервизора или стороннего ПО. Рекомендуется ежедневное создание снимков перед началом рабочего дня с глубиной хранения до семи дней.
5. Обеспечение мониторинга свободного дискового пространства виртуальных машин и своевременное удаление старых данных (лог-файлы, устаревшие записи экранов, устаревшие файлы, передаваемые между оператором-абонентом). Пример реализации удаления старых данных описан в соответствующем разделе.

   Необходимо как плановое проведение мероприятия, так и при достижении пороговых показателей. Плановое удаление данных рекомендуется выполнять не реже одного раза в две недели. Критическими (пороговыми) показателями являются отметки в 70 %, 80 % и 90 % занятого дискового пространства от общего объёма накопителя виртуальной машины или файловой шары. При достижении максимального порогового значения в 90 % – возможны проблемы с эксплуатацией отдельных узлов и сервисов системы.
6. Резервное копирование баз данных системы. Пример реализации описан в разделе «Обслуживание серверов баз данных».

Рекомендуется выполнение полного резервного копирования баз данных системы ежедневно после окончания рабочего дня. Рекомендуемая глубина хранения ежедневных резервных копий составляет семь дней.

Также в обязательном порядке необходимо полное резервное копирование баз данных системы перед установкой обновлений.

7. Обеспечение контроля срока действия сертификатов, используемых системой.
8. Разграничение прав доступа к серверам Системы. Ограничение доступа неквалифицированным сотрудникам. Обеспечение своевременного исключения доступа уволенным/отстраненным сотрудникам.
9. Обеспечение контроля сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).
10. Обеспечение мониторинга версии ПО на ПК операторов.
11. Обеспечение контроля сетевой доступности с ПК операторов до узлов системы согласно диаграмме развёртывания системы (см. Приложение 1).

## Обслуживание серверов модуля аутентификации и авторизации пользователей

Обслуживание серверов модуля аутентификации и авторизации пользователей подразумевает:

1. Обеспечение стандартного мониторинга состояния ОС (см. раздел Мониторинг).
2. Своевременную установку критических обновлений ОС и компонентов безопасности.
3. Контроль состояния службы docker.
4. Контроль состояния контейнера, в котором выполняется сервис модуля.

## Обслуживание серверов приложений локального контура

Обслуживание серверов приложений локального контура подразумевает:

1. Обеспечение стандартного мониторинга состояния ОС (см. раздел Мониторинг).

2. Своевременную установку критических обновлений ОС и компонентов безопасности.
3. Контроль состояния служб Продукта и наличия ошибок в лог-файлах (1, 2, 3).
4. Обеспечение очистки старых лог-файлов, расположенных по пути **/var/log/Product/**. Пример очистки устаревших данных описан в соответствующем разделе. Рекомендуемая частота выполнения процедуры очистки – один раз в две недели.
5. Обеспечение своевременной очистки от устаревших данных в случае использования сервера приложений как файловой службы или хранилища записей экранов (см. пример реализации).

## Обслуживание серверов приложений DMZ-зоны

Обслуживание серверов приложений DMZ-зоны подразумевает:

1. Обеспечение стандартного мониторинга состояния операционной системы (см. соответствующий раздел).
2. Своевременную установку критических обновлений ОС и компонентов безопасности.
3. Контроль состояния служб Продукта и наличия ошибок в лог-файлах (1, 2).
4. Обеспечение очистки старых лог-файлов, расположенных по пути **/var/log/Product/**. Пример очистки устаревших данных описан в соответствующем разделе. Рекомендуемая частота выполнения процедуры очистки – один раз в две недели. В случае отсутствия специализированного ПО рекомендуется использование планировщика заданий cron и sh скриптов очистки. Пример использования cron описан в пункте Пример очистки устаревших данных описан в соответствующем разделе.
5. Обеспечение очистки старых лог-файлов сервиса NGINX, расположенных по пути /var/log/nginx. Пример очистки устаревших данных описан в Пример очистки устаревших данных описан в соответствующем разделе. Рекомендуемая частота выполнения процедуры очистки – один раз в две недели. В случае отсутствия специализированного ПО – рекомендуется использование планировщика заданий cron и sh скриптов очистки. Пример использования cron описан в соответствующем разделе.

6. В случае использования сервера приложений как файловой службы или хранилища записей экранов – обеспечить своевременную очистку от устаревших данных (см. пример реализации).

## ОБСЛУЖИВАНИЕ СЕРВЕРОВ БАЗ ДАННЫХ

Обслуживание серверов баз данных подразумевает:

1. Обеспечение стандартного мониторинга состояния операционной системы (см. соответствующий раздел).
2. Своевременную установку критических обновлений ОС и компонентов безопасности.
3. Обеспечение мониторинга. В случае репликации – мониторинга всех нод.
4. Обеспечение мониторинга службы PGAgent на сервере с ролью PGPool.
5. В случае репликации – мониторинг состояния кластера и статуса репликации (большинство систем мониторинга предусматривают шаблоны для реализации).
6. Организацию резервного копирования баз данных Product, Product_stats и Product_ticketing. Рекомендация по частоте выполнения процедуры резервного копирования описана в разделе Общие положения.

   Резервное копирование можно выполнять различными способами, в том числе с использованием стороннего ПО. В случае отсутствия специализированного ПО у Заказчика, резервное копирование можно осуществлять с помощью утилиты «PG_DUMP», входящей в стандартный набор при установке сервера PostgreSQL.

   **Резервное копирование БД средствами утилиты PG_DUMP**

   Предварительно, необходимо определить место хранения резервных копий. Например, */backups*.

   Создать каталог и назначить владельцем пользователя postgres:

   ```
   mkdir /backups
   chown -R postgres:postgres /backups
   ```

   Переключиться на пользователя postgres:

   ```
   su – postgres
   ```

   Выполнить команду на создание резервных копий:

```
pg_dump --file "/backups/Product-$(date +"%Y-%m-%d-%s").backup" --verbose --format=c --blobs Product
pg_dump --file "/backups/Product-$(date +"%Y-%m-%d-%s").backup" --verbose --format=c --blobs Product_stats
pg_dump --file "/backups/Product-$(date +"%Y-%m-%d-%s").backup" --verbose --format=c --blobs Product_ticketing
```

В случае получения ошибки вида:

```
pg_dump: server version: 12.7; pg_dump version: 9.2.24
```

необходимо под пользователем root выполнить команду:

```
ln -s /usr/pgsql-12/bin/pg_dump /usr/bin/pg_dump –force
```

После переключиться на пользователя postgres и повторить попытку – резервные копии будут созданы.

В зависимости от потребностей резервные копии можно архивировать, например, с помощью Zip или Tar.

Для автоматизации процесса создания резервных копий рекомендуется использовать Cron (см. пример реализации).

## ОБСЛУЖИВАНИЕ СЕРВЕРОВ ШИНЫ ДАННЫХ

Обслуживание серверов шины данных подразумевает:

1. Обеспечение стандартного мониторинга состояния операционной системы (см. соответствующий раздел).
2. Своевременную установку критических обновлений ОС и компонентов безопасности.
3. Обеспечение мониторинга (1, 2).
4. Проверка состояния служб RabbitMQ Server и Redis.

   Сервисы, установленные на сервере шины данных (RabbitMQ, Redis), самостоятельно архивируют и удаляют устаревшие журналы событий и позволяют менять глубину хранения лог-файлов и архивов путём конфигурирования сервиса. Вследствие этого отсутствует необходимость настройки дополнительной архивации и очистки старых данных для оптимизации свободного дискового пространства.

# Обслуживание файлового хранилища

## Общие сведения

Обслуживание файлового хранилища заключается в контроле свободного места и своевременной очистке дискового пространства путём удаления старых данных.

Период хранения данных определяется Заказчиком исходя из аппаратных ресурсов, выделенных для файлового хранилища, а именно размера файловой системы.

Рекомендуется проводить аудит и удаление старых данных не реже одного раза в месяц.

Также необходимо обеспечить мониторинг свободного дискового пространства в файловом хранилище с уведомлениями о достижении пороговых значений, классифицируемых следующим образом:

- 70 % – предупреждение;
- 80 % – средняя критичность;
- 90 % – максимальная критичность.

## Удаление старых данных

В случае использования Заказчиком систем резервного копирования и архивации данных процедура удаления старых данных настраивается в зависимости от системы. В большинстве случаев это архивация «устаревших» файлов и размещение их во временном хранилище с последующим удалением.

В случае отсутствия у Заказчика подобных систем можно использовать штатные средства операционных систем.

Файловое хранилище организуется в соответствии с ПУР, следовательно, доступно как с серверов приложений локального контура, так и с серверов приложений DMZ-зоны. Это значит, что процедура очистки может быть инициирована с любого сервера приложений и будет отличаться способом реализации для конкретной операционной системы.

Для очистки от старых данных с Linux-хостов предлагается использование утилиты find.

Пример скрипта очистки:

```
find /SharedFiles/ -atime +90 | xargs rm -f
```

В данном примере:

- **/SharedFiles/** – путь к точке монтирования файлового хранилища;
- **-atime +90** – количество дней, определяющих актуальность файлов, т. е. файлы с датой создания старше 90 дней будут удалены.

Данный скрипт можно сохранить, например по пути */Support/clean_shared.sh*.

Разрешить выполнение командой:

```
chmod +x /Support/clean_shared.sh
```

Добавить в Cron (crontab -e) запись:

```
0 * * 0 /Support/clean_shared.sh
```

Данная запись в cron добавит в планировщик выполнение скрипта очистки каждое воскресенье в полночь. Время и частоту выполнения можно скорректировать.

**Важно!**

Данный скрипт является примером реализации очистки через bash&cron. Может быть модифицирован или полностью изменён в зависимости от потребностей Заказчика.

## ОБСЛУЖИВАНИЕ РАБОЧИХ МЕСТ ОПЕРАТОРОВ

Обслуживание рабочих мест операторов подразумевает:

1. Обеспечение стандартного мониторинга состояния операционной системы (см. соответствующий раздел).
2. Своевременную установку критических обновлений ОС и компонентов безопасности.
3. Обеспечение разрешения на использование камеры и микрофона в настройка операционной системы. для этого открыть Параметры → Конфиденциальность → Камера, включить параметр «Разрешить приложениям использовать камеру» (Settings → Privacy → Camera, «Allow apps to access your camera»).

Такие же настройки необходимо выполнить для микрофона, т. е.: Параметры → Конфиденциальность → Микрофон, включить параметр «Разрешить приложениям использовать микрофон» (Settings → Privacy → Microphone, «Allow apps to access your microphone»).

⚠ Данные настройки рекомендуется установить групповыми политиками:

– Конфигурация компьютера → Политики → Административные шаблоны → Компоненты Windows → Камера → Разрешить использование камер (Включено).

  *For EN Windows Server: Computer Configuration → Policies → Administrative Templates → Windows Components → Camera → Allow Use of Camera (Enable)*.

– Конфигурация компьютера → Политики → Административные шаблоны → Компоненты Windows → Конфиденциальность приложения → Разрешить приложениям для Windows доступ к камере (Включено, По умолчанию для всех приложений: разрешить принудительно).

  *For EN Windows Server: Computer Configuration → Policies → Administrative Templates → Windows Components → App Privacy → Let Windows apps access the camera (Enable, Default for all apps: User is in control)*.

– Конфигурация компьютера → Политики → Административные шаблоны → Компоненты Windows → Конфиденциальность приложения → Разрешить приложениям для Windows доступ к микрофону (Включено, По умолчанию для всех приложений: разрешить принудительно).

  *For EN Windows Server: Computer Configuration → Policies → Administrative Templates → Windows Components → App Privacy → Let*

*Windows apps access the camera (Enable, Default for all apps: User is in control)*.

4. Обеспечение контроля за установкой дополнительного ПО, описанного в ПУР, а также рекомендаций по установке дополнительного ПО при обновлении системы.
5. Обеспечение контроля свободного дискового пространства.
6. Обеспечение контроля версии ПО операторов.

# Проблемы и их решение

## Проблема выполнения .NET Core на серверах приложений

### Проявление проблемы

- Не запускаются сервисы Системы;
- Команда dotnet --info возвращает ошибку:

  A fatal error occurred, the folder [/usr/local/share/dotnet/host/fxr] does not contain any version-numbered child folders

### Причины возникновения проблемы

- Не корректное обновление пакетов .NET Core;
- Нарушение целостности PATH;
- Не корректная установка пакета;
- Отсутствие сим.линков.

### Решение проблемы

1. Убедиться в наличии установленных пакетов .NET Core выполнив команду:

   sudo find /usr/ -name fxr* |xargs ls -ldh

   Должен быть получен не пустой вывод. Например:

   drwxr-xr-x. 4 root root 34 Sep  6 11:27 /usr/lib64/dotnet/host/fxr

2. Выполнить команду:

   sudo mv /usr/lib64/dotnet{,0} ; sudo ln -s /usr/share/dotnet /usr/lib64/dotnet ; sudo rsync -va /usr/lib64/dotnet0/* /usr/lib64/dotnet/

3. Проверить выполнение команды dotnet --info.

## Проблемы регистрации обращений

Изначально необходимо определить, что обращения действительно не регистрируются в системе. Для этого можно воспользоваться любым из каналов приёма обращений и попытаться зарегистрировать обращение, например, через чат на сайте:

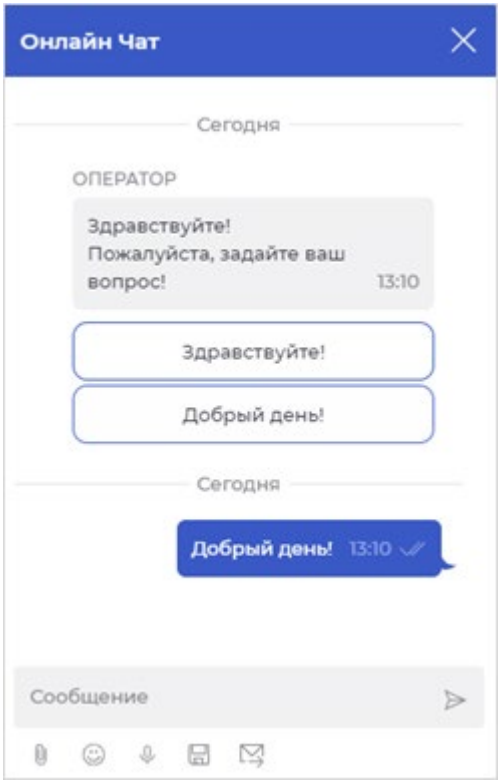


Рис. 5

Проверить, что обращение зарегистрировано в системе, можно подключившись к серверу БД с помощью PgAdmin и выполнив в БД Product запрос:

В результате будет выведен список последних 10 обращений, зарегистрированных в системе, и в данном случае обращение из примера:

Также процедуру можно выполнить из консоли. Для этого необходимо подключиться к серверу БД по SSH и выполнить следующие команды:

В выводе будет отображён список последних 10 обращений, зарегистрированных в системе, и в данном случае обращение из примера:

В примере выше обращение успешно зарегистрировано в системе. В случае, если оно не поступает в работу операторам и/или не отображается в списке открытых

обращений в приложении **АРМ супервизора**, необходимо провести диагностику, описанную в последующих разделах.

В случае, если обращение не регистрируется (не отображается в БД как зарегистрированное), необходимо:

1. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).

   1.1. Проверить состояние worker-службы **Svc.WorkExecution**.service на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

   1.2. Проверить файл журнала службы **Svc.WorkExecution.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log//Svc/WorkExecution**.

   1.3. Перезапустить службу **Svc.WorkExecution.service**.

   1.4. Проверить состояние worker-службы **Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий, а также журналы событий службы в техническую поддержку.

   1.5. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.

   1.6. Перезапустить службу **Svc.InputAdapters.service**.

   1.7. Проверить состояние web-службы **Web.CRPM.WorkCoordination**.service на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

   1.8. Перезапустить web-службу **Web.CRPM.WorkCoordination.service** на сервере приложений локального контура. Проверить journalctl на отсутствие ошибок при запуске web-службы. В случае наличия ошибок выгрузить журнал

событий за последний день и предоставить в службу технической поддержки с лог-файлами сервиса, расположенными по умолчанию по пути **/var/log/Web/CRPM.WorkCoordination**.

1.9. Проверить лог-файлы web-службы **CRPM.WorkCoordination** на сервере приложений локального контура на наличие ошибок, расположенными по умолчанию по пути **/var/log/Web/CRPM.WorkCoordination**. В случае наличия ошибок в файле журнала – предоставить логи в службу технической поддержки.

1.10. Проверить состояние web-службы **Web.CRPM.StateProcessing**.service на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

1.11. Перезапустить web-службу **Web.CRPM.StateProcessing.service** на сервере приложений локального контура. Проверить journalctl на отсутствие ошибок при запуске службы. В случае наличия ошибок – выгрузить журнал событий за последний день и предоставить в службу технической поддержки с лог-файлами сервиса, расположенными по умолчанию по пути **/var/log/Web/CRPM.StateProcessing**.

1.12. Проверить лог-файлы web-службы **CRPM.StateProcessing** на сервере приложений локального контура на наличие ошибок, расположенными по умолчанию по пути **/var/log/Web/CRPM.StateProcessing**. В случае наличия ошибок в файле журнала – предоставить логи в службу технической поддержки.

1.13. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, указанных в пунктах в предыдущих пунктах.

## ПРОБЛЕМЫ ПЕРЕДАЧИ ФАЙЛОВ

При проблемах передачи файлов от оператора клиенту или от клиента оператору, а также при проблемах открытия/сохранения файлов вне зависимости от канала приёма обращения необходимо:

1. Проверить статус службы **WEB.FileManagerService.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl status WEB.FileManagerService.service

   Служба должна находиться в статусе Active: active (running):

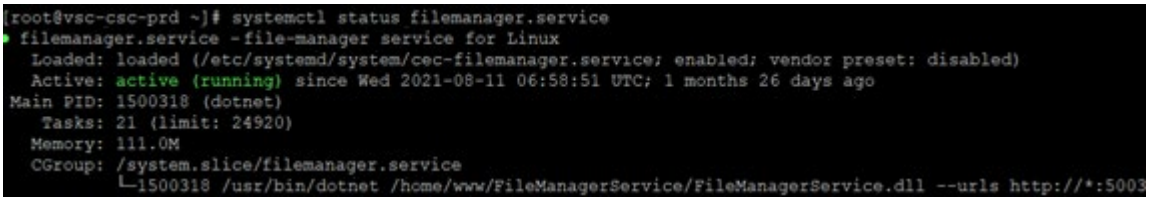


   Рис. 12

   В случае если служба остановлена – запустить ее командой:

   systemctl start WEB.FileManagerService.service

   Если служба не запускается, выполнить команды:

   systemctl stop WEB.FileManagerService.service
   cd /etc/FileManagerService/
   dotnet FileManagerService.dll --urls http://*:5003

   В результате выполнения данных команд, в консоль будет выведен лог с ошибкой запуска. Результат вывода команды передать в службу технической поддержки, а также приложить лог-файлы, расположенные по умолчанию по пути **/var/log/Product_logs/FileManagerService**.

2. Перезапустить службу **WEB.FileManagerService.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl restart WEB.FileManagerService.service

3. Проверить доступность файлового хранилища с сервера приложений DMZ-зоны и сервера приложений локального контура. Проверить права на чтение и запись в файловом хранилище с серверов приложений DMZ-зоны и локального контура.

4. Проверить сетевую доступность с сервера приложений DMZ-зоны и сервера приложений локального контура до сервера шины данных (RabbitMQ). Например, выполнив команды:

   ping ip-rmq
   telnet ip-rmq 5672

5. Проверить лог-файлы службы **WEB.FileManagerService.service** на сервере приложений DMZ-зоны, расположенные по умолчанию по пути

**/var/log/FileManagerService** на наличие ошибок. В случае наличия ошибок (события [ERR] в файле журнала) – передать лог-файлы в службу технической поддержки.

6. Проверить состояние web-службы **Web.FileManagerService.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
7. Перезапустить web-службу **Web.FileManagerService.service** на сервере приложений локального контура. Проверить journalctl на отсутствие ошибок при запуске приложения. В случае наличия ошибок – выгрузить журнал событий за последний день и предоставить в службу технической поддержки с лог-файлами сервиса, расположенного по умолчанию по пути **/var/log/Web/FileManagerService**.
8. Проверить лог-файлы web-службы **FileManagerService** на сервере приложений локального контура на наличие ошибок, расположенных по умолчанию по пути **/var/log/Web/FileManagerService**. В случае наличия ошибок в файле журнала – предоставить логи в службу технической поддержки.

## Проблемы с обращениями по различным каналам

При наличии проблем с обработкой обращений по текстовым каналам (например, отправка или получение сообщений) в зависимости от канала принимаются различные меры.

### Канал «Голос»

При проблемах с обработкой голосовых обращений, таких как обрывы звонка, ухудшение качества связи, пропадание звука у одной из сторон (абонент, оператор), необходимо:

1. Проверить сетевую доступность сервера телефонии с ПК оператора. Проанализировать трафик и возможные потери пакетов (в случае если модуль «Голосовой шлюз»[19] не используется).
2. Проверить сетевую доступность сервера модуля «Голосовой шлюз» с ПК оператора. Проанализировать трафик и возможные потери пакетов.
3. На ПК оператора при помощи Wireshark снять дамп SIP-трафика и передать в службу технической поддержки

### Канал «Чат»

При наличии проблем с отправкой/получением сообщений через канал «Чат» необходимо:

1. Проверить состояние службы **WEB.FrontMessageSender.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl status WEB.FrontMessageSender.service

   Служба должна находиться в статусе Active: active (running).

   В случае если служба остановлена – запустить ее командой:

   systemctl start WEB.FrontMessageSender.service

   Если служба не запускается, выполнить команды:

   systemctl stop WEB.FrontMessageSender.service
   cd /etc/Product/FrontMessageSender
   dotnet FrontMessageSender.dll --urls "http://*:5001"

   В результате выполнения данных команд в консоль будет выведен лог с ошибкой запуска. Результат вывода команды передать в службу технической поддержки, а также приложить лог-файлы, расположенные по умолчанию по пути **/var/log/Product_logs/FrontMessageSender**.

2. Перезапустить службу **WEB.FrontMessageSender.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl restart WEB.FrontMessageSender.service

3. Проверить состояние службы **WEB.VerificationService.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl status WEB.VerificationService.service

   Служба должна находиться в статусе Active: active (running).

   В случае если служба остановлена – запустить ее командой:

   systemctl start WEB.VerificationService.service

   Если служба не запускается, выполнить команды:

   systemctl stop WEB.VerificationService.service
   cd /etc/Product/VerificationService
   dotnet VerificationService.dll --urls "http://*:5000"

   В результате выполнения данных команд, в консоль будет выведен лог с ошибкой запуска. Результат вывода команды передать в службу технической поддержки, а также приложить лог-файлы, расположенные по умолчанию по пути **/var/log/VerificationService**.

4. Перезапустить службу **WEB.VerificationService.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl restart WEB.VerificationService.service

5. Проверить состояние worker-службы **Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

6. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.

7. Проверить состояние worker-службы **Svc.SendMessageSagaService.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

8. Проверить файл журнала службы **Svc.SendMessageSagaService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SendMessageService**.

9. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).
10. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям:
    - /var/log/VerificationService – для **службы WEB.VerificationService.service**;
    - /var/log/FrontMessageSender – для **службы WEB.FrontMessageSender.service**;
    - /var/log/Svc/InputAdapters – для **службы Svc.InputAdapters.service**;
    - /var/log/Svc/SendMessageService – для **службы Svc.SendMessageSagaService.service**.

## Канал «VKontakte»

При наличии проблем с отправкой/получением сообщений через канал «VKontakte» необходимо:

1. Проверить состояние службы **WEB.Vkontakte.CallbackService. service** на сервере приложений DMZ-зоны, выполнив команду:

   ```
   systemctl status WEB.Vkontakte.CallbackService.service
   ```

   Служба должна находиться в статусе Active: active (running).

   В случае если служба остановлена – запустить ее командой:

   ```
   systemctl start WEB.Vkontakte.CallbackService.service
   ```

   Если служба не запускается, выполнить команды:

   ```
   systemctl stop WEB.Vkontakte.CallbackService.service
   cd /etc/Product/Vkontakte.CallbackService
   dotnet Vkontakte.CallbackService.dll --urls "http://*:5010"
   ```

   В результате выполнения данных команд, в консоль будет выведен лог с ошибкой запуска. Результат вывода команды передать в службу технической поддержки, а также приложить лог-файлы, расположенные по умолчанию по пути **/var/log/Vkontakte.CallbackService**.

2. Перезапустить службу **WEB.Vkontakte.CallbackService.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl restart WEB.Vkontakte.CallbackService.service

3. Проверить состояние worker-службы *.Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

4. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.

5. Проверить состояние worker-службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

6. Проверить файл журнала службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/ApiServices**.

7. Проверить состояние worker-службы **SendMessageSagaService** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

8. Проверить файл журнала службы **Svc.SendMessageSagaService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SendMessageService**.

9. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).

10. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб, необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям:

- /var/log/Vkontakte.CallbackService – для службы WEB.Vkontakte.CallbackService.service**;
- /var/log/Svc/InputAdapters – для **службы Svc.InputAdapters.service**;
- /var/log/ApiServices – для **службы Svc.ApiServices.service**;
- /var/log/Svc/SendMessageService – для **службы SendMessageSagaService**.

## Канал «Telegram»

При наличии проблем с отправкой/получением сообщений через канал «Telegram» необходимо:

1. Проверить состояние службы WEB.Telegram.CallbackService.service на сервере приложений DMZ-зоны, выполнив команду:

   ```
   systemctl status WEB.Telegram.CallbackService.service
   ```

   Служба должна находиться в статусе Active: active (running).

   В случае если служба остановлена – запустить ее командой:

   ```
   systemctl start WEB.Telegram.CallbackService.service
   ```

   Если служба не запускается, выполнить команды:

   ```
   systemctl stop WEB.Telegram.CallbackService.service
   cd /etc/Product/Telegram.CallbackService
   dotnet Telegram.CallbackService.dll --urls "http://*:5008"
   ```

   В результате выполнения данных команд, в консоль будет выведен лог с ошибкой запуска. Результат вывода команды передать в службу технической поддержки, а также приложить лог-файлы, расположенные по умолчанию по пути **/var/log/Telegram.CallbackService**.

2. Перезапустить службу WEB.Telegram.CallbackService.service на сервере приложений DMZ-зоны, выполнив команду:

   ```
   systemctl restart WEB.Telegram.CallbackService.service
   ```

3. Проверить состояние worker-службы **Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий

journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

4. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.
5. Проверить состояние worker-службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
6. Проверить файл журнала службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/ApiServices**.
7. Проверить состояние worker-службы **SendMessageSagaService** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
8. Проверить файл журнала службы **Svc.SendMessageSagaService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SendMessageService**.
9. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).
10. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб, необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям:
    - /var/log/Telegram.CallbackService – для **службы WEB.Telegram.CallbackService.service**;
    - /var/log/Svc/InputAdapters – для **службы Svc.InputAdapters.service**;
    - /var/log/ApiServices – для **службы Svc.ApiServices.service**;
    - /var/log/Svc/SendMessageService – для **службы SendMessageSagaService**.

## Канал «Viber»

При наличии проблем с отправкой/получением сообщений через канал Viber необходимо:

1. Проверить состояние службы **WEB.Viber.CallbackService.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl status WEB.Viber.CallbackService.service

   Служба должна находиться в статусе Active: active (running).

   В случае если служба остановлена – запустить ее командой:

   systemctl start WEB.Viber.CallbackService.service

   Если служба не запускается, выполнить команды:

   systemctl stop WEB.Viber.CallbackService.service
   cd /etc/Product/Viber.CallbackService
   dotnet Viber.CallbackService.dll --urls "http://*:5009"

   В результате выполнения данных команд в консоль будет выведен лог с ошибкой запуска. Результат вывода команды передать в службу технической поддержки, а также приложить лог-файлы, расположенные по умолчанию по пути **/var/log/Viber.Callback**.

2. Перезапустить службу **WEB.Viber.CallbackService.service** на сервере приложений DMZ-зоны, выполнив команду:

   systemctl restart WEB.Viber.CallbackService.service

3. Проверить состояние worker-службы **Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

4. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.

5. Проверить состояние worker-службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl.

Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

6. Проверить файл журнала службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/ApiServices**.
7. Проверить состояние worker-службы **SendMessageSagaService** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
8. Проверить файл журнала службы **Svc.SendMessageSagaService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SendMessageService**.
9. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).
10. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям:
    - /var/log/Viber.Callback – для **службы WEB.Viber.CallbackService.service**;
    - /var/log/Svc/InputAdapters – для **службы Svc.InputAdapters.service**;
    - /var/log/ApiServices – для **службы Svc.ApiServices.service**;
    - /var/log/Svc/SendMessageService – для **службы SendMessageSagaService**.

## Канал «WhatsApp»

При наличии проблем с отправкой/получением сообщений через канал «WhatsApp» необходимо:

1. Проверить состояние службы
2. Проверить состояние worker-службы **Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе

«Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

3. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.
4. Проверить состояние worker-службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
5. Проверить файл журнала службы **Svc.ApiServices.service** на серверах приложений DMZ-зоны на наличие ошибок. По умолчанию путь хранения журналов службы /**var/log/ApiServices**.
6. Проверить состояние worker-службы **SendMessageSagaService** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
7. Проверить файл журнала службы **Svc.SendMessageSagaService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SendMessageService**.
8. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).
9. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб, необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям (в зависимости от используемого провайдера):

### Канал «SMS»

При наличии проблем с отправкой/получением сообщений через канал «SMS» необходимо:

1. Проверить состояние worker-службы **Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
2. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.
3. Проверить состояние worker-службы **Svc.SmsManagerService.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
4. Проверить файл журнала службы **Svc.SmsManagerService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SmsManagerService**.
5. Проверить состояние worker-службы **Svc.SmsConcatenationService.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
6. Проверить файл журнала службы **Svc.SmsConcatenationService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SmsConcatenationService**.
7. Проверить состояние worker-службы **SendMessageSagaService** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
8. Проверить файл журнала службы **Svc.SendMessageSagaService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/SendMessageService**.

9. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).
10. Убедиться в отсутствии проблем сетевой доступности с сервера приложений локального контура до сервера SMPP-провайдера.
11. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб, необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям:
    - /var/log/Svc/SmsConcatenationService – для **службы Svc.SmsConcatenationService.service**;
    - /var/log/Svc/SmsManagerService – для **службы Svc.SmsManagerService.service**;
    - /var/log/Svc/InputAdapters – для **службы Svc.InputAdapters.service**;
    - /var/log/Svc/SendMessageService – для **службы SendMessageSagaService**.

### Канал «Почта»

При наличии проблем с отправкой/получением сообщений через канал Почта необходимо:

1. Проверить состояние worker-службы **Svc.InputAdapters.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.
2. Проверить файл журнала службы **Svc.InputAdapters.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/InputAdapters**.
3. Проверить состояние worker-службы **Svc.OutputService.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

4. Проверить файл журнала службы **Svc.OutputService.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/OutputAdapters**.
5. Убедиться в отсутствии проблем сетевой доступности с сервера приложений локального контура до почтового сервера.
6. Убедиться в актуальности учётных данных, используемых системой для входа на почтовый сервер (например, выполнив авторизацию через web-интерфейс почтового сервера). В случае если учётные данные были изменены (например, по истечении срока действия пароля, определённого политиками организации) – обновить учётные данные в приложении Credential Manager (подробнее описано в документе **«Руководство по настройке параметров системы»**).
7. Перезапустить worker-службы **Svc.InputAdapters.service** и **Svc.OutputService.service**.
8. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания системы (см. Приложение 1).
9. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб, необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям:
   - /var/log/Svc/InputAdapters – для **службы Svc.InputAdapters.service**;
   - /var/log/Svc/OutputAdapters – для службы **Svc.OutputService.service**.

# ПРОБЛЕМА ОПРЕДЕЛЕНИЯ ПРИНАДЛЕЖНОСТИ ОБРАЩЕНИЯ НЕСКОЛЬКИМ КЛИЕНТАМ

## ОПИСАНИЕ ПРОБЛЕМЫ

Если адрес клиента в канале добавлен в профили нескольких клиентов, то в Системе обращение, поступившее с данного адреса, должно регистрироваться без привязки к клиенту.

В случае, если обращение в данной ситуации «прикрепляется» к какому-либо клиенту, данное поведение является не валидным (ошибкой).

### Решение проблемы

Необходимо проверить настройку адаптера соответствующего канала. Для этого:

1. Запустить утилиту «Редактор каналов».
2. В списке каналов выделить (1) нужный канал, открыть на редактирование настройку input-адаптера (2):

   Рис. 30
3. Проверить наличие атрибута ReflectNullAsOriginatorIdIfMoreThanOneContactForFromAddress в значении true (3).
4. В случае отсутствия необходимо добавить атрибут и нажать «Сохранить».
5. На серверах приложений локального контура выполнить команду:

   sudo systemctl restart Svc.InputAdapters.service

## Проблемы рабочего места оператора/супервизора

необходимо:

3.1. Убедиться в отсутствии проблем сетевой доступности между узлами диаграмме развёртывания системы (см. Приложение 1).

3.2. Убедиться, что запущены worker-службы Продукта и web-службы

3.3. Проверить состояние web-службы **Web.Api.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

3.4. Перезапустить web-службу **Web.Api.service** на сервере приложений локального контура.

3.5. Проверить лог-файлы web-службы **Web.Api.service** на сервере приложений локального контура на наличие ошибок, расположенных по умолчанию по пути **/var/log/Web/Api**. В случае наличия ошибок в файле журнала – предоставить логи в службу технической поддержки.

3.6. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб, необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, расположенных по путям:

- /var/log/Web/Api – для **службы Web.Api.service**;

1. **Ошибка прохождения обращения по схеме**:

Если после регистрации обращения в системе обращение не двигается по схеме («застревает» в каком-либо статусе дольше, чем ожидается) необходимо:

4.1. Убедиться в отсутствии проблем сетевой доступности между узлами диаграмме развёртывания системы (см. Приложение 1).

4.2. Проверить состояние worker-службы **Svc.WorkExecution.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

4.3. Проверить файл журнала службы **Svc.WorkExecution.service** на наличие ошибок. По умолчанию путь хранения журналов службы **/var/log/Svc/WorkExecution**.

4.4. Перезапустить службу **Svc.WorkExecution.service**.

4.5. Проверить web-службы **Web.CRPM.WorkCoordination.service** на сервере приложений локального контура. Служба должна находиться в статусе «Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

4.6. Перезапустить службу **Web.CRPM.WorkCoordination.service**.

4.7. Проверить лог-файлы службы **Web.CRPM.WorkCoordination.service** на сервере приложений локального контура на наличие ошибок, расположенные по умолчанию по пути **/var/log/Web/CRPM.WorkCoordination**. В случае наличия ошибок в файле журнала – предоставить логи в службу технической поддержки.

4.8. Проверить web-службы **Web.CRPM.StateProcessing.service** на сервере приложений локального контура. Служба должна находиться в статусе

«Running». В случае если служба остановлена – выполнить запуск. Если служба не запускается, проверить ошибку запуска в журнале событий journalctl. Предоставить выгрузку журнала событий journalctl, а также журналы событий службы в техническую поддержку.

4.9. Перезапустить службу **Web.CRPM.StateProcessing.service**.

4.10. Проверить лог-файлы службы **Web.CRPM.StateProcessing.service** на сервере приложений локального контура на наличие ошибок, расположенные по умолчанию по пути **/var/log/Web/CRPM.StateProcessing**. В случае наличия ошибок в файле журнала – предоставить логи в службу технической поддержки.

4.11. В случае отсутствия проблем сетевой доступности между узлами, а также сохранения проблем после перезапуска служб, необходимо обратиться в службу технической поддержки, предоставив лог-файлы сервисов, указанных в пунктах выше.

# Порядок остановки и запуска серверов/сервисов при проведении технических работ

При проведении технических работ на оборудовании (гипервизоры, файловые хранилища и пр.), для которого требуется остановка работы Системы, необходимо придерживаться нижеизложенного регламента.

## Порядок остановки серверов/сервисов

1. Остановить балансировщик нагрузки DMZ-зоны (в случае развёртывания в отказоустойчивой конфигурации).
2. Поочередно остановить сервера/сервер приложений DMZ-зоны.
3. Остановить балансировщик нагрузки локального контура (в случае развёртывания в отказоустойчивой конфигурации).
4. Поочередно остановить сервера/сервер приложений локального контура.
5. Поочередно остановить сервера/сервер модуля аутентификации и авторизации пользователей.
6. Поочередно или одновременно остановить сервера/сервер кластера шины данных RabbitMQ/Redis.
7. Остановить файловый сервер.
11. В случае развёртывания PostgreSQL в отказоустойчивой конфигурации:

    11.1. Остановить сервер PgPool.

    11.2. Поочередно остановить ноды СУБД PostgreSQL. Сначала Standby, потом Primary (выяснить роли серверов перед остановкой).

    В случае развёртывания PostgreSQL в не отказоустойчивой конфигурации остановить сервер СУБД PostgreSQL.

## Порядок запуска серверов/сервисов

Запуск производится в обратном остановке порядке:

1. В случае развёртывания PostgreSQL в отказоустойчивой конфигурации:

   1.1. Поочередно запустить все ноды базы данных. Сначала Primary, потом Standby.

   1.2. Запустить сервер PgPool.

   В случае развёртывания PostgreSQL в не отказоустойчивой конфигурации запустить сервер СУБД PostgreSQL.

2. Запустить файловый сервер.
3. Запустить сервера/сервер кластера шины данных RabbitMQ/Redis.
4. Запустить сервера/сервер модуля аутентификации и авторизации пользователей.
5. Запустить сервера/сервер приложений локального контура.
6. Запустить нагрузки локального контура (в случае развёртывания в отказоустойчивой конфигурации).
7. Запустить сервера/сервер приложений DMZ-зоны.
8. Запустить балансировщик нагрузки DMZ-зоны (в случае развёртывания в отказоустойчивой конфигурации).

# Отработка аварийных ситуаций

## Предопределяющие факторы

Основными факторами, сигнализирующими о приближении остановки работы Системы, являются:

- массовые проблемы запуска приложения Продукта у операторов/супервизоров;
- массовые сообщения об ошибках в приложении Продукта у операторов/супервизоров;
- значительное увеличение времени прохождения обращений по схеме до статуса «Ожидание распределения на оператора» или остановка («застревание») обращения на одном из этапов автоматической обработки;
- прекращение регистрации обращений;
- значительное увеличение времени обработки запросов к БД при обновлении online-данных или получении исторических данных (например, обновление списка операторов в АРМ - ервизора или построение отчётов);
- наличие уведомлений в системе мониторинга о достижении предельно допустимых пороговых значений утилизации ресурсов CPU, RAM, DISK I/O на ключевых узлах системы, а именно:
  - сервера приложений локального контура;
  - сервера баз данных;
  - сервера шины данных RabbitMQ/Redis.
- наличие уведомлений в системе мониторинга о достижении предельно допустимых пороговых значений утилизации ресурсов CPU, RAM, DISK I/O на хост-машине (гипервизоре);
- наличие уведомлений в системе мониторинга о стремительном росте connections (подключений) к БД;
- наличие уведомлений в системе мониторинга о большом количестве prepared transactions в БД;
- наличие уведомлений в системе мониторинга о большом количестве блокировок в БД;

- наличие уведомлений в системе мониторинга о проблемах сетевой доступности узлов Системы;
- наличие уведомлений в системе мониторинга о прекращении работы worker/web-служб Системы;
- наличие уведомлений в системе мониторинга о большом количестве ошибок в логах worker/web-служб Системы;
- наличие уведомлений в системе мониторинга о большом количестве ошибок в логах БД;
- наличие уведомлений в системе мониторинга о большом количестве ошибок в логах RabbitMQ/Redis.

## Анализ ситуации и действия при аварии

При наличии предопределяющих факторов и/или остановки работы Системы необходимо:

1. Убедиться в отсутствии проблем сетевой доступности между узлами согласно диаграмме развёртывания Системы (см. Приложение 1).
2. Убедиться в отсутствии проблем общего характера в инфраструктуре (отсутствии плановых или внеплановых работ на сетевом оборудовании, гипервизорах).
3. Проверить состояние гипервизоров, на которых работают узлы Системы. Убедиться, что отсутствуют проблемы на других VM, расположенных на данных гипервизорах.
4. Убедиться, что на гипервизорах, на которых работают узлы Системы, другие VM не оказывают критическое влияние на утилизацию общих ресурсов гипервизора, таких как CPU/RAM/файловая система.
5. Убедиться, что запущены все службы/сервисы/демоны, обеспечивающие работу Системы. В случае остановки работы служб – запустить вручную. В случае если сервис/служба/демон не запускается – собрать диагностические данные (логи сервиса и системный журнал) для дальнейшей передачи в службу технической поддержки.
6. Перезапустить все сервисы/службы/демоны Системы.
7. Проверить количество подключений к базе данных (используя данные системы мониторинга или PGAdmin). При штатной работе системы

показатели Total и Idle отличаются на значение показателя Active, т. е. практически одинаковы:

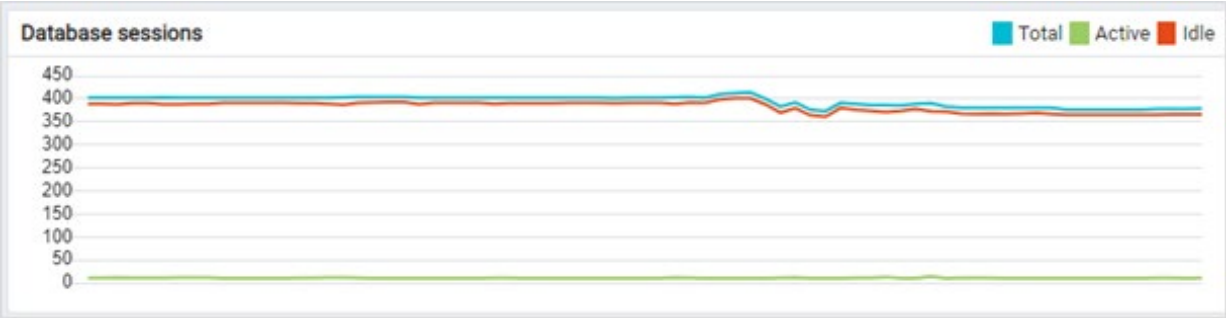


Рис. 27

Также, как правило, данные показатели в штатном режиме не превышают 600–700.

В случае расхождения показателей на графике или количестве подключений, превышающих средние значения – необходимо убедиться в отсутствии prepared transactions. Данные о наличии prepared transactions можно получить из системы мониторинга в интерфейсе PGAdmin на соответствующей вкладке Dashboard БД Product:

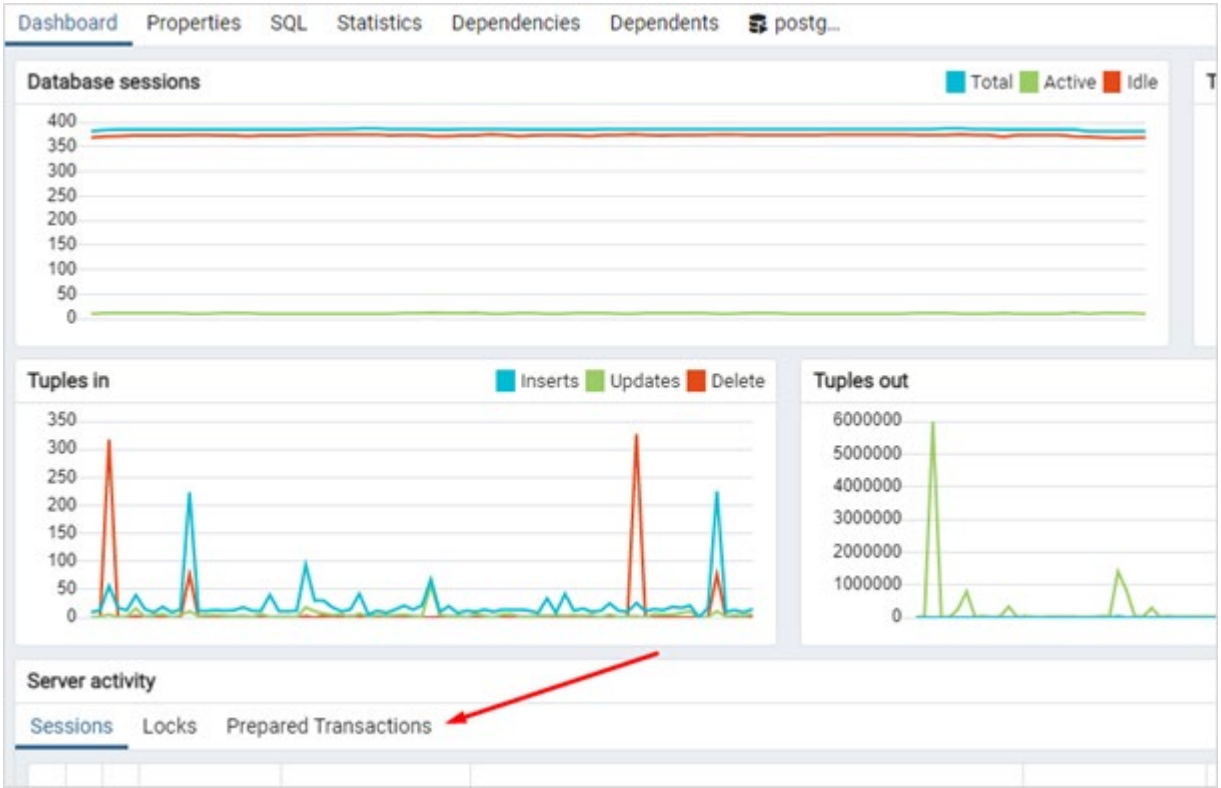


Рис. 28

или выполнив запрос:

```
select * from pg_prepared_xacts order by prepared desc;
```

После выполнения работы скрипта убедиться, что prepared transactions отсутствуют. В случае отсутствия:

- проблем сетевой доступности;
- проблем общего характера;
- корректной работы служб;
- корректной работы серверов баз данных;
- работ на инфраструктуре;
- проблем на гипервизорах;
- влияния машин, расположенных на гипервизоре,

а также после выполнения следующих рекомендаций:

- перезапуск служб/сервисов/демонов;
- проверка и очистка зависших транзакций в БД, –

если работа Системы не восстановлена – необходимо собрать диагностические данные (логи сервисов, журналы системы, графики загрузки ресурсов узлов системы) и передать их в службу технической поддержки.

# Обновление SSL сертификатов

Данный раздел описывает последовательность действий, необходимых для замены SSL-сертификатов, используемых Продуктом.

Крайне важно отслеживать срок действия сертификатов и своевременно выполнять их обновление/замену, во избежание блокировки работы Продукта, так как сертификаты используются для:

- Взаимодействия компонентов Продукта между собой;
- Взаимодействия пользователей Продукта с его сервисами/компонентами;
- Взаимодействия внешних источников (социальные сети, мессенджеры, чат-боты, интеграции и т.д.) с Продуктом.

**Важно!**

В случае развертывания в отказоустойчивой конфигурации, так же необходимо обеспечить замену сертификатов на балансировщиках нагрузки лоального и внешнего контура.

## Сервера приложений локального контура

### Определение расположения сертификатов

Перед началом процедуры замены сертификатов, необходимо определить путь их расположения на сервере/серверах роли, для этого необходимо:

1. Подключиться к серверу/серверам приложений локального контура по ssh.
2. Переключиться на пользователя root, выполнив команду:

   ```
   sudo -i
   ```

3. Выполнить команду, которая отобразит расположение файла сертификата и ключа:

   ```
   cat /opt/product/.config.sh | grep -P 'CERTPATH|KEYPATH'
   ```

   Пример вывода:

```
[root@localhost ~]$ cat /opt/product/.config.sh | grep -P 'CERTPATH|KEYPATH'
CERTPATH='./untrusted_certs/ssl.crt'
KEYPATH='./untrusted_certs/ssl.key'
```

В данном примере:

- /opt/product/untrusted_certs/ssl.crt - путь до файла сертификата;
- /opt/product/untrusted_certs/ssl.key - путь до файла ключа сертификата.

## Замена сертификатов

**Важно!**

Перед началом процедуры обновления сертификатов, настоятельно рекомендуется создать резервную копию существующих сертификатов.

1. Выполнить команду создания резервных копий существующих файлов сертификата и ключа:

   ```
   cp /cert_path/ssl.crt /cert_path/ssl.crt.bak
   cp /cert_path/key.key /cert_path/key.key
   ```

   Заменив /cert_path/ssl.crt на путь к файлу сертификата и /cert_path/key.key на путь к файлу ключа сертификата соответственно, полученные на предыдущем шаге.

   Например:

   ```
   cp /opt/product/untrusted_certs/ssl.crt /opt/product/untrusted_certs/ssl.crt.bak
   cp /opt/product/untrusted_certs/ssl.key /opt/product/untrusted_certs/ssl.key.bak
   ```

2. Скопировать на серер/сервера приложений локального контура файлы сертификата и ключа, по ранее полученным путям, с такими же именами файлов.

   **Важно!**

   Файл сертификата должен быть в формате fullchain, т.е. содержать всю цепочку сертификатов удостоверящюих/промежуточных центров сертификации.

3. Выполнить команду перезагрузки сервисов Продукта, для применения изменений:

   ```
   cd /opt/product/ && docker-compose down && docker-compose up -d
   ```

   **Важно!**

Данная команда остановит работу Продукта, перед её выполнением необходимо убедиться в отсутствии в системе работающих операторов/активных обращений.

## Сервера приложений внешнего контура (DMZ-зона)

### Определение расположения сертификатов

Перед началом процедуры замены сертификатов, необходимо определить путь их расположения на сервере/серверах роли, для этого необходимо:

1. Подключиться к серверу/серверам приложений внешнего контура по ssh.
2. Переключиться на пользователя root, выполнив команду:

   sudo -i

3. Выполнить команду, которая отобразит расположение файла сертификата и ключа:

   cat /opt/product/.config.sh | grep -P 'SERTPATH|KEYPATH'

   Пример вывода:

   ```
   [root@localhost-dev ~]$ cat /opt/product/.config.sh | grep -P 'SERTPATH|KEYPATH'
   SERTPATH=/etc/ssl/cert.crt
   KEYPATH=/etc/ssl/key.key
   ```

   В данном примере:

   – /etc/ssl/cert.crt - путь до файла сертификата;

   – /etc/ssl/key.key - путь до файла ключа сертификата.

### Замена сертификатов

**Важно!**

Перед началом процедуры обновления сертификатов, настоятельно рекомендуется создать резервную копию существующих сертификатов.

1. Выполнить команду создания резервных копий существующих файлов сертификата и ключа:

```
cp /cert_path/ssl.crt /cert_path/ssl.crt.bak
cp /cert_path/key.key /cert_path/key.key
```

Заменив /cert_path/ssl.crt на путь к файлу сертификата и /cert_path/key.key на путь к файлу ключа сертификата соответственно, полученные на предыдущем шаге.

Например:

```
cp /etc/ssl/cert.crt /etc/ssl/cert.crt.bak
cp /etc/ssl/key.key /etc/ssl/key.key.bak
```

2. Скопировать на серер/сервера приложений внешнего контура файлы сертификата и ключа, по ранее полученным путям, с такими же именами файлов.

**Важно!**

Файл сертификата должен быть в формате fullchain, т.е. содержать всю цепочку сертификатов удостоверящюих/промежуточных центров сертификации.

1. Выполнить команду перезагрузки сервисов Продукта, для применения изменений:

   ```
   cd /opt/product/ && docker-compose down && docker-compose up -d
   ```

   **Важно!**

   Данная команда остановит работу Продукта, перед её выполнением необходимо убедиться в отсутствии в системе работающих операторов/активных обращений.

## Сервера шины данных (RabbitMQ/Redis)

### Определение расположения сертификатов

Перед началом процедуры замены сертификатов, необходимо определить путь их расположения на сервере/серверах роли, для этого необходимо:

1. Подключиться к серверу/серверам шины данных по ssh.
2. Переключиться на пользователя root, выполнив команду:

   ```
   sudo -i
   ```

3. Выполнить команду, которая отобразит расположение файла сертификата и ключа:

cat /etc/nginx/conf.d/rmq.conf | grep -P 'ssl_certificate|ssl_certificate_key'

Пример вывода:

[root@localhost-rmq ~]# cat /etc/nginx/conf.d/rmq.conf | grep -P 'ssl_certificate|ssl_certificate_key'
ssl_certificate /etc/nginx/ssl/ssl.crt;
ssl_certificate_key /etc/nginx/ssl/ssl.key;

В данном примере:

- /etc/nginx/ssl/ssl.crt - путь до файла сертификата;
- /etc/nginx/ssl/ssl.key - путь до файла ключа сертификата.

## Замена сертификатов

**Важно!**

Перед началом процедуры обновления сертификатов, настоятельно рекомендуется создать резервную копию существующих сертификатов.

1. Выполнить команду создания резервных копий существующих файлов сертификата и ключа:

   cp /cert_path/ssl.crt /cert_path/ssl.crt.bak
   cp /cert_path/key.key /cert_path/key.key

   Заменив /cert_path/ssl.crt на путь к файлу сертификата и /cert_path/key.key на путь к файлу ключа сертификата соответственно, полученные на предыдущем шаге.

   Например:

   cp /etc/nginx/ssl/ssl.crt /etc/nginx/ssl/ssl.crt.bak
   cp /etc/nginx/ssl/ssl.key /etc/nginx/ssl/ssl.key.bak

2. Скопировать на серер/сервера шины данных файлы сертификата и ключа, по ранее полученным путям, с такими же именами файлов.

   **Важно!**

   Файл сертификата должен быть в формате fullchain, т.е. содержать всю цепочку сертификатов удостоверящюих/промежуточных центров сертификации.

3. Выполнить команду перезагрузки сервиса nginx (осуществляющего проксирование/ssl-терминирование для сервиса RabbitMQ), для применения изменений:

   ```
   sudo systemctl restart nginx
   ```

# Диаграмма развертывания