**Система «RBT/RFT»**

**Информация по эксплуатации ПО**

Оглавление

[1 Web GUI 4](#_Toc124162430)

[1.1 Логин и пароль на платформу: 4](#_Toc124162431)

[2 SSH доступ 4](#_Toc124162432)

[2.1 Конфигурация стенда 4](#_Toc124162433)

[3 Система «RBT/RFT» 8](#_Toc124162434)

[4 Логическая архитектура платформы 8](#_Toc124162435)

[5 Аппаратная реализация 9](#_Toc124162436)

[5.1 Схема взаимодействия компонентов платформы 10](#_Toc124162437)

[5.2 Отказоустойчивость и масштабирование 11](#_Toc124162438)

[5.2.1 Распределение ВМ по подсетям 14](#_Toc124162439)

[5.3 Телефонное соединение 14](#_Toc124162440)

[5.3.1 Используемые протоколы 16](#_Toc124162441)

[6 Интеграция с Оператором 16](#_Toc124162442)

[6.1 Интеграция с биллингом 17](#_Toc124162443)

[6.2 Создание, настройка и администрирование ВМ 17](#_Toc124162444)

[6.3 API 18](#_Toc124162445)

[6.4 Диаграмма компонентов 19](#_Toc124162446)

[6.4.1 Внутренние соединения 20](#_Toc124162447)

[6.4.2 Защищенные соединения 20](#_Toc124162448)

[6.4.3 Внешние соединения 20](#_Toc124162449)

[6.5 Стандартное ПО, устанавливаемое на ВМ 20](#_Toc124162450)

[6.6 Дополнительно устанавливаемое ПО 21](#_Toc124162451)

[6.6.1 Системные ВМ 21](#_Toc124162452)

[6.6.2 Прикладные ВМ 22](#_Toc124162453)

[6.6.3 ВМ СУБД 22](#_Toc124162454)

[7 Протоколирование событий 22](#_Toc124162455)

[8 Статистика 24](#_Toc124162456)

[9 Системы управления и отчетности 25](#_Toc124162457)

[9.1 GUI 25](#_Toc124162458)

[9.2 Ansible 26](#_Toc124162459)

[9.3 Git 27](#_Toc124162460)

[9.4 Prometheus 27](#_Toc124162461)

[9.5 Grafana 27](#_Toc124162462)

[10 Информационная безопасность 27](#_Toc124162463)

[10.1 Общие сведения 27](#_Toc124162464)

[10.1.1 Безопасность операционных систем, баз данных 27](#_Toc124162465)

[10.1.2 Конфигурирование сетевых настроек 28](#_Toc124162466)

[10.2 Идентификация и аутентификация и управление доступом 29](#_Toc124162467)

[10.2.1 Конфигурирование учетных записей ОС 29](#_Toc124162468)

[10.2.2 Конфигурирование прав доступа ОС 29](#_Toc124162469)

[10.2.3 Конфигурирование учетных записей БД 30](#_Toc124162470)

[10.2.4 Безопасность при управлении абонентами и услугами 30](#_Toc124162471)

[10.3 Безопасность при интеграции RBT/RFT-платформы в IP сети 30](#_Toc124162472)

[10.3.1 Организация сетевых доступов 30](#_Toc124162473)

[11 Система мониторинга 31](#_Toc124162474)

[11.1 Основные параметры проверочных скриптов 32](#_Toc124162475)

[11.2 Покрытие мониторинга и локализация 32](#_Toc124162476)

[11.3 Автоматический перезапуск 32](#_Toc124162477)

[12 Резервное копирование и восстановление 33](#_Toc124162478)

[12.1 Общие требования к резервному копированию 33](#_Toc124162479)

[12.2 Общие требования к восстановлению 33](#_Toc124162480)

# Web GUI

<http://rbt.demo.mdcm.co/index.html#/login>

## Логин и пароль на платформу:

Имя пользователя rr

Пароль Sea5Gaet

Дополнительные логин и пароль для авторизации (basic auth защита стенда):

Имя пользователя rr

Пароль eF0piavu

# SSH доступ

rbt.demo.mdcm.co

Имя пользователя: rr

Ключ для авторизации: передается отдельно через персональный запрос на электронную почту: sergey.butenin@mdcm.co

## Конфигурация стенда

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование** | **Описание** | **Развернут?** | **Комментарий** |
| TERMINAL | Сервер доступа к площадкам RFT/RFT-платформы в периметре Оператора | нет | В Stage окружении не требуется. |
| MGMT | Управление и мониторинг | нет | В Stage окружении не требуется |
| MAINTENANCE | Управление и мониторинг | нет | В Stage окружении не требуется |
| LOGIC | Сервис подбора контента | да | Доступ с rbt-stage-telephony:  ssh admin@172.21.24.12 |
| SRV | API платформы и обработка асинхронных задач из очередей | да | Доступ с rbt-stage-telephony:  ssh admin@172.21.24.12 |
| GUI | Интерфейс администрирования платформы | да | Доступ с rbt-stage-telephony:  ssh admin@172.21.24.12 |
| MEDIA STORAGE | Хранилище контента | да | Доступ с rbt-stage-telephony:  ssh admin@172.21.24.12 |
| QUEUE | Система очередей RabbitMQ | да | Доступ с rbt-stage-telephony:  ssh admin@172.21.24.11 |
| INTEGRATION | Интеграция с подсистемами Оператора | нет | В Stage окружении отсутствует. Для каждого оператора проводится кастомизация |
| SIP | Обработка и маршрутизация SIP-трафика | да | rbt-stage-telephony (172.21.24.14)  Статус и логи  systemctl status balancer |
| MEDIA | Обеспечение проигрывания контента | да | rbt-stage-telephony (172.21.24.14)  Статус и логи  systemctl status rbt  systemctl status stat  systemctl status medianode  systemctl status sipstats |
| SMPP | Интеграция с SMSC/USSD оператора. | нет | В Stage окружении отсутствует. Для каждого оператора проводится кастомизация |
| NGINX | Балансировщик запросов к платформе | да | rbt-stage-telephony (172.21.24.14)  Статус и логи  systemctl status nginx |
| PGPOOL | Балансировщик запросов к MAIN DB | нет | В Stage окружении не требуется |
| DB, MAIN DB | Основная база данных платформы, хранит профили абонентов, метаданные контента и другие данных для предоставления услуги | да | Доступ с rbt-stage-telephony:  ssh admin@172.21.24.11 |
| STATISTIC | Хранилище логов работы ПО платформы за длительный срок | да | Доступ с rbt-stage-telephony:  ssh admin@172.21.24.11 |

# Система «RBT/RFT»

В настоящем документе рассмотрена архитектура Системы «RFT/RFT» ООО Медиа Ком.

Документ включает в себя высокоуровневое описание, схемы, компоненты платформы, а также иные сведения, необходимые для ознакомления. Платформа выполнена в виде HA/DR-решения (работоспособность и отказоустойчивость в условиях постоянных изменений). Изменение параметров работы Решения происходит без остановки настраиваемых подсистем.

Является совокупностью программных средств, способных работать в любой из известных сред виртуализации, поддерживающих архитектуру x86/x64.

# Логическая архитектура платформы



В состав RFT/RFT-платформы входят следующие компоненты:

1. Пользовательские интерфейсы, обеспечивающие взаимодействие RFT/RFT-платформы с конечным абонентом: IVR, SMS, USSD.
2. Сервисная платформа, обеспечивающая работу основного функционала, предоставляемого RFT/RFT-платформой: API платформы, определение списка услуг и подбор контента, внесение изменений в параметры услуг и формирование данных тарификации, взаимодействие с подсистемами оператора через модуль Custom Integration.
3. Базы данных профилей абонентов и контента, содержащие данные об абонентах системы и аудиофайлы с метаданными. Хранилище контента и логов работы платформы.
4. Телефония, обеспечивающая телефонное соединение с MSS и воспроизведение аудиофайлов.
5. Подсистема управления и мониторинга.
6. Custom Integration – промежуточный интерфейс, обеспечивающий взаимодействие платформы с подсистемами Оператора.
7. Подсистема отчётов и статистики.

# Аппаратная реализация

В данном разделе рассматриваются основные физические компоненты платформы без указания требуемых ресурсов и количества виртуальных машин (далее – ВМ) для размещения каждого из компонентов. Ниже приведен предполагаемый список ВМ с указанием логических компонентов, к которым они относятся.

**Системные ВМ:**

* **TERMINAL** (Управление и мониторинг)

Сервер доступа к площадкам RFT/RFT-платформы в периметре Оператора

* **MGMT** (Управление и мониторинг)

Репозиторий прикладного и системного ПО, необходимого для развертывания RBT/RFT-платформы

* **MAINTENANCE** (Управление и мониторинг)

Nagios-сервер, осуществляющий мониторинг платформы

**Прикладные ВМ:**

* **LOGIC** (Телефония, Подбор контента)

Сервис подбора контента

* **SRV** (Сервисная платформа)

API платформы и обработка асинхронных задач из очередей

* **STATISTIC** (БД и хранилища)

Хранилище логов работы ПО платформы за длительный срок

* **MEDIA STORAGE** (БД и хранилища)

Хранилище аудио контента платформы

* **GUI** (Управление и мониторинг)

Интерфейс администрирования платформы

* **QUEUE** (Сервисная платформа)

Система очередей RabbitMQ

* **INTEGRATION** (Custom Integration)

Интеграция с подсистемами Оператора

* **SIP** (Телефония, Модуль сигнализации)

Обработка и маршрутизация SIP-трафика

* **MEDIA** (Телефония, Модуль воспроизведения)

Обеспечение проигрывания контента

* **SMPP** (Custom Integration)

Интеграция с SMSC/USSD оператора. Маршрутизация и обработка USSD/SMS-трафика

* **NGINX** (Сервисная платформа)

Балансировщик HTTP-запросов

**ВМ СУБД:**

* **PGPOOL** (БД и хранилища)

Балансировщик запросов к MAIN DB.

* **DB, MAIN** **DB** (БД и хранилища)

Основная база данных платформы, хранит профили абонентов, метаданные контента и другие данных для предоставления услуги. Каждая физическая единица контента хранится в единственном экземпляре и может соответствовать нескольким логическим.

* **STATISTIC** **DB** (БД и хранилища)

БД статистики по звонкам и операциям абонентов, а также агрегированных данных по абонентам и их активностям;

Производительность и количество хранимых данных для платформы теоретически не ограничены и зависят исключительно от предоставляемых ресурсов.

## Схема взаимодействия компонентов платформы

Данная схема является наглядной для понимания взаимосвязей между компонентами, включая очередность процессов, и является дополнением к схеме в разделе 2.1. Часть аппаратных компонентов объединена в кластеры для удобства восприятия (например, СУБД).



Описание компонентов схемы:

* Business Logic – реализация основной логики управления профилем абонента
* Cache – система кэширования временных данных
* Media Service – обеспечение проигрывания контента
* SIP balancer – обработка и маршрутизация SIP-трафика
* Queue Service – управление и обработка очереди задач RabbitMQ
* Deferred actions – управление отложенными действиями.
* Integration module – набор интерфейсов к подсистемам оператора (биллинг/провижининг и т. д.).
* Database – кластер баз данных PostgreSQL: БД профилей абонентов, статистики, метаданных, CMS и т.д.
* SMPP client – маршрутизация и обработка USSD/SMS-трафика
* RBT platform GUI – интерфейс управления платформой
* O&M services – Nagios, git
  + Nagios – система мониторинга.
  + Prometheus – сервис обработки, хранения и отдачи метрик (Time series DB).
  + Grafana – графический интерфейс для отображения метрик

## Отказоустойчивость и масштабирование

Отказоустойчивость осуществляется на уровне ключевых компонентов с использованием горячего резерва ACTIVE-ACTIVE и ACTIVE-STANDBY по схеме N+1. Описание критичности отказа компонентов и комментарии к реализации отказоустойчивости приведены в Таблице 1.

Реализация отказоустойчивости балансировкой трафика подразумевает задействование всех резервных ВМ путем распределения трафика между ними. Выход из строя какой-либо ВМ не сказывается на качестве предоставления услуги. Отказоустойчивость балансировщика трафика обеспечивается его резервированием.

Реализация ввода в эксплуатацию резервных ВМ при ACTIVE-STANDBY для разных компонентов отличается. Для компонента SMPP контроль и переключение осуществляет платформа. Переключение выполняется подключением к SMPP-серверу оператора SMPP-клиента на резервной ВМ.

При применении облачных технологий возможно дальнейшие увеличение показателей отказоустойчивости, а также пересмотр резервирования узлов с низкой критичностью отказа.

**Таблица 1**

|  |  |  |
| --- | --- | --- |
| **Компонент** | **Критичность отказа** | **Реализация отказоустойчивости** |
| **SRV, LOGIC** | Высокая | Балансировка трафика с ВМ MEDIA установленным на них http-балансировщиком nginx |
| **SIP** | Высокая | Сигнальный трафик балансируется оператором на N+M активных ВМ |
| **MEDIA** | Высокая | Балансировка трафика через ВМ SIP |
| **MEDIA STORAGE** | Высокая | Наличие резервного ВМ на каждом выносе. При отказе основного обращения переключаются к резервному |
| **GUI** | Средняя | Балансировка трафика на резервный вынос |
| **INTEGRATION** | Высокая | Балансировка трафика через ВМ NGINX на резервный вынос |
| **MAINTENANCE** | Низкая |  |
| **PGPOOL** | Высокая | Переключение трафика на PGPOOL резервного выноса |
| **MAIN DB** | Высокая | Репликация master-slave. В случае выхода из строя master db срабатывает failover, передающий slave db обязанности master-а |
| **STATISTIC DB** | Низкая | Репликация master-slave. В случае выхода из строя master db срабатывает failover, передающий slave db обязанности master-а |
| **STATISTIC** | Низкая |  |
| **CONSUMER** | Высокая | Одновременная работа нескольких обработчиков очередей |
| **QUEUE** | Высокая | Кластер RabbitMQ из двух ВМ |
| **SMPP** | Высокая | ACTIVE-STANDBY. В случае отказа главной ВМ, к smpp-серверу подключается резервная ВМ |

При применении данной схемы отказоустойчивость системы составляет не менее 99,9%. При применении облачных технологий возможно дальнейшие увеличение показателей отказоустойчивости, а также пересмотр резервирования узлов с низкой критичностью отказа.

Также, в связи с необходимостью географического распределения архитектуры и возможностью управления из регионов с ограниченными полномочиями, применяется следующая схема: ВМ медиа-ноды резервируются путём Load-Sharing и составляют медиа-кластер, являющийся FrontEnd’ом (FE) платформы. Предполагается 6 FrontEnd-выносов.

BackEnd-выносов (BE) предполагается два – основной и резервный.

При полном отказе облачного хранилища либо дата-центра, ведущем к фактической неработоспособности любого регионального медиа-кластера, трафик маршрутизируется Оператором на центральные медиа-кластеры. При этом, по результатам нагрузочного тестирования, для центральных медиа-кластеров обеспечивается производительность, достаточная для обработки абонентского трафика во время наибольшей нагрузки (ЧНН) с учётом сценария неработоспособность одного из медиа-кластеров (при расчёте запаса мощности выбирается наиболее нагруженный). В этом случае трафик распределяется на центральные медиа-кластеры.

При этом каждый из медиа-кластеров (FronEnd’ов) способен обрабатывать трафик любого абонента вне зависимости от его домашнего региона. При необходимости осуществления профилактических работ или внесения изменений ПО переключение трафика возможно как в автоматическом режиме, так и в ручном администратором.

В платформе предусмотрено гибкое изменение синхронизации BE и FE, в случае наличия задержки в транспортном канале. Наличие задержки между FE и BE не влияет на качество предоставления услуги абоненту. В случае недоступности FE в течение длительного времени предусмотрена синхронизация контента и профилей пользователей в автоматическом режиме после восстановления связи. При синхронизации контента задержка не превышает 1000 мсек.

Масштабирование платформы осуществляется тремя способами:

* добавление медиа-кластеров;
* добавление резервных ВМ для основных компонентов;
* увеличение ресурсов имеющихся ВМ.

Добавление новых подсистем в платформу, а также новых узлов в систему происходит без остановки работы всей системы и потери полной ее функциональности.

Обеспечивается производительность не менее 3000 Эрланг на каждый FrontEnd во время максимальной нагрузки при следующих ресурсах:

* CPU – 976 vCPU;
* RAM – 1 456 Gb;
* HDD – 76 078 Gb.

Емкость системы составляет не менее 5 000 000 абонентов с возможностью расширения.

### Распределение ВМ по подсетям

В рамках обеспечения информационной безопасности платформы применяется распределение ВМ по выделенным подсетям:

* OAM (Management)
* Signaling
* Voice

## Телефонное соединение



Каждый блок телефонной части Системы RBT/RFT (Balancer, Media node) на данной схеме представляет собой виртуальный контейнер с соответствующими сервисами внутри.

Для обеспечения отказоустойчивости системы создаются два SIP-транка в режиме load-share между MSS (или SBC) и «Balancer 1», «Balancer 2». Получаемый от MSS (или SBC) трафик распределяется между медиа-нодами, количество которых зависит от общей нагрузки на систему.

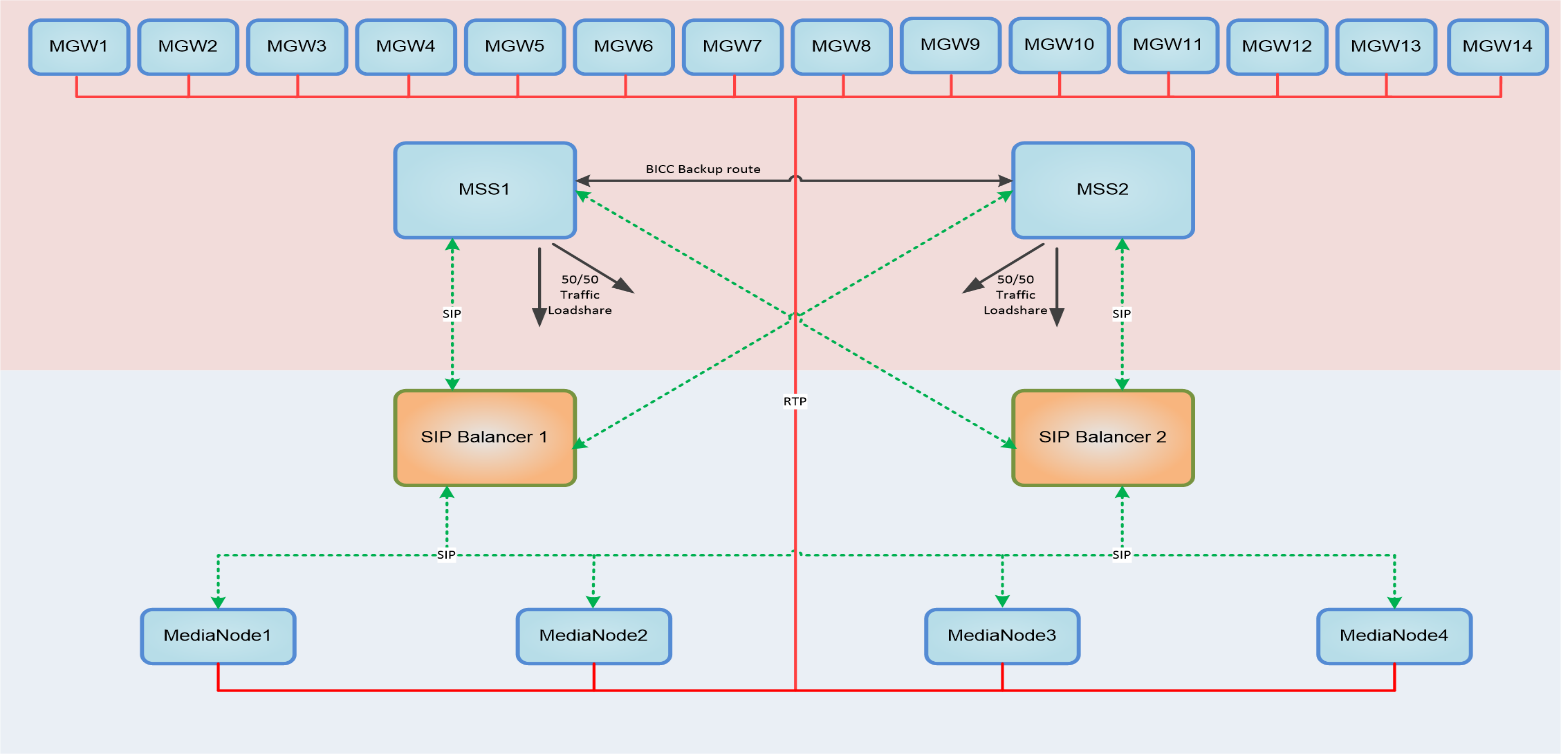
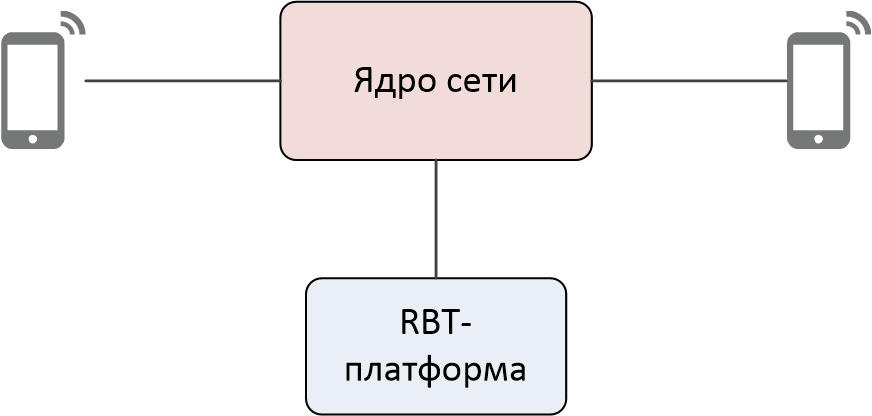


Рисунок 3: Схема сигнализации и медиатрафика

SIP-вызовы всегда осуществляются в сторону от оператора к платформе, что обозначено направленными стрелками.



RTP-трафик двусторонний, согласование кодеков осуществляется по протоколу SDP.

Прохождение RTP-трафика от абонента до платформы является необходимым условием для осуществления услуг типа Catch.

Платформа поддерживает кодеки:

* G.711A,
* GSM (Full Rate и Enhanced Full Rate),
* AMR (FR\_AMR, UMTS\_AMR и UMTS\_AMR2) для битрейтов 12.2, 10.2, 7.95, 7.40, 6.7, 5.9, 5.15 и 4.75 кбит/сек.
* AMR-WB (FR\_AMR-WB и UMTS\_AMR-WB) для битрейтов 6.60, 8.85, 12.65, 15.85, 23.85 кбит/сек.

Система хранит контент в loseless формате и производит транскодирование на лету в используемый в настоящее время тип кодека, непосредственно при проигрывании абоненту.

Платформа позволяет настроить приоритет выбора кодека при проигрывании, давая возможность исключать кодек, в котором на текущий момент отсутствует необходимость, из списка.

При интеграции согласуются следующие параметры:

1. IP-адреса и порты SIP роутеров
2. Диапазон IP-адресов и портов для RTP, с обоих сторон (для IP firewall)
3. Необходимые голосовые кодеки
4. Необходимость в PRACK сообщениях
5. Тип ответа платформы на RFT-вызов (180 Ringing /183 Progress)

Тиражирование музыкального контента по всем подсистемам обработки голосового трафика осуществляется автоматически. Подсистемы обработки голосового трафика обслуживают абонентов как региона, в котором они установлены, так и абонентов внутрисетевого роуминга. При этом профиль и установки роуминг-абонента запрашивает в "домашней сети" БД данного абонента.

### Используемые протоколы

* Протокол SIP RFC 2543, RFC 3261, RFC 3262, RFC 3263, RFC 2976, RFC 4028
* SDP RFC 4566 и RFC 3264
* RTP/RTCP RFC 3550
* Telephone-event RFC 4733 и RFC 2833
* DiffServ RFC 2474
* DNS RFC 2916 и RFC 2782
* HTTP RFC 2616
* NFS RFC 3010

# Интеграция с Оператором

Проект предусматривает участие в процессе специалистов Медиа Ком и Оператора. Предполагается установка RBT/RFT-платформы на оборудование Оператора.

Предполагается следующее разделение зон ответственности согласно активностям:

* Предоставление аппаратной составляющей проекта – Оператор.
* Обеспечение бесперебойной работы аппаратной составляющей в соответствии с согласованными типами виртуальных машин – Оператор.
* Обеспечение бесперебойной работы подсистем оператора, связанных с проектом – Оператор.
* Настройка и обеспечение работоспособности программной части – Оператор, Медиа Ком.
* Обеспечение прохождения абонентского трафика до платформы – Оператор.
* Обеспечение безопасности хранения пользовательских данных – Оператор, Медиа Ком.
* Развитие и дополнение функциональности платформы – Медиа Ком.
* Мониторинг работоспособности всей системы в рамках коммерческого запуска – Медиа Ком, Оператор.
* Техническая поддержка – Медиа Ком.

## Интеграция с биллингом

Производится подключение по HTTP/SOAP с согласованным набором параметров запроса. При необходимости возможна интеграция по иным протоколам. Производится онлайн-тарификация абонента. При технических сбоях на стороне биллинга возможна отложенная (офлайн) тарификация, осуществляемая в настраиваемые временные промежутки. Также, настраивается максимальное количество повторных запросов к биллингу.

Возможна настройка параметров списания средств для приоритетной тарификации RBT/RFT. Допускается отложенная тарификация. Вызовы для биллинговых событий осуществляется по протоколам SOAP/CAP. При необходимости возможна настройка иных протоколов, в частности DIAMETER.

Список доступных методов:

* Создание профиля абонента (с возможностью автоматического подключения услуги;
* Подключение услуги;
* Отключение услуги;
* Удаление профиля;
* Блокировка;
* Разблокировка;
* Смена MSISDN;
* Проверка статуса профиля по MSISDN

## Создание, настройка и администрирование ВМ

Создание ВМ RBT/RFT-платформы в среде виртуализации VMWare осуществляется на основе трех предоставляемых от Медиа Ком образов ВМ в формате ova:

1. Общий образ для создания всех ВМ, кроме MEDIA и SIP. Содержит настройки учетных записей, базовый набор ПО для мониторинга и управления ВМ, настроенную синхронизацию времени и DNS.
2. Образ для создания ВМ MEDIA. Помимо настроек из общего образа содержит ПО для воспроизведения контента и взаимодействия с сервисом подбора контента
3. Образ для создания ВМ SIP. Помимо настроек из общего образа содержит ПО для обработки и балансировки SIP-трафика.

Процедура установки и настройки системы выполняется в следующем порядке:

1. Создание всех требуемых ВМ.
2. Настройка доступа к RDP-терминалу и MGMT.
3. Установка недостающего системного ПО и настройка созданных ВМ. Производится с помощью сервиса управления конфигурацией Ansible.
4. Установка прикладного ПО. Производится с помощью Ansible и Git.

## API

Решение обладает унифицированным API, поддерживающим набор инструкций для обеспечения следующих действий:

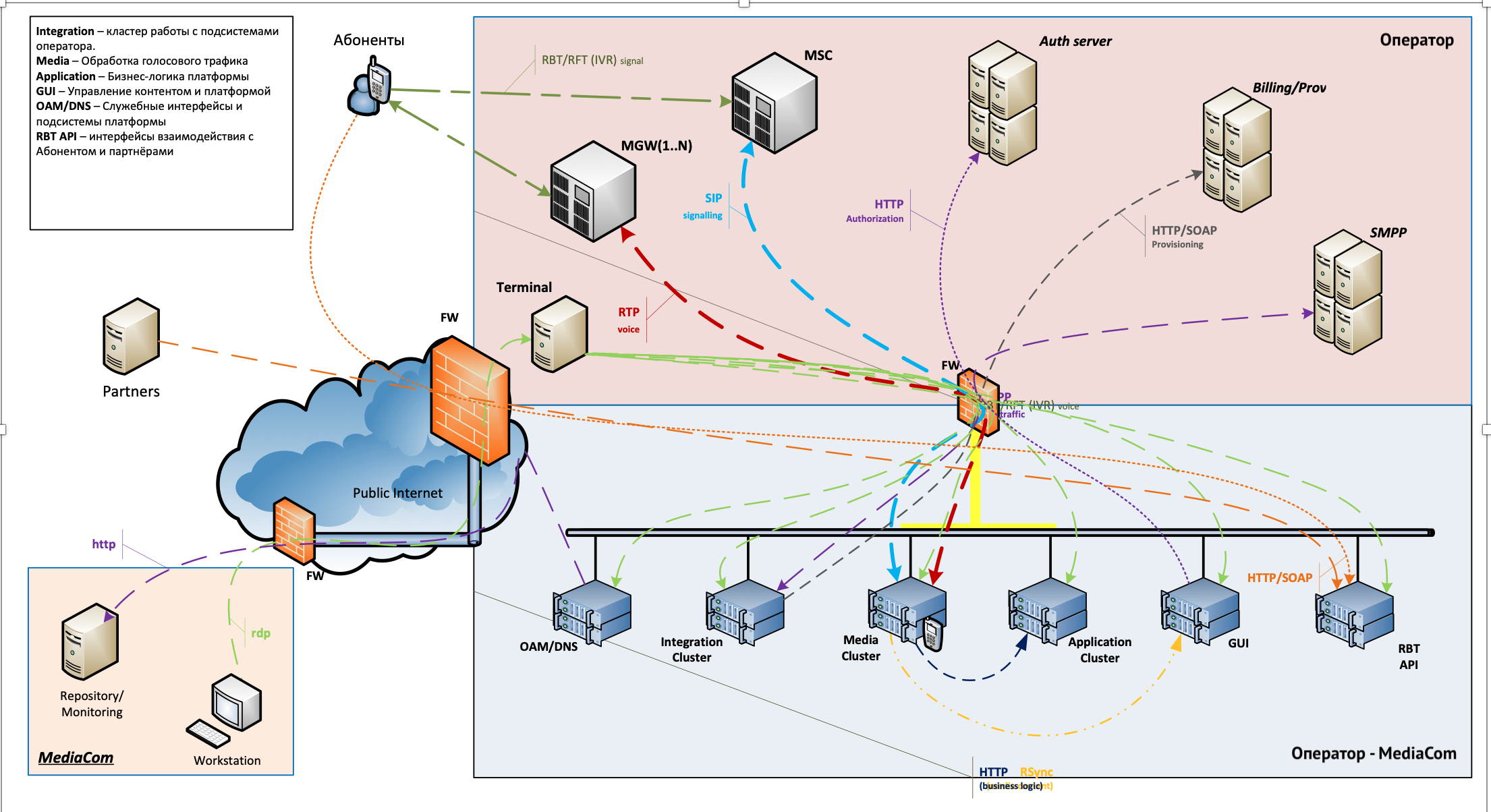
* загрузка физических файлов;
* загрузка метаданных;
* удаление;
* кодирование;
* замена физических файлов;
* изменение метаданных;
* выгрузка данных о загруженном контенте (наличие физических файлов, кодировка, метаданные);

Реализация производится по протоколу HTTP(s)/SOAP. Для интеграции по согласованию с Заказчиком также может использоваться иной протокол, например, Diameter. Для авторизации используется пара «логин-пароль», предоставляемая Медиа Ком. Количество аккаунтов технически не ограничено. Применяется политика разделения прав доступа, для каждого аккаунта можно настроить список доступных команд. Формат высылаемого абоненту при регистрации пароля настраивается в системе администратором.

Также, решение обладает унифицированным витринным API для самообслуживания абонентов. Подробно рассмотрено в документе «Руководство администратора Системы».

Поставщик реализует API для WEB-интерфейса управления услугой. Поддерживаются GET-запросы через WEB Agent от внешних партнеров.

## Диаграмма компонентов



На диаграмме компонентов представлены схемы взаимодействия Медиа Ком – Оператор. Все связи между блоками можно разделить на три группы:

### Внутренние соединения

* Integration Cluster -> Billing/Provisioning – управление услугами и онлайн-тарификация.
* Integration Cluster -> SMPP (v3.4+) – SMS/USSD-трафик.
* GUI -> Auth Server – интеграция с сервером авторизации оператора
* Media Cluster -> MSC – сигнальный трафик.
* Media Cluster -> MGW(1…N) – голосовой трафик.
* Media Cluster -> GUI – синхронизация медиа-контента.
* Media Cluster -> Application Cluster – реализация бизнес-логики на прикладном уровне.

### Защищенные соединения

* MEDIACOM Network -> OPERATOR-MEDIACOM – доступ на все сервера для разработчиков и администраторов платформы для анализа логов, настройки ПО и оказания технической поддержки во время настройки системы. Доступ через защищенный VPN-канал на базе IPSec.
* OPERATOR-MEDIACOM (OAM/DNS) -> Repository/Monitoring MEDIACOM (http/nsca) – доступ к репозиторию ПО и отправка алертов мониторинга

### Внешние соединения

* Абоненты -> MSC; Абоненты -> MG (1…N) – голосовой/сигнальный трафик.
* Абоненты -> RBT API – управление абонентом услугой через витрины
* Partners -> RBT API – управление партнерами партнерским контентом

## Стандартное ПО, устанавливаемое на ВМ

Для установки используются последние стабильные версии (stable). В дальнейшем осуществляется их обновление по договоренности. Ниже приведен список ПО, устанавливаемого на все ВМ:

* less
* strace
* sudo
* bind utilities
* mailx
* vixie cron
* iptables
* openssh clients
* openssh server
* rsync
* monit
* postfix
* vim enhanced
* elinks
* ImageMagick
* sysstat
* wget
* telnet
* lftp
* zip
* net tools
* lsof
* nrpe
* postgresql10
* nagios plugins nrpe
* zabbix agent

Для application-ВМ дополнительно устанавливается (по умолчанию):

* PHP версии(диапазон): 7 - 8.1

Для файлового сервера дополнительно устанавливается:

* Proftpd
* Nginx 1.14.0

## Дополнительно устанавливаемое ПО

### Системные ВМ

**TERMINAL** (Управление и мониторинг) – доступ к ВМ

* Windows Server 2012 R2

**MAINTENANCE** (Управление и мониторинг) – Nagios

* Nagios – система мониторинга
  + Дополнительно устанавливаемое ПО: Nagios

**MGMT** (Управление и мониторинг) – Ansible, Git

* Ansible – система хранения и деплоймента конфигураций рабочего окружения
  + Дополнительно устанавливаемое ПО: Ansible
* Git – система хранения и деплоймента прикладного ПО
  + Дополнительно устанавливаемое ПО: Git

**Nginx** – балансировщик нагрузки и прокси-сервер

* Дополнительно устанавливаемое ПО: Nginx, Perl URI

**Memcache** – сервер кэширования запросов

* Дополнительно устанавливаемое ПО: Memcached

**RabbitMQ** – сервер управления очередью задач

* Дополнительно устанавливаемое ПО: RabbitMQ

### Прикладные ВМ

**Php.nginx** – сервер приложений PHP (LOGIC, SRV, MEDIA, GUI)

* Дополнительно устанавливаемое ПО:
* RabbitMQ
* PHP
* PHP-FPM

**Java.service** – сервер Java-сервисов (LOGIC, SRV)

* Дополнительно устанавливаемое ПО:
* openjdk
* openjdk-devel
* jakarta-commons-daemon-jsvc

**Java.tomcat** – сервер Java-сервлетов (INTEGRATION)

* Дополнительно устанавливаемое ПО:
* openjdk
* Tomcat

### ВМ СУБД

**PosgreSQL** – сервер СУБД

* Дополнительно устанавливаемое ПО: PostgreSQL

**PgPool** – балансировщик запросов к СУБД

* Дополнительно устанавливаемое ПО: PgPool

# Протоколирование событий

В рамках RBT/RFT-платформы ведется протоколирование на уровне ОС, сервисов и СУБД. Для всех лог-файлов предусмотрены ротация и архивация, период выбирается в зависимости от объема информации, но не менее 1 раза в сутки. Протоколирование событий на системном и прикладном уровнях соответствует требованиям стандарта CT-014.

Уровень протоколирования системных событий – по умолчанию (INFO). Запись логов производится в /var/log/syslog/, куда имеют доступ только привилегированные пользователи. В частности, протоколируются следующие события:

* Выполнение команд по повышению прав доступа (sudo, su);
* Все виды попыток аутентификаций пользователей вне зависимости от их успешности;
* Ошибки в работе системы;
* Все действия суперпользователя на любом из уровней доступа (использование учетных записей администратор/суперпользователь) ;
* Обновление/изменение прав доступ пользователя;
* Логирование экспорта любых данных из системы;
* Запись всех попыток изменения/добавления/уничтожения предопределённых объектов данных;
* Блокировка учетной записи пользователя;
* Изменение конфигурации логирования;
* Все действия любого пользователя через удалённую сессию (если применимо) ;
* Все успешные и неуспешные попытки аутентификации (logon и logoff) ;
* Факты выхода из системы;
* Любые попытки аутентификации от неизвестных ID пользователей и неизвестных ID рабочей станции;
* Попытки открыть несколько сессий под одной учетной записью;
* Изменения конфигурации формирования журналов событий;
* Тенденции использования специфических учетных записей;
* Любые обращения к СУБД, включая данные о транзакциях;
* Образа любых данных перед и после изменения.

Типы событий при нештатных ситуациях:

* critical, после возникновения которого произошел останов работы или полная потеря функциональности;
* major, ведущие к сбою в работе или потери части функциональности, а также искажению данных;
* minor, не влекущие за собой потерю производительности или функциональности
* warning, информация о возникновении ситуаций, которые могут повлечь за собой сбои и ошибки в работе.

Данные об оповещениях логируются с разной степенью детализации.

Каждая запись, относящаяся к действиям пользователя, обязательно содержит идентификатор пользователя и рабочей станции. В системных логах находятся следующие данные:

* Дата и время активности, либо период её выполнения (можно реализовать с помощью двух записей – начала и окончания). Для длительных активностей – дата и время начала и окончания;
* ID пользователя;
* ID рабочей станции;
* Тип активности;
* Вспомогательный инструмент (ПО), если применимо;
* Статус (успешность/неуспешность);
* Информация, позволяющая идентифицировать объект, над которым выполнялось действие (файл, группа файлов, таблица СУБД и т. д.);
* Запись образа данных до и после изменения;
* Тип учетной записи пользователя (привилегии);
* Метка использования учетных записей за пределами рабочего времени (конфигурируется отдельно);
* Метка использования удалённых рабочих станций;
* Уникальный идентификатор записи.

Для просмотра системных событий используется единый GUI для управления событиями информационной безопасности. Возможности по просмотру и выгрузке логов

* Фильтр поиска логов по имени пользователя (логин) ;
* Фильтр поиска по NE;
* Фильтр поиска по типу лога (системный, лог СУБД, лог прикладного ПО);
* Возможность указания интервала даты и времени с точностью до секунды;
* Фильтр по событию или комбинации событий (например, авторизация в системе, либо успешное изменение параметров приложения);
* Настройка получения по расписанию запрошенного типа логов с применением фильтрации;
* Хранение логов в виде, пригодном для фильтрации и анализа за последние 6 месяцев;
* Хранение архивных логов с группированием по интервалу не более суток, с возможностью получения через интерфейс;
* Выгрузка логов в формате MS Excel.

Для формируемых журналов событий настроена система архивации и экспорта. Период архивации настраивается в зависимости от средней активности пользователей. После архивации журнала производится его экспорт в защищенное хранилище. Период хранения журналов согласовывается на этапе размещения.

Учетные записи, используемые для управления абонентами и услугами, не имеют доступа к информации, составляющей тайну связи абонентов. Для привилегированных пользователей доступен перечень учетных записей, включающий в себя роль каждой записи, права доступа, дату начала и окончания периода действия.

На Системе «RBT/RFT» есть возможность формирования журналов high usage reports.

# Статистика

Платформа осуществляет сбор и агрегацию статистики по следующим операциям:

* Статус услуг, относящихся к Системе «RBT/RFT»;
* Проигрывание контента абоненту (звонки абонента А со временем);
* Операции абонента с контентом и услугой;
* История тарификации абонента;
* История взаимодействий со всех витрин.

Схема формирования статистики:

Изначально на VPS, являющимися серверами приложений формируются текстовые лог-файлы. Каждые десять минут эти лог-файлы заливаются по FTP на VPS статистики, где они группируются по дням и передаются в БД статистики. В БД они хранятся в течение 3 месяцев, а на VPS статистики – 3 года. Формат даты: DD.MM.YYYY H24:MM: SS.

Статистика звонков включает в себя A-номер, дату и время начала проигрывания, информацию о проигранном контенте, длительность проигрывания, идентификатор услуги, в рамках который был проигран контент.

Статистика операций абонента содержит MSISDN абонента, дату и время выполнения операции, кодовое наименование операции, тип и идентификатор объекта операции (услуга/контент/группа контента), а также идентификатор витрины, посредством которой операция была выполнена, и код выполнения операции.

История тарификации содержит только информацию о датах и размере списаний абонентской платы за пользование абонентом услугой.

При каждой операции (абонентские, тарификация) платформа сохраняет информацию о произведенных действиях, о профиле абонента (в т. ч. контента) до и после произведенного действия. Запись операций происходит посредством отправки в очередь (RabbitMQ) со стороны витрин и телефонного бэкенда (LOGIC), на основании данной статистики платформа формирует CDR-логи с произвольной периодичностью, согласованной с оператором. Идентификатор CDR-файла содержит UID инсталляции.

Агрегированная статистика формируется на основе данных из БД и представляет собой суммированную информацию за день или месяц по различным критериям – количество активных абонентов, подписок/отписок от услуг, проигрываний. Агрегированная статистика хранится в БД статистики и доступна в WEB-интерфейсе RFT-платформы в виде графиков, на которых представлено распределение количественных данных по временной шкале. Возможна выгрузка статистики в формате xls/csv.

# Системы управления и отчетности

## GUI

CMS платформа предназначена для решения прикладных задач по администрированию платформы. К платформе может быть подключено не менее 100 контент-провайдеров. Номерная емкость для каждого провайдера не менее 100K кодов заказа. У контент-провайдеров и контент-агрегаторов есть конфигурируемая возможность администрирования доступа (доступ к настройкам двух и более контент-провайдеров).

Общее количество пользователей BackOffice может быть на уровне полутора тысяч пользователей с возможностью дальнейшего расширения. Одновременно полнофункциональную работу могут осуществлять не менее 250 сотрудников.

Присутствует возможность вызова http(s) страницы BackOffice с указанием MSISDN абонента в составе строки URL.

Основные возможности GUI:

* Управление выносами;
* Управление контентом (в т.ч. и его количеством в аккаунте у абонента), а также его модерацией, включая отклонённый контент;
* Управление абонентами;
* Управление тарификационными группами;
* Просмотр статистики;
* Формирование отчетов online;
* Управление справочниками;
* Справочный интерфейс;
* Управление СМС-информированием;
* Управление пользователями и ролями;
* Управление конфигурационными параметрами в режиме online;

Обеспечивается корректная работа в следующих браузерах:

* Microsoft Internet Explorer v9 и выше;
* Google Chrome v51 и выше.

При ошибочных действиях пользователя в GUI ему выводится соответствующее уведомление.

## Ansible

Установка и обновление системного ПО производится с помощью системы Ansible, предназначенной для хранения и деплоймента конфигураций рабочего окружения и расположенной на ВМ MGMT. Для разных ролей ВМ существуют стандартные конфигурационные файлы, в которых содержится информация для установки набора системного ПО, протестированного на совместимость и безопасность. При возникновении ошибок в процессе установки Ansible создает уведомление и откатывает неуспешную операцию. Также, Ansible по запросу проверяет соответствие конфигурации системного ПО и его окружения на обслуживаемых ВМ. Обновление происходит следующим образом: при принятии решения о необходимости обновления на сервере политик Ansible вносятся изменения в конфигурационный файл, далее производится проверка и обновление ВМ согласно их ролям.

## Git

С помощью системы Git, расположенной на ВМ MGMT, производится установка и обновление прикладного программного обеспечения в штатном режиме, в два этапа. Сначала производится обновление репозитория на ВМ MGMT, находящейся на площадке оператора, может быть инициировано обновление прикладного ПО на необходимых application-ВМ своими силами.

## Prometheus

Для сбора метрик работы платформы используется система Prometheus. Prometheus регулярно опрашивает компоненты платформы и сохраняет полученные метрики во встроенную «time series» базу данных. Опрашиваются также стандартные метрики операционной системы каждого хоста.

На основании собранных данных основные KPI платформы визуализируются с помощью системы Grafana. Для метрик настраиваются пороги срабатывания оповещений, которые отправляются по почте (протокол SMTP) в дежурную службу.

## Grafana

Grafana может визуализировать настраиваемую аналитику поведения пользователя в системе в виде круговых диаграмм, гистограмм времени и других графических элементов.

Более подробно о системе Grafana и её возможностях можно узнать в документации от производителя: <https://grafana.com/docs/>.

Интеграция Grafana с Prometheus описана в документации Prometheus: <https://prometheus.io/docs/visualization/grafana/>

# Информационная безопасность

## Общие сведения

### Безопасность операционных систем, баз данных

Для платформы используется решение на базе РЕД ОС. Устанавливается сборка РЕД ОС, которая содержит только служебные утилиты, необходимые для настройки и обеспечения работоспособности основного функционала ОС, стандартных служб и протоколов.

На регулярной основе проверяется информация об обновлении Common Vulnerabilities and Exposures (CVE), а также наличия патчей для закрытия обнаруженных уязвимостей и/или оптимизации работы системы. Перед установкой патча на виртуальные машины (ВМ) производится установка на тестовый стенд.

После конфигурирования ВМ, системного и прикладного ПО производится расчет максимально допустимого количества процессов на уровне ОС. Ограничение производится средствами Pluggable Authentication Modules (PAM).

Для управления дисковым пространством используется Volume Manager LVM, файловая система – ext4. Установка приложений производится в отдельные файловые системы (/home), системные файловые системы (/, /var), не используются. В качестве общедоступной директории используется /tmp, для нее устанавливается sticky bit.

Для контроля целостности конфигурации системы используется решение на основе Osec. Каждые 10 минут производится проверка всех системных каталогов. При обнаружении изменений в конфигурации генерируется отчет, а также происходит срабатывание системы мониторинга.

Конфигурирование синхронизации времени NTP производится вручную, для синхронизации используется NTP-сервер, предоставляющий данные о времени UTC безотносительно часового пояса физической установки оборудования. В случае отказа основного NTP-сервера используется резервный.

### Конфигурирование сетевых настроек

Для каждой ВМ производится конфигурирование сетевых служб, используются только необходимые для взаимодействия с остальными компонентами. Доступ к ВМ возможен по следующим протоколам:

* SSH – доступ для конфигурирования ПО, устранения сбоев;
* HTTP – синхронизация (обновление) прикладного ПО;
* NSCA – протокол, используемый системой Nagios для мониторинга работоспособности.

В рамках системы NFS и DHCP не используется. Статические маршруты запрещены. В sysctl.conf прописан запрет на возможность приема и отправки ICMP-ответов на широковещательные запросы, а также прием и отправку ICMP-редиректов. Также, запрещен протокол IPv6. Отключена возможность доступа по протоколам telnet и FTP, а также IP-forwarding/routing.

При конфигурировании SSH-доступа используются следующие параметры:

* Применяется только вторая версия SSH-протокола (SSH-2), поддерживающая двойной шифрованный обмен ключами RSA.
* Разрешена аутентификация только с использованием RSA-ключей длиной не менее 2048 бит. Аутентификация без ключа, в том числе с использованием только .rhosts/. shosts – запрещена.
* SSH-туннелирование запрещено.

При конфигурировании протоколов HTTP и NSCA используется аналогичный уровень безопасности.

В РЕД ОС используется версия ядра, в которой реализован усложненный алгоритм создания номеров TCP-пакетов (RFC 1948). Для защиты от SYN-flood атак используется SYN-cookies (в файле /etc/sysctl.conf параметр net.ipv4.tcp\_syncookies = 1).

## Идентификация и аутентификация и управление доступом

Для выполнения любого действия в системе пользователь должен быть успешно авторизован.

### Конфигурирование учетных записей ОС

Минимальная длина пароля – 8 символов. Авторизация по пустым паролям через SSH запрещена. В случае трех неудачных попыток ввода пароля учетная запись будет заблокирована. Разблокировка производится по запросу только с учетной записи суперпользователя.

В рамках RBT/RFT-платформы используются следующие учетные записи:

* учетные записи(ограниченный список), необходимые для настройки и установки системного и прикладного ПО. Имеют права доступа на все ВМ;
* girard – учетная запись, используемая для запуска на ВМ java-сервиса. Имеет ограниченные права, достаточные для запуска сервиса;
* girar – учетная запись системы деплоймента, необходимая для обновления прикладного ПО. Доступ на чтение/запись имеется только в местах физического размещения и каталогах данных прикладного ПО. Требуется обеспечение SSH-доступа по ключу без ввода пароля при аутентификации;
* nagios – учетная запись системы мониторинга, имеющая доступ исключительно к получению данных, необходимых для наблюдения за работоспособностью системы;
* apache – учетная запись, необходимая для работы системного и прикладного ПО, имеющая ограниченные права, достаточные для запуска приложений.

### Конфигурирование прав доступа ОС

Права на файлы и директории устанавливаются по умолчанию для РЕД ОС. При этом, для каждой ВМ производится настройка типовых учетных записей.

Авторизация пользователей происходит через центральную систему каталогов компании, использование локальных учетных записей для пользователей запрещено.

Для домашних директорий пользователей устанавливаются права по умолчанию 700 (доступ только у владельца учетной записи). Домашние директории находятся на отдельной файловой системе, перемонтированной в home. При создании профиля пользователя используется параметр umask = 022, соответственно все создаваемые директории имеют права доступа 755, а файлы – 644.

Удаленный вход в систему для суперпользователя (root) запрещен   
(PermitRootLogin = no).

Для учетной записи суперпользователя (root) устанавливается UID = 0, для остальных UID отличен от 0. Работа учетных записей приложений организована через /bin/false, что ограничивает их в правах доступа на сервер.

### Конфигурирование учетных записей БД

Для доступа к БД по умолчанию используются учетные записи:

* postgres – встроенная учетная запись суперпользователя БД. Доступ только по SHA-256 ключу с использованием пароля на локальной ВМ;
* user(#) – для каждого пользователя, которому необходимо иметь доступ к управлению БД, создается уникальная учетная запись, доступ осуществляется только по SHA-256 ключу. При создании пользователю присваивается определенная роль (исключая роль суперпользователя) и доступы только к необходимым базам и таблицам. Пароль меняется не реже, чем 1 раз в 6 месяцев;
* inform – учетная запись, используемая прикладным ПО. Разрешенные операции: INSERT, SELECT, UPDATE для таблиц с данными. Доступ по SHA-256 ключу только с ВМ, на которых расположено прикладное ПО, использующее данную БД;
* nagios – учетная запись мониторинга. Имеет доступ к операции SELECT, а также UPDATE для таблицы monitoring, если она присутствует в структуре БД. Доступ по SHA-256 ключу с ВМ, на которой расположен сервер мониторинга.

### Безопасность при управлении абонентами и услугами

Для управления абонентами и услугами на RBT/RFT-платформе имеется отдельный GUI (описан в документе «Руководство по WEB интерфейсу Системы»), а также отдельный набор ролей с различными привилегиями. Неавтоматизированное управление услугами и абонентами возможно только для отдельных элементов. Проведение массовых операций, связанных с управлением услугами и абонентами, осуществляются через Provisioning-интерфейс.

## Безопасность при интеграции RBT/RFT-платформы в IP сети

### Организация сетевых доступов

При настройке межсетевого экранирования для Системы «RBT/RFT» предоставляется доступ извне по следующим протоколам:

* SSH через RDP на основе Balabit – доступ для конфигурирования ПО, устранения сбоев. Во время эксплуатации доступ предоставляется по запросу. Подключение производится из сети Медиа Ком по VPN-туннелю, со строго определенных IP-адресов;
* HTTP – синхронизация (обновление) прикладного ПО. Доступ необходим к application-ВМ. Подключение производится из сети Медиа Ком по VPN-туннелю, со строго определенных IP-адресов.

# Система мониторинга

Для мониторинга используется решение, основанное на системе Nagios. Также, для сбора статистики и формирования отчётов используется связка Prometheus+Grafana. Основной сервис мониторинга размещается совместно с остальной системой (ВМ MAINTENANCE). Решение обеспечивает возможность функционирования в 12-ти часовых поясах. Нагрузка на систему мониторинга не влияет на производительность остальных сервисов.

С заданной периодичностью сервис мониторинга запускает набор проверочных скриптов. Также на каждой виртуальной машине системы запущен агент, собирающий общесистемную информацию (LA, использование RAM, HDD и т. п.). При превышении порога срабатывания проверки генерируется алерт системы мониторинга.

Опрос машин происходит по портам сетевых служб и протоколов (SSH, HTTP и т. д.), а также по специализированным протоколам NRPE (5667) и NSCA (5666).

При необходимости возможна отправка данных по протоколам SNMP/NSCA/NRPE в систему мониторинга. Доступно формирование и отправка автоматических e-mail уведомлений по протоколу SMTP и оповещение посредством SMS, в том числе с возможностью выбора языка формируемого оповещения.

Для обеспечения максимального покрытия сценариев возникновения сбоев применяется несколько групп и типов проверок:

1. Простые проверки работоспособности и доступности серверов и иных ресурсов, основанные на стандартных алгоритмах. К ним относится доступность по различным протоколам (TCP, SSH, Telnet и т. д.), наличие свободного места, Load Average (LA), доступная оперативная память, целостность таблиц СУБД и т. д.
2. Проверки отсутствия ошибочных статусов в логах сервисов и таблицах СУБД.

Срок хранения событий мониторинга по умолчанию не ограничен. Возможна настройка по согласованию с оператором.

События мониторинга формируются в отчет, который включает в себя:

* KPI
* Отчетность по всем типам трафика
* Ошибки

Все несоответствия должны указываются в графе "Comments".

Выбранные администратором отчеты доступны как пользователям BackOffice, так и Партнерам

Выгрузка отчетов может быть реализована в следующих форматах:

* Excel-документов;
* HTML/XML-документов;
* PDF

Сам отчет содержит в себе следующие критерии:

* Количество запросов (вызовов, запусков), полученных с подразделением, выполненным внешними системами;
* Количество успешно обработанных запросов;
* Количество не успешно обработанных запросов с подразделением по причинам сбоя и внешним системам;
* Количество запросов, при отправке которых произошел сбой, с подразделением по причинам сбоя и внешним системам;
* Процентное соотношение загрузки/использования системы касательно максимальной пропускной способности;
* Процентное соотношение загрузки/использования системы касательно максимального разрешенного значения.

## Основные параметры проверочных скриптов

По умолчанию каждый проверочный скрипт для отдельной точки мониторинга запускается 1 раз в 5 минут. При превышении порогового значения (алерт), проверочный скрипт отрабатывает каждые 3 минуты. Протоколируется каждое изменение состояния проверяемого сервера/сервиса.

## Покрытие мониторинга и локализация

Для реализации мониторинга предусмотрено покрытие всех основных сбоев, связанных с обработкой запросов абонентов, прогнозируемых после этапа тестирования.

Покрытие мониторинга включает в себя:

* Типовые проверки работоспособности всех ВМ площадки
* Проверки всех центральных узлов на возникновение любых ошибок платформы, предупреждение чрезмерной нагрузки, а также процента внешних ошибок согласно статистической логике.

Список проверок Nagios, их описание, возможные статусы, действия и примеры аварийных и информационных сообщений приведены в документе

## Автоматический перезапуск

Автоматический перезапуск необходим для устранения известных сбоев простого характера, например, зависание скрипта. Для выполнения данной задачи используется система Monit. Интервал проверки составляет 1 минуту. В случае, если перезапуск не устранил проблему, при следующей проверке происходит оповещение ответственных лиц через систему Nagios.

Объект автоматического перезапуска должен удовлетворять следующим критериям:

* Известный характер проблемы с простым решением – ситуация, в которой простой перезапуск скрипта исправляет неполадку.
* Безопасность автоматического перезапуска – исключение наступления негативных последствий, таких как повреждение данных или последующая неработоспособность зависимых сущностей.
* Допустимый интервал повторения проблемы за период – условие, при котором срабатывание автоматического мониторинга более N раз за период является нештатной ситуацией и требует вмешательства специалиста.
* Минимальный интервал перезапуска – исключение ситуации, когда перезапуск осуществляется быстрее, чем восстанавливается нормальная работа системы.

# Резервное копирование и восстановление

В связи с использованием облачных технологий для обеспечения отказоустойчивости системы платформой реализовано резервное копирование только для баз данных PostgreSQL. Система резервного копирования данных работает в автоматическом режиме. Для резервирования используется утилита pg\_dump. В зависимости от роли БД выбирается период резервного копирования. Процесс производится в ночное время при минимальной нагрузке на систему. Интервал (от 1 суток) настраивается в зависимости от критичности информации и частоты её обновления.

Для обеспечения оперативного восстановления хостов требуется резервное копирование виртуальных машин со следующей периодичностью:

## Общие требования к резервному копированию

Обеспечивается поддержка следующих процедур:

* создание резервных копий для всех необходимых ресурсов;
* отдельная процедура восстановления от резервных копий для всех необходимых ресурсов;
* переключение между компонентами резервного копирования.

## Общие требования к восстановлению

Обеспечивается поддержка следующих процедур:

* восстановление системы в целом
* автоматическое восстановление системы
* ручное восстановление системы
* полное сохранение всех элементов, функциональных компонентов и линий связи системы при аварии
* отклик в чрезвычайных ситуациях
* переход в специальный режим работы в аварийных условиях
* задачи восстановления
* переход в режим стандартной работы после восстановления

Время восстановления системы по приоритетам:

* 1 приоритет - 4 часа;
* 2 приоритет - 12 часов;
* 3 приоритет - 24 часа;
* 4 приоритет - 72 часа;
* 5 приоритет - 168 часов.