

Руководство администратора

v.3.12.86 - 28.04.2023



Оглавление

1	Введение.....	4
1.1	Описание документа.....	5
1.2	Назначение системы.....	6
2	Системные требования.....	7
2.1	Системные требования к серверу.....	8
2.2	Системные требования к агенту.....	9
2.3	Сетевые доступы.....	10
3	Задачи администратора.....	12
3.1	Настройка параметров работы системы.....	13
3.1.1	Установка агента.....	14
3.1.1.1	Автоинсталляция.....	15
3.1.1.2	Linux.....	16
3.1.1.3	Mac OS X.....	17
3.1.1.4	Windows.....	18
3.1.1.5	Wiren Board 6.....	20
3.1.2	Конфигурация агента.....	21
3.1.2.1	Подключение к Kafka Cluster.....	23
3.1.3	Конфигурация сервера.....	24
3.1.4	Настройка элементов web-интерфейса.....	49
3.1.5	Служба "saumon-server".....	60
3.1.6	Просмотр websocket-нотификаций.....	61
3.1.7	Увеличение количества обработчиков SNMP-Trap.....	62
3.1.8	Сброс системы к заводским настройкам.....	63
3.1.9	Включение функционала генерации аварий.....	64
3.1.10	Передача аварий в сторонние сервисы.....	65
3.1.11	Работа со свойствами аварий.....	66
3.1.12	Перевод SNMP OID в текстовый формат.....	68
3.1.13	Выполнение скриптов при создании и удалении объектов.....	69
3.1.14	Автоматическое обнаружение объектов.....	70
3.2	Модуль аналитики.....	71
3.2.1	Подключение модуля аналитики к Центральному Пульту.....	72
3.2.2	Мониторинг работы модуля аналитики.....	73
3.3	Управление сенсорами мониторинга.....	74
3.3.1	Скрытие неиспользуемых сенсоров.....	75
3.3.2	Настройка пользовательских сенсоров.....	76

3.4	Настройка уведомлений	78
3.4.1	Активация функционала отправки SMS и голосовых вызовов	79
3.4.2	Отправка почтовых уведомлений	80
3.4.3	Настройка уведомлений в Telegram	81
3.5	Интеграция со сторонними системами.....	83
3.5.1	Интеграция с Zabbix	84
3.5.2	Интеграция с Grafana	88
3.5.3	Интеграция с Keycloak	92
3.5.3.1	Настройка сервера	93
3.5.3.2	Настройка web-интерфейса.....	98
3.6	Управление логированием	102
3.6.1	Конфигурация log-файлов агента	103
3.6.2	Конфигурация ротации log-файлов сервера	105
3.6.3	Просмотр информации о Журнале событий.....	106
3.6.4	Назначение ответственного за событие	107
3.6.5	Установка ограничения для логирования	108
3.6.6	Удаление всех SNMP-Trap'ов из Журнала событий.....	109
3.6.7	Удаление логов	110
3.7	Управление учётными записями пользователей	111
3.7.1	Авторизация пользователей через LDAP	112
3.7.2	Авторизация пользователей через Keycloak.....	114
3.7.3	Создание учётной записи.....	115
3.7.4	Назначение пользователям прав доступа.....	117
3.7.5	Назначение парольных политик	119
3.7.6	Изменение пароля от учётной записи.....	120
3.7.7	Настройка доступа к объектам.....	121
3.7.8	Блокировка учётной записи.....	122
3.7.9	Удаление учётной записи	124
3.8	Работа с объектами и связями.....	125
3.8.1	Создание объекта.....	126
3.8.2	Клонирование объекта	127
3.8.3	Удаление объекта	128
3.8.4	Создание ссылки на объект	129
3.8.5	Создание связи.....	130
3.8.6	Удаление связи	132
3.9	Настройка интерфейса.....	133
3.9.1	Выравнивание/расстановка объектов в стандартном виде.....	134
3.9.2	Настройка заголовка web-интерфейса.....	135

3.9.3	Перемещение/отключение фоновой иконки объекта	136
3.9.4	Вертикальное отображение имени объекта	137
3.9.5	Редактирование стилей состояний.....	138
3.10	Настройка мониторинга.....	139
3.10.1	Мониторинг основных параметров ПК	140
3.10.2	Мониторинг процесса памяти	141
3.10.3	Мониторинг изменения файлов и папок	142
3.10.4	Проверка доступности web-ресурса.....	143
3.10.5	Безагентный мониторинг web-сервера	144
3.11	Страницы для внедрения в IFrame	145
3.11.1	Страница с авариями	146
3.11.2	Страница с графиками.....	148
3.11.3	Страница с журналом сессий.....	153
3.12	Открытие терминала удалённого доступа	155
3.13	Переход к web-интерфейсу устройства.....	157
3.14	Резервное копирование и восстановление данных	158
3.15	Серверные расширения.....	162
4	Проблемы в работе системы и способы их решения	165
4.1	Недостаточно места на виртуальной машине с сервером	166
4.2	Отсутствие подключения агента к серверу	168
4.3	Проверка работы MongoDB	169
4.4	Проверка работы Redis	170
4.5	500 Internal Server Error и отсутствие графиков	171
4.6	Ошибка работы HTTP-проверки	172
	Приложение А (обязательное).....	173
	Приложение Б (обязательное)	178

1 Введение

Центральный Пульт - это платформа для визуализации и мониторинга работы сети, оборудования, приложений и служб.

1.1 Описание документа

Настоящий документ является руководством для администрирования автоматизированной системы "Центральный Пульт" и предназначен для конкретизации задач и функций должностных лиц организации (предприятия, фирмы), планирующих и осуществляющих сбор, хранение, передачу и анализ данных по объектам мониторинга с применением системы.

В документе приведены основные функции администратора, архитектура системы и её модулей, алгоритм создания учётных записей, порядок установки прав доступа пользователей и другие сведения, необходимые для управления АС "Центральный Пульт".

1.2 Назначение системы

Система предназначена для визуализации и мониторинга различных объектов. Центральный Пульт нацелен на упрощение сбора данных, ускорение их анализа, визуализации результатов и непрерывного хранения.

Автоматизации подвергаются следующие функциональные возможности процесса мониторинга:

- процесс обработки данных;
- хранение оригинальных значений;
- обеспечение анализа информации;
- управление объектами мониторинга;
- уведомление пользователей о состояниях объектов;
- исправление аварийных ситуаций;
- преобразование данных в компактный вид;
- экспорт данных;
- удаление устаревших данных.

2 Системные требования

Система может быть установлена на выделенных аппаратных или виртуальных мощностях.

Для стабильной работы клиента системы необходим web-браузер Google Chrome версии не ниже 58.0.

2.1 Системные требования к серверу

Для работы сервера системы требуется следующая конфигурация:

- 64-bit OS;
- CPU - 4 cores;
- RAM - 8 GB;
- HDD - 72 GB.

Гарантируется корректная работа инсталляционного скрипта сервера на следующих ОС:

- Ubuntu Linux 20.04;
- Ubuntu Linux 18.04.

Установка системы также возможна на операционные системы:

- РЕД ОС,
- Red Hat Enterprise Linux,
- Astra Linux,
- Debian.

"Центральный Пульт" может быть запущен и на других дистрибутивах Linux. Свяжитесь с нами welcome@saymon.info, если вы не нашли нужную вам операционную систему среди перечисленных.

Серверная часть системы может быть поставлена в виде готового образа виртуальной машины или Docker-контейнера. Ссылки можно получить в службе технической поддержки по адресу welcome@saymon.info.

2.2 Системные требования к агенту

Агенты обладают кросс-платформенной совместимостью и могут быть установлены на различные операционные системы, например:

- Ubuntu Linux;
- Red Hat Enterprise Linux / CentOS Linux;
- Raspberry Pi;
- Mac OS X;
- Windows.

Требованием к операционным системам является поддержка Java SE 6, 7 и 8.

Рекомендуемая конфигурация для работы агентов системы:

- OS with Java 6/7/8 support;
- CPU — 2 GHz single core;
- RAM — 1 GB;
- HDD — OS + 2 GB

2.3 Сетевые доступы

Порты по умолчанию, необходимые для корректной работы Центрального Пульта (часть 1 из 2):

Порт	Протокол	Сервис	Инициатор соединения	Место назначения	Комментарий
22	TCP	SSH	Сотрудники технической поддержки	Все серверы платформы	Удалённый доступ к серверам для настройки и оказания технической поддержки.
80	TCP	HTTP	Пользователи Центрального Пульта	Серверы с сервисами Центрального Пульта	Доступ к web-интерфейсу платформы. Рекомендуется перенаправление на 443 порт.
162	UDP	SNMP Trap	Оборудование, отправляющее SNMP Trap	Серверы с агентами	Получение SNMP Trap от оборудования. По умолчанию на каждом сервере с сервисами Центрального Пульта установлен агент, который получает SNMP Trap'ы.
443	TCP	HTTPS	Пользователи Центрального Пульта	Серверы с сервисами Центрального Пульта	Доступ к web-интерфейсу Центрального Пульта с шифрованием трафика.
3001	TCP	Wetty	Пользователи Центрального Пульта	Оборудование в инфраструктуре заказчика	Доступ к терминалам устройств через SSH и Telnet.
4242	TCP	OpenTSDB	Серверы с сервисами Центрального Пульта	Серверы с OpenTSDB	Доступ к базе данных хранения временных рядов для построения графиков. Необходим при инсталляции OpenTSDB на отдельных серверах.
6379	TCP	Redis	Серверы с сервисами Центрального Пульта	Серверы с Redis	Доступ к кэшу данных. Необходим при инсталляции Redis на отдельных серверах.

Руководство администратора

Глава 2: Системные требования

Порты по умолчанию, необходимые для корректной работы Центрального Пульта (часть 2 из 2):

Порт	Протокол	Сервис	Инициатор соединения	Место назначения	Комментарий
8090	TCP	SAYMON REST API	Пользователи, интеграционные модули и расширения	Серверы с сервисами Центрального Пульта	Взаимодействие с системой и данными через REST API.
8091	TCP	SAYMON Notification Actor	Пользователи Центрального Пульта	Серверы с сервисами Центрального Пульта	Необходим для быстрого обновления данных в web-интерфейсе и мобильных клиентах через WebSocket.
8092	TCP	SAYMON Resource Server	Пользователи, интеграционные модули и расширения	Серверы с сервисами Центрального Пульта	Отображение в web-интерфейсе приложенных к объектам документов и фоновых изображений.
9092	TCP	Kafka	Серверы с сервисами Центрального Пульта	Серверы с Kafka	Доступ к шине данных. Необходим при инсталляции системы на нескольких серверах и при использовании агента для сбора данных.
27017	TCP	MongoDB	Серверы с сервисами Центрального Пульта	Серверы с MongoDB	Доступ к базе данных основной информации об объектах и пользователях. Необходим при инсталляции MongoDB на отдельных серверах.

3 Задачи администратора

Глава содержит информацию об основных задачах, возникающих в процессе администрирования платформы.


3.1 Настройка параметров работы системы

Раздел настройки - один из самых важных разделов, предназначенный для администратора системы. Этот раздел наполнен советами о том, как настроить Центральный Пульт для мониторинга вашей среды, начиная настройкой сервера для получения необходимой информации и заканчивая просмотром данных, настройкой оповещений и удалённых команд, выполняемых в случае возникновения проблем.

3.1.1 Установка агента

Перед началом работы с платформой "Центральный Пульт" необходимо выполнить следующие действия:

1. Получить актуальную версию агента одним из способов:
 - зайти на сайт платформы на страницу "Загрузки" saymon.info/support_ru/downloads_en/ и скачать подходящую под ОС сборку агента;
 - перенести с CD-ROM, USB-накопителя или другого носителя, на котором поставляется платформа "Центральный Пульт", подходящую под пользовательскую ОС сборку агента на компьютер, сервер или устройство, на котором планируется осуществлять сбор данных.
2. Установить и настроить агента согласно дальнейшим инструкциям.

 При установке агента на Linux в системе автоматически создаётся пользователь **saymon**, от имени которого будет работать агент.

Если в системе уже есть пользователь с таким логином, работа агента будет проходить от его имени.

3.1.1.1 Автоинсталляция

Чтобы приступить к началу работы и настройке мониторинга, необходимо выполнить следующие действия:

1. Открыть web-интерфейс платформы "Центральный Пульс".
2. Ввести логин и пароль учётной записи с правами на управление объектами, свойствами и документами.

i Назначение прав пользователей описано в подразделе 3.7.4 "Назначение пользователям прав доступа" на стр. 117.

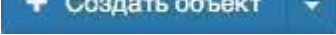
3. Создать объект-агент, для этого нажать кнопку  на панели инструментов, ввести имя объекта и выбрать класс **Saymon Agent**.
4. Навести курсор на созданный объект и нажать на появившуюся иконку - Настройки агента (Рис. 3.1.1.1.1):



Рис. 3.1.1.1.1. Мониторинговый агент

5. В появившемся окне скопировать ссылку из строки "Команда для установки агента" (Рис. 3.1.1.1.2):

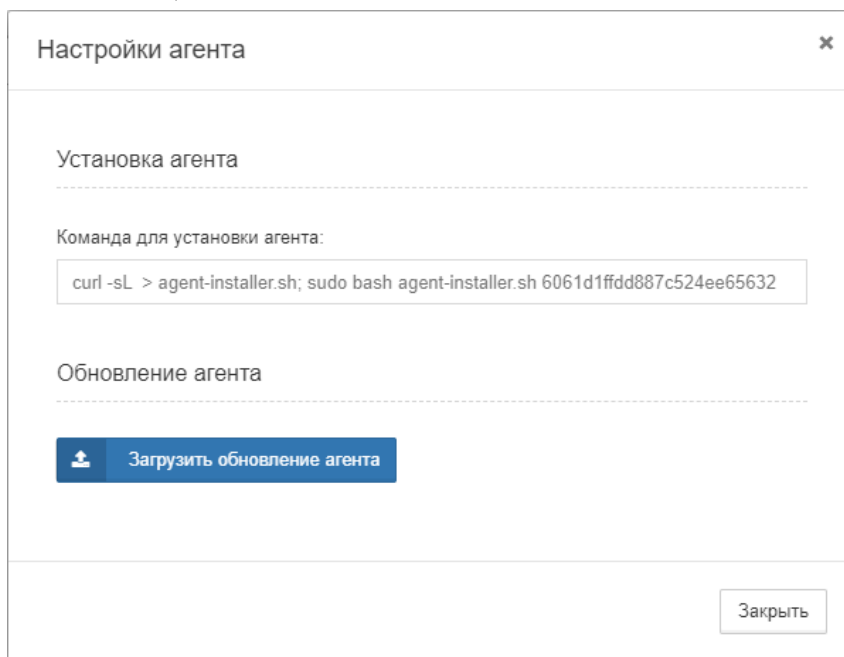
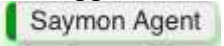


Рис. 3.1.1.1.2. Команда для установки агента

6. Выполнить эту команду в терминале на необходимом сервере.

i Номер, который дал сервер - последние 24 символа команды - совпадает с ID агента.


В течение 30 секунд агент скачивается и устанавливается. Если установка выполнена корректно, состояние агента в web-интерфейсе будет отражено зелёным цветом: .

3.1.1.2 Linux

Инструкция применима к операционным системам с менеджерами служб "systemd", "upstart" и "init.d", например:

- Ubuntu Linux;
- Red Hat Enterprise Linux;
- CentOS Linux;
- Debian 8 "Jessie" (для пользователей Raspberry Pi).

Если вы используете другого менеджера, пишите нам на care@saymon.info.

 При установке агента в системе автоматически создаётся пользователь **saymon**, от имени которого будет работать агент.
Если в системе уже есть пользователь с таким логином, работа агента будет проходить от его имени.

Для установки агента на Linux необходимо:

На хосте без доступа в Интернет:

1. [Скачать sh-скрипт установщика агента](#) для Linux 64bit или Linux 32bit.
2. Перенести скрипт на нужный хост в домашнюю директорию пользователя.
3. Сделать скрипт исполняемым:

64bit:

```
sudo chmod +x saymon-agent-rl-linux-x64-jre-installer.sh
```

32bit:

```
sudo chmod +x saymon-agent-rl-linux-i586-jre-installer.sh
```

4. Запустить скрипт:

64bit:

```
sudo ./saymon-agent-rl-linux-x64-jre-installer.sh
```

32bit:

```
sudo ./saymon-agent-rl-linux-i586-jre-installer.sh
```

5. Выполнить дальнейшие инструкции в терминале.

На хосте с доступом в Интернет:

1. Выполнить однострочник:

64bit:

```
curl https://saymon.info/downloads/saymon-agent-rl-linux-x64-jre-installer.sh -o saymon-agent-instal.sh ; chmod +x saymon-agent-instal.sh ; sudo ./saymon-agent-instal.sh
```

32bit:

```
curl https://saymon.info/downloads/saymon-agent-rl-linux-i586-jre-installer.sh -o saymon-agent-instal.sh ; chmod +x saymon-agent-instal.sh ; sudo ./saymon-agent-instal.sh
```

2. Выполнить дальнейшие инструкции в терминале.

Конфигурация агента выполняется в файле `/opt/saymon-agent/conf/agent.properties`.

3.1.1.3 Mac OS X

Для установки агента на Mac OS X необходимо:

1. Создать системного пользователя "Saymon agent", из-под которого будет запускаться агент.
2. [Скачать архив Mac OS X 64bit](#) и распаковать его в папку `/opt`.
3. Отредактировать файл конфигурации агента `saymon-agent/conf/agent.properties`.
4. Создать папку для хранения log-файлов:

```
sudo mkdir saymon-agent/log && sudo chown -R saymon:staff saymon-agent
```
5. При необходимости включить централизованное логирование агента через SYSLOG в файле `saymon-agent/conf/logback.xml`.
6. Сделать файл агента исполняемым:

```
sudo chmod +x saymon-agent/saymon-agent.sh
```
7. Запустить агента:

```
cd saymon-agent && sudo -u saymon ./saymon-agent.sh
```

3.1.1.4 Windows

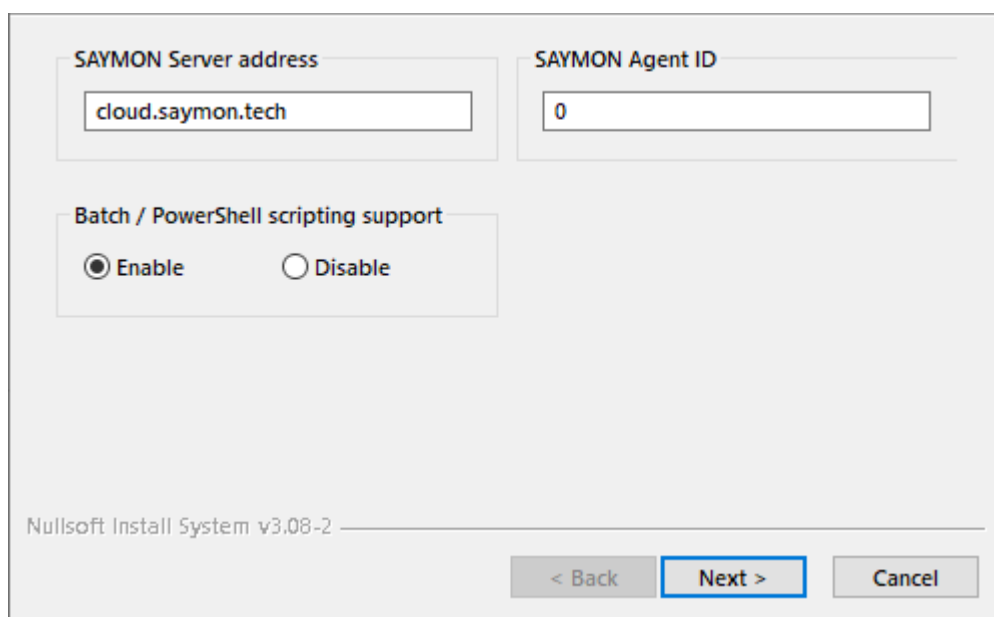
Для установки агента на Windows необходимо:

1. [Скачать инсталлятор](#) для Windows 64bit или Windows 32bit.
2. Запустить скачанный файл от имени администратора.
3. Выбрать папку установки (например, `C:\Program Files (x86)\SAYMON Agent`) и нажать кнопку **Install**.
4. После завершения установки нажать кнопку **Next**.
5. В открывшемся окне (Рис. 3.1.1.4.1):

указать адрес сервера,

указать ID агента,

при необходимости включить выполнение агентом скриптов;



The screenshot shows a standard Windows installation wizard window. It has a light gray background and a title bar. The main area contains three input fields: 'SAYMON Server address' with the text 'cloud.saymon.tech', 'SAYMON Agent ID' with the text '0', and a section for 'Batch / PowerShell scripting support' with two radio buttons, 'Enable' (selected) and 'Disable'. At the bottom, there are three buttons: '< Back' (disabled), 'Next >' (active/highlighted), and 'Cancel' (disabled). The text 'Nullsoft Install System v3.08-2' is visible at the bottom left of the window.

Рис. 3.1.1.4.1. Первичная настройка агента

и нажать кнопку **Next**.

6. В следующем окне (Рис. 3.1.1.4.2) отметить Start SAYMON Agent service и нажать кнопку **Finish**:

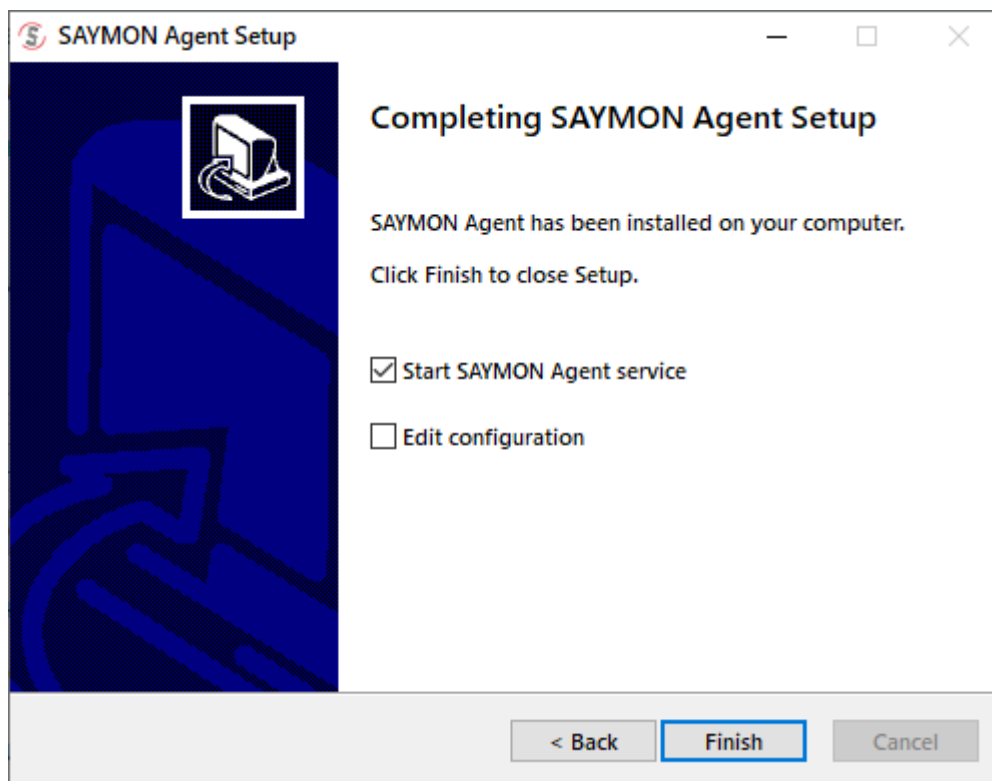


Рис. 3.1.1.4.2. Завершение установки агента

Конфигурационный файл агента хранится в папке установки агента из шага 3: `C:\Program Files (x86)\SAYMON Agent\conf\agent.properties`.

Работа агента успешно протестирована со следующими версиями ОС:

- Windows 7 SP1, 64 bit;
- Windows 7 SP1, 32 bit;
- Windows 10 22H2, 64 bit;
- Windows 10 22H2, 32 bit;
- Windows 10 Enterprise, 64 bit;
- Windows 10 Enterprise, 32 bit;
- Windows 11 Enterprise 22H2, 64 bit;
- Windows Server 2012 (R2 Datacenter), 64 bit;
- Windows Server 2016 (R2 Datacenter), 64 bit;
- Windows Server 2019, 64 bit;
- Windows Server 2022 (Standard Evaluation 21H2), 64 bit.

3.1.1.5 Wiren Board 6

Wiren Board 6 - это универсальный контроллер для автоматизации с открытым ПО на базе Linux. Предназначен для домашней и промышленной автоматизации и мониторинга: опроса датчиков и счетчиков, использования в качестве УСПД, в системах АСКУЭ, для замены ПЛК, а также в системах "умного дома".

Для установки агента на контроллер автоматизации Wiren Board 6 необходимо:

1. [Скачать архив с агентом](#).
2. Распаковать архив в папку `/opt/saymon-agent`.
3. [Скачать архив с JDK](#) (потребуется регистрация на сайте).
4. Распаковать архив в папку `temp`, оттуда полностью скопировать директорию `jre` в папку `/opt/saymon-agent`.
5. Выполнить следующие команды:

```
useradd -M -r -s /bin/false -K MAIL_DIR=/dev/null saymon
chown -R saymon:saymon /opt/saymon-agent
cp /opt/saymon-agent/systemd/* /etc/systemd/system
systemctl enable saymon-agent
service saymon-agent start
```

6. При необходимости отредактировать файл конфигурации агента `/opt/saymon-agent/conf/agent.properties`.

Благодарим за оказанную помощь пользователя [svdu](#) с [форума компании Wiren Board](#).

3.1.2 Конфигурация агента

Конфигурация агента выполняется в файле `.../saymon-agent/conf/agent.properties`.

Для применения изменений необходимо перезапустить службу **saymon-agent**.

Общие параметры конфигурационного файла агента (часть 1 из 2):

Параметр	Описание
agent.discoveryEnabled	<p>Включает автоматический поиск агентом сетевых устройств;</p> <ul style="list-style-type: none">• false - автоматический поиск выключен,• true - автоматический поиск включен. <p>По умолчанию - false - автоматический поиск выключен.</p> <p><i>Задать родительский объект для обнаруженных устройств можно с помощью параметра discovery_parent_id в секции Server конфигурационного файла сервера <code>/etc/saymon/saymon-server.conf</code>.</i></p>
agent.id	<p>Уникальный идентификатор объекта класса Saymon Agent в web-интерфейсе системы.</p> <p><i>При указании agent.id=0 на сервере будет создан новый объект класса Saymon Agent. По умолчанию агенты создаются в корневом объекте, задать родительский объект для создаваемых агентов можно с помощью параметра agent_registration_parent_id в секции Server конфигурационного файла сервера <code>/etc/saymon/saymon-server.conf</code>.</i></p> <p><i>ID созданного объекта будет передан агенту. На хосте с агентом будет создан файл <code>.../saymon-agent/storage/registration.json</code>, где будет записан данный идентификатор.</i></p> <p><i>Чтобы заново инициализировать процедуру получения ID, к примеру, если необходимо подключить агента к другому серверу, достаточно удалить файл <code>registration.json</code> и перезапустить агента.</i></p>
agent.scriptsEnabled	<p>Включает выполнение агентом скриптов с указанным текстом;</p> <ul style="list-style-type: none">• false - режим оптимизации выключен,• true - режим оптимизации включен. <p>По умолчанию - true - выполнение скриптов включено.</p>

Общие параметры конфигурационного файла агента (часть 2 из 2):

Параметр	Описание
agent.snmpTrapEnabled	Позволяет использовать агента в качестве получателя трапов; <ul style="list-style-type: none">• false - получение трапов агентом выключено,• true - получение трапов агентом включено. По умолчанию - false - получение трапов выключено.
agent.snmpTrapListenPort	Порт для получения трапов. По умолчанию - 1162 .
agent.snmpTrapReceiverThreadPoolSize	Количество одновременных потоков для получения трапов. По умолчанию - 4 .
metrics.buffer.in-memory.capacity	Включает буфер для сохранения данных от агента при отсутствии связи между агентом и сервером. Значение параметра - количество наборов данных от агента (результатов проверок), которые будут храниться в буфере до восстановления связи с сервером. После восстановления связи все данные из буфера пересылаются на сервер, и буфер очищается. При переполнении буфера очередные наборы данных заменяют наиболее старые из имеющихся в буфере. По умолчанию буфер выключен. <i>Функционал поддерживается агентами версии 4.5.72 и выше.</i>
server.host	Адрес сервера Kafka. По умолчанию - 127.0.0.1 .
server.port	Порт Kafka, по которому осуществляется подключение агентов к серверу. По умолчанию - 9092 .

3.1.2.1 Подключение к Kafka Cluster


При использовании Kafka Cluster необходимо также использовать дополнительные параметры подключения, начинающиеся на **kafka**.

Все возможные параметры представлены в [документации по Kafka](#).

Пример:

```
...
kafka.bootstrap.servers=localhost:9092
kafka.security.protocol=SASL_SSL
kafka.ssl.truststore.location=/opt/kafka/kafka.client.truststore.jks
kafka.ssl.truststore.password=saymon
kafka.sasl.mechanism=PLAIN
kafka.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required \
username="user" \
password="password"
...
```

kafka.bootstrap.servers - список пар хост:порт, использующихся для установки первоначального соединения с кластером Kafka.

 При использовании Kafka Cluster поле **server.host** не должно быть пустым, там необходимо указать адрес одного из **kafka.bootstrap.servers**.

Параметры конфигурационного файла агента для авторизации и шифрования:

Параметр	Описание
kafka.sasl.jaas.config	Параметры контекста входа в систему для SASL-соединений в формате, используемом конфигурационными файлами JAAS.
kafka.sasl.mechanism	Механизм SASL, используемый для клиентских подключений.
kafka.security.protocol	Протокол, используемый для взаимодействия с брокерами. Возможные значения: <ul style="list-style-type: none">• PLAINTEXT,• SSL,• SASL_PLAINTEXT,• SASL_SSL.
kafka.ssl.truststore.location	Расположение файла truststore .
kafka.ssl.truststore.password	Пароль для файла truststore . Если пароль не задан, сконфигурированный файл также будет использоваться, но без проверки целостности.

3.1.3 Конфигурация сервера

Конфигурация сервера системы выполняется в файле `/etc/saymon/saymon-server.conf`.

Для применения изменений необходимо перезапустить службу `saymon-server`:

```
sudo service saymon-server restart
```

Параметры конфигурационного файла сервера (часть 1 из 23):

Секция/Параметр	Описание
Agent_stat	<p>В этом разделе задаются настройки хранения истории данных от агента.</p> <pre>"agent_stat": { "write_to": "mongo", "default_ttl": 20, "ttl": [{ "key": "payload.cpuInformation.vendor", "value": "Intel", "expire": 10 }] }</pre>
agent_stat.write_to	<p>Выбор хранилища данных от агента.</p> <p>При указании значения "mongo" данные от агента хранятся в mongoDB.</p> <p>По умолчанию данные от агента хранятся в ELK.</p>
agent_stat.default_ttl	Срок жизни наборов данных (в секундах) по умолчанию.
Agent_stat.ttl	Сроки жизни наборов данных, для которых нужен срок жизни, отличающийся от принятого по умолчанию.
agent_stat.ttl.key	Имя метрики.
agent_stat.ttl.value	Значение метрики.
agent_stat.ttl.expire	Срок жизни набора данных.
Cache	<p>В этой секции задаются настройки сервера Redis.</p> <pre>"cache": { "host": "127.0.0.1", "port": 6379 }</pre>
cache.auth_pass	Пароль для доступа к серверу Redis.
cache.host	Адрес сервера Redis. По умолчанию - "127.0.0.1".
cache.port	Порт сервера Redis. По умолчанию - 6379.

Параметры конфигурационного файла сервера (часть 2 из 23):

Секция/Параметр	Описание
cache.cluster	<p>В этой подсекции задаются настройки при использовании Redis Cluster.</p> <pre>"cache": { "cluster": { "nodes": [{ "port": 7000, "host": "127.0.0.1" }, { "port": 7001, "host": "127.0.0.1" }] }, "options": {} }</pre> <p>Если задействована эта подсекция, система использует указанные здесь настройки подключения, параметры <i>cache.host</i> и <i>cache.port</i> игнорируются.</p>
cache.cluster.options	Дополнительные параметры подключения к кластеру.
cache.cluster.nodes	Серверы кластера, к которым необходимо подключиться.
cache.cluster.nodes.host	Адрес сервера кластера.
cache.cluster.nodes.port	Порт сервера кластера.
Custom_scripts	<p>В этой секции задаются настройки пользовательских скриптов, срабатывающих при создании и удалении объектов.</p> <pre>"custom_scripts": { "entity_triggers_path": "/opt/saymon-extensions/entity-triggers-path" }</pre>
custom_scripts. entity_triggers_path	Полный путь до папки с файлами скриптов.
DB	<p>В этом разделе задаются настройки подключения к базе данных для хранения объектной модели. В качестве базы данных используется MongoDB.</p> <pre>"db" : { "mongodb": { "url": "mongodb://localhost:27017/saymon?w=1" } }</pre>
db.mongodb	Данные для подключения к MongoDB.

Параметры конфигурационного файла сервера (часть 3 из 23):

Секция/Параметр	Описание
db.mongodb.url	<p>Адрес сервера MongoDB и дополнительные параметры подключения.</p> <p>По умолчанию - <code>"mongodb://localhost:27017/saymon?w=1"</code>.</p> <p>При использовании кластера из нескольких хостов их адреса указываются через запятую в произвольном порядке:</p> <pre>"url": "mongodb://host01:27017,host02:27017,host03:27017/saymon?w=1"</pre> <p>Все возможные дополнительные параметры URL представлены в документации по MongoDB.</p>
Elasticsearch	<p>В этой секции задаются настройки для работы с Elasticsearch.</p> <pre>"elasticsearch": { "node": "http://127.0.0.1:9200", "auth": { "username": "elastic", "password": "ypezA1ZoVv46fJh8Abj4" }, "index_pattern": "myindex*", "request_timeout": 30000, "hits_per_request": 1000 }</pre>
elasticsearch.hits_per_request	<p>Максимальное число записей, запрашиваемых в одном обращении к elasticsearch.</p> <p>По умолчанию - 1000.</p> <p>При повышении значения параметра снижается число запросов к Elasticsearch, но увеличивается расход памяти и время блокировки потока на сервере Центрального Пульта при обработке ответа.</p>
elasticsearch.index_pattern	Индекс Elasticsearch, в котором происходит поиск.
elasticsearch.node	IP-адрес инстанса Elasticsearch.
elasticsearch.request_timeout	<p>Время ожидания ответа от сервера elasticsearch (в миллисекундах).</p> <p>По умолчанию - 30000 - 30 секунд.</p>
elasticsearch.auth	Авторизационные данные пользователя elasticsearch.
elasticsearch.auth.password	Пароль пользователя elasticsearch.
elasticsearch.auth.username	Логин пользователя elasticsearch.

Параметры конфигурационного файла сервера (часть 4 из 23):

Секция/Параметр	Описание
Kafka	<p>В этой секции задаются настройки подключения к брокеру Kafka.</p> <pre data-bbox="544 349 1485 562">"kafka" : { "host" : "localhost", "port" : 9092, "requestTimeout" : 30000, "fetch_latest" : false, "logLevel" : 2 }</pre> <p>Помимо перечисленных здесь параметров, возможно также использовать дополнительные параметры подключения.</p>
kafka.brokers	<p>Пул адресов для подключения при использовании Kafka Cluster.</p> <pre data-bbox="544 739 1485 981">"kafka" : { ... "brokers": ["192.168.1.10:9092", "192.168.1.11:9092"], ... }</pre> <p>При указании данного параметра система игнорирует параметры kafka.host и kafka.port.</p> <p><i>При использовании Kafka Cluster необходимо дополнительно настроить конфигурационный файл агента. Подробнее в подразделе 3.1.2 "Конфигурация агента" на стр. 21 и части 3.1.2.1 "Подключение к Kafka Cluster" на стр. 23.</i></p>
kafka.fetch_latest	<p>Данный параметр определяет правило обработки сообщений, поступивших в Kafka при выключенной системе:</p> <ul data-bbox="592 1352 1222 1435" style="list-style-type: none"> • false - обработать накопленные данные, • true - игнорировать накопленные данные. <p>По умолчанию - false.</p>
kafka.host	<p>Адрес брокера Kafka.</p> <p>По умолчанию - "localhost".</p>
kafka.logLevel	<p>Уровень логирования Kafka;</p> <p>0 - NOTHING, 1 - ERROR, 2 - WARN, 4 - INFO, 5 - DEBUG.</p> <p>По умолчанию - 2 - WARN.</p>
kafka.port	<p>Порт брокера Kafka.</p> <p>По умолчанию - 9092.</p>

Параметры конфигурационного файла сервера (часть 5 из 23):

Секция/Параметр	Описание
kafka.requestTimeout	Время на ожидание ответа от брокера (в миллисекундах). По умолчанию - 30000 - 30 секунд.
kafka.ssl	Настройки шифрования . Ключ и сертификат можно указывать как путь к файлу: <pre>"kafka" : { ... "ssl": { "certFile": "/opt/kafka/for-saymon-server/cert.pem", "keyFile": "/opt/kafka/for-saymon-server/key.pem" }, ... }</pre>
kafka.sasl	Настройки аутентификации . Параметры зависят от механизма аутентификации, используемом в Kafka. Пример настроек для механизма PLAIN/SCRAM: <pre>"kafka" : { ... "sasl": { "mechanism": "plain", "username": "user", "password": "password" }, ... }</pre>
kafka.sasl.mechanism	Механизм аутентификации.
Keycloak	В этом разделе задаются параметры для взаимодействия с сервером Keycloak для авторизации пользователей. <pre>"keycloak": { "realm_certificate": "<данные из keycloak_realm_certificate>", "realm_certificate_file": "/etc/saymon/keycloak_realm_certificate", "config_file": "/etc/saymon/keycloak_backend.json" }</pre> <i>Параметры в примере перечислены в порядке понижения приоритета при одновременном указании. Для работы с Keycloak достаточно указать один из параметров.</i>
keycloak.config_file	Путь к файлу конфигурации, сгенерированному сервером Keycloak для Backend-клиента.
keycloak.realm_certificate	Данные сертификата (Realm Certificate), которым сервер Keycloak подписывает пользовательские токены.
keycloak.realm_certificate_file	Путь к файлу с Keycloak Realm Certificate.

Параметры конфигурационного файла сервера (часть 6 из 23):

Секция/Параметр	Описание
LDAP	<p>В этой секции задаются параметры внешнего LDAP-сервера для авторизации.</p> <pre data-bbox="563 387 1487 696"> "ldap" : { "url" : "ldaps://192.168.1.1:636", "suffix" : "dc=example,dc=com", "login" : "cn=admin,dc=example,dc=com", "pass" : "root", "allow_self_signed" : true, "create_user_for_existing_group_only": true, "import_non_existing_groups": false, "update_existing_groups": false } </pre>
ldap.allow_self_signed	<p>Разрешает соединение по LDAPs с сервером, на котором установлен самоподписанный SSL-сертификат;</p> <ul data-bbox="612 808 1070 887" style="list-style-type: none"> • false - соединение запрещено, • true - соединение разрешено. <p>По умолчанию - false - соединение запрещено.</p>
ldap.create_user_for_existing_group_only	<p>Ограничивает авторизацию новых LDAP-пользователей только теми пользователями, у которых имя группы на LDAP-сервере совпадает с именем существующей (созданной ранее) группы в Центральном Пульте:</p> <ul data-bbox="612 1137 1410 1328" style="list-style-type: none"> • false - разрешена авторизация всех новых LDAP-пользователей, • true - разрешена авторизация только тех новых LDAP-пользователей, для которых заготовлены группы в Центральном пульте. <p>По умолчанию - false - разрешена авторизация всех новых LDAP-пользователей.</p> <p><i>На LDAP-пользователей, у которых уже есть учётная запись, применение данного параметра не распространяется.</i></p>
ldap.group_name_attribute	<p>Атрибут, где хранятся имена групп пользователей.</p> <p>Указывается, если необходимо использовать не стандартный атрибут.</p> <p>Стандартный атрибут - cn.</p>

Параметры конфигурационного файла сервера (часть 7 из 23):

Секция/Параметр	Описание
ldap.import_non_existing_groups	<p>Разрешает автоматическое создание групп, в которых пользователь состоит на LDAP-сервере, но которых нет в Центральном Пульте:</p> <ul style="list-style-type: none"> • false - при авторизации LDAP-пользователя в Центральном Пульте не создаются новые группы; • true - при авторизации LDAP-пользователя создаются все его группы в Центральном Пульте, пользователь автоматически добавляется в свои группы. <p>По умолчанию - false - при авторизации LDAP-пользователей в Центральном Пульте не создаются новые группы.</p>
ldap.login	Логин администратора LDAP.
ldap.login_attribute_name	<p>Атрибут, где хранятся логины пользователей для входа в систему. Указывается, если необходимо использовать не стандартный атрибут.</p> <p>Стандартный атрибут - "name".</p>
ldap.pass	Пароль администратора LDAP.
ldap.suffix	Корневой элемент (как правило, доменное имя организации).
ldap.update_existing_groups	<p>Разрешает обновлять группы пользователей, созданные в Центральном Пульте, до LDAP-групп при импорте групп пользователя из LDAP и совпадении имен групп:</p> <ul style="list-style-type: none"> • false - при входе LDAP-пользователей обновления групп не происходит. • true - при входе LDAP-пользователя его группы в Центральном Пульте, совпадающие с группами в LDAP, обновляются до LDAP-групп. <p>По умолчанию - false - при входе LDAP-пользователей обновления групп не происходит.</p> <p>Для обновленной группы отключается возможность смены имени и добавляется источник - LDAP.</p>
ldap.url	Адрес LDAP-сервера. Поддерживаются протоколы LDAP и LDAPS .
Monitoring	<p>В этой секции задаются настройки пользовательских сенсоров мониторинга.</p> <pre>"monitoring": { "custom_tasks_path": "/opt/saymon-agent/custom_tasks" }</pre>
monitoring.custom_tasks_path	Полный путь до папки с файлами пользовательских проверок.

Параметры конфигурационного файла сервера (часть 8 из 23):

Секция/Параметр	Описание
MQTT	В этой секции задаются настройки подключения к MQTT-брокеру. <pre>"mqtt" : { "broker" : "mqtt://username:password@localhost:1883" }</pre>
mqtt.broker	Адрес и порт брокера. По умолчанию - "mqtt://localhost:1883" . <i>Для аутентификации по имени пользователя и паролю нужно указать пользовательские данные перед адресом сервера.</i>
OpenTSDB	В этой секции задаются параметры доступа к OpenTSDB.
openTsdB.enabled	Запись исторических данных в OpenTSDB; <ul style="list-style-type: none"> • false - запись выключена, • true - запись включена. По умолчанию - true - запись включена.
openTsdB.host	Адрес хоста с OpenTSDB. По умолчанию - "localhost" .
openTsdB.port	Порт OpenTSDB. По умолчанию - 4242 .
openTsdB.timeout	Время на ожидание ответа от OpenTSDB (в миллисекундах). По умолчанию - 15000 - 15 секунд.
Push_notification	В этой секции задаются параметры push-уведомлений в мобильном приложении. Для работы с ними используется Firebase Cloud Messaging (FCM).
push_notification.disabled	Выключает уведомления; <ul style="list-style-type: none"> • true - уведомления выключены, • false - уведомления включены. По умолчанию - true - уведомления выключены.
push_notification.key_path	Путь к ключу авторизации сервера Центрального Пульта на сервере Firebase. По умолчанию - "/etc/saymon/saymon-mobile-firebase-adminsdk.json" .

Параметры конфигурационного файла сервера (часть 9 из 23):

Секция/Параметр	Описание
push_notification.on_state_change	Включает отправку уведомления при изменении состояний на случай другого источника уведомлений - MQTT-сообщений. <ul style="list-style-type: none">• true - отправка включена,• false - отправка выключена. По умолчанию - true - отправка включена.
push_notification.timeout	Время, через которое каждому пользователю отправляется уведомление (в миллисекундах). По умолчанию - 0 - задержки нет.
push_notification.url	URL, полученный пользователем от Firebase, для принятия содержимого уведомлений с сервера. По умолчанию - "https://saymon-mobile.firebaseio.com" .
Resource_server	В этой секции задаются параметры, связанные с хранением файлов, загруженных в Центральный Пульт.
resource_server.debug	Включает debug-режим для логирования в файл <code>/var/log/saymon/saymon-server.log</code> ; <ul style="list-style-type: none">• false - режим выключен,• true - режим включен. По умолчанию - false - режим выключен.
resource_server.file_storage_dir	Путь к директории для хранения документов, прикрепляемых к объектам. По умолчанию - "/var/saymon/resources" .
resource_server.ip_address	Адрес Resource-сервера. По умолчанию - "127.0.0.1" .
resource_server.port	Порт Resource-сервера. По умолчанию - 8092 .
Rest_server	В этой секции задаются параметры REST-сервера.
rest_server.base_url	Путь к API. По умолчанию - "/api" .
rest_server.colorize_log	Включает цветную раскраску лога; <ul style="list-style-type: none">• false - раскраска выключена,• true - раскраска включена. По умолчанию - false - раскраска выключена.

Параметры конфигурационного файла сервера (часть 10 из 23):

Секция/Параметр	Описание
rest_server.debug	Включает debug-режим для логирования в файл <code>/var/log/saymon/saymon-server.log</code> ; <ul style="list-style-type: none">• false - режим выключен,• true - режим включен. По умолчанию - false - режим выключен.
rest_server.document_download_url	URL к файлам, сохраненным в <code>\$document_storage_dir</code> . По умолчанию - " http://localhost/node/api/docs ".
rest_server.ip_address	Адрес хоста для запуска REST-сервера. По умолчанию - " 127.0.0.1 ".
rest_server.keepAliveTimeout	Время ожидания сервером следующего запроса до разрыва текущего соединения (в миллисекундах). По умолчанию - 5000 - 5 секунд.
rest_server.num_workers	Число процессов для загрузки данных. По умолчанию - 1 .
rest_server.port	Порт REST-сервера. По умолчанию - 8090 .
rest_server.public_url	Адрес для доступа к web-интерфейсу из уведомлений.
rest_server.session_ttl	Время, по истечении которого происходит автоматическое завершение сессии при неактивности пользователя (в миллисекундах). По умолчанию - 3600000 - 1 час.
rest_server.snmp_mib_url	Адрес сервера трансляции SNMP OID в текстовый формат.
rest_server.update_download_url	Путь к файлу для обновления агента. По умолчанию - " http://localhost/node/api/agents/update ".

Параметры конфигурационного файла сервера (часть 11 из 23):

Секция/Параметр	Описание
rest_server.limits	<p>В этой подсекции задаются ограничения на число запросов к API.</p> <pre data-bbox="564 349 1477 1339">"limits" : [{ "__comment": "администратора не ограничиваем", "user": "5048c849d7b6e40593dfec71" }, { "__comment": "запросы на states и classes не ограничиваем", "uri": ["/states", "/classes"] }, { "__comment": "ограничиваем запросы на объекты", "uri": ["/objects"], "rate": "100/minute" }, { "__comment": "ограничиваем авторизовавшихся пользователей с 127.0.0.1", "user": true, "ip": '127.0.0.1', "rate": "120/minute" }, { "__comment": "ограничения для неавторизованных пользователей", "user": false, "rate": "10/minute" }]</pre> <p>По умолчанию ограничения не накладываются.</p> <p><i>Для каждого запроса поиск правил осуществляется сверху вниз. Применяется только одно правило.</i></p>

Параметры конфигурационного файла сервера (часть 12 из 23):

Секция/Параметр	Описание
rest_server.limits.group	<p>Группы пользователей, для которых устанавливается ограничение;</p> <ul style="list-style-type: none">• string string[] - ID группы или групп, к которым применяется правило. <p>Примеры:</p> <pre>"limits": [{ "group": "60e562277936944ebf158282", ... }]</pre> <pre>"limits": [{ "group": ["60e562277936944ebf158282", "616406e1a3db5948cd815438"], ... }]</pre>
rest_server.limits.ip	<p>IP-адреса, для которых устанавливается ограничение:</p> <ul style="list-style-type: none">• true - свой лимит для каждого IP-адреса;• string string[] - IP-адрес или список адресов, к которым применяется правило. <p>Примеры:</p> <pre>"limits": [{ "ip": true, ... }]</pre> <pre>"limits": [{ "ip": "127.0.0.1", ... }]</pre> <pre>"limits": [{ "ip": ["127.0.0.1", "192.168.1.2"], ... }]</pre>

Параметры конфигурационного файла сервера (часть 13 из 23):

Секция/Параметр	Описание
rest_server.limits.rate	<p>Количество запросов в единицу времени. Если не указано, то ограничение не накладывается.</p> <p>Задаётся в формате количество_запросов/единица_измерения_времени.</p> <p>Возможные единицы измерения времени:</p> <ul style="list-style-type: none"> y - год, Q - квартал, M - месяц, w - неделя, d - день, h - час, m/minute - минута, s - секунда, ms - миллисекунда. <p>Пример:</p> <pre>"limits": [{ "rate": 100/minute, ... }]</pre>
rest_server.limits.uri	<p>REST-методы, к которым устанавливается ограничение;</p> <ul style="list-style-type: none"> • true - свой лимит для каждого метода; • string string[] - метод или список методов, к которым применяется правило. <p>В качестве пути могут быть заданы любые API без приставки /node/api, например, "/time".</p> <p>Примеры:</p> <pre>"limits": [{ "uri": true, ... }]</pre> <pre>"limits": [{ "uri": "/ping", ... }]</pre> <pre>"limits": [{ "uri": ["/ping", "/node/api/objects:id/stat"], ... }]</pre>

Параметры конфигурационного файла сервера (часть 14 из 23):

Секция/Параметр	Описание
rest_server.limits.user	<p>Пользователи, для которых устанавливается ограничение;</p> <ul style="list-style-type: none"> • true - свой лимит для каждого авторизованного пользователя; • false - лимит по IP-адресу для каждого авторизованного пользователя; • string string[] - ID пользователя или пользователей, к которым применяется правило. <p>Примеры:</p> <pre>"limits": [{ "user": true, ... }]</pre> <pre>"limits": [{ "user": false, ... }]</pre> <pre>"limits": [{ "user": "6048c849d7b6e40593dfce71", ... }]</pre> <pre>"limits": [{ "user": ["57ff6853fa6db3a63d16d07b", "6048c849d7b6e40593dfce71"], ... }]</pre>
Server	В этой секции задаются общие параметры сервера.
server.agent_registration_parent_id	ID объекта, в котором появляются агенты при саморегистрации. По умолчанию - "1".
server.analytics_enabled	<p>Включает аналитику значений метрик в процесс обработки данных;</p> <ul style="list-style-type: none"> • false - аналитика выключена, • true - аналитика включена. <p>По умолчанию - false - аналитика выключена.</p>

Параметры конфигурационного файла сервера (часть 15 из 23):

Секция/Параметр	Описание
server.analytics_processes	Количество логических ядер, выделяемых для обработки аналитики временных рядов. По умолчанию используются все доступные ядра.
server.colorize_log	Включает цветную раскраску лога; <ul style="list-style-type: none">• false - раскраска выключена,• true - раскраска включена. По умолчанию - false - раскраска выключена.
server.comet_ping_interval	Временной интервал между отправками comet-сервером сообщений (в миллисекундах). По умолчанию - 5000 - 5 секунд.
server.comet_ping_timeout	Время ожидания сообщения от comet-сервера (в миллисекундах). По умолчанию - 12000 - 12 секунд.
server.comet_port	Порт для соединения. По умолчанию - 8091 .
server.comet_secure	Включает SSL-соединение; <ul style="list-style-type: none">• false - соединение выключено,• true - соединение включено. По умолчанию - false - соединение выключено.
server.comet_ssl_certificate	Путь к сертификату.
server.comet_ssl_key	Путь к ключу.
server.conditional_incidents_enabled	Включает функционал генерации аварий; <ul style="list-style-type: none">• false - функционал выключен,• true - функционал включен. По умолчанию - false - функционал выключен.
server.conditional_incidents_script	Путь до скрипта, выполняющегося при возникновении аварии. <i>Подробности описаны в подразделе 3.1.10 "Передача аварии в сторонние сервисы" на стр. 65.</i>
server.debug	Включает debug-режим для логирования в файл <code>/var/log/saymon/saymon-server.log</code> ; <ul style="list-style-type: none">• false - режим выключен,• true - режим включен. По умолчанию - false - режим выключен.

Параметры конфигурационного файла сервера (часть 16 из 23):

Секция/Параметр	Описание
server. default_result_timeout	<p>Время, через которое срабатывает условие Нет данных от объекта с момента создания объекта или получения последних данных (в миллисекундах).</p> <p>По умолчанию - 120000 - 2 минуты.</p>
server.default_state_id	<p>Состояние объекта по умолчанию.</p> <p>По умолчанию - 7 - NO DATA.</p>
server. discovery_parent_id	<p>ИД объекта, в котором появляются найденные агентами сетевые устройства.</p> <p>По умолчанию - "1".</p>
server. event_log_max_bytes	<p>Размер записей консоли в MongoDB, при достижении которого происходит ротация данных (в байтах).</p> <p>По умолчанию - "1 G" - 1 гигабайт.</p>
server.history_ temporary_storage_ period	<p>Интервал времени для буферизации метрик, по истечении которого все данные из Redis записываются в OpenTSDB (в миллисекундах).</p> <p>Применяется, только если history_update_period равен 0.</p>
server.history_update_ period	<p>Интервал записи исторических данных (в миллисекундах).</p> <p>0 - немедленная запись пришедших значений.</p> <p>По умолчанию - 60000 - 1 минута.</p>
server. history_write_length	<p>Ограничение количества точек в одном запросе к OpenTSDB. При указании этого параметра данные в базу записываются по частям.</p> <p>По умолчанию ограничения нет, запись данных в OpenTSDB происходит без разбиения на части.</p> <p><i>Функционал полезен при превышении размера записываемых за один раз данных. Рекомендуемое значение в таком случае - 100000.</i></p>
server. incident_timeout	<p>Время перехода аварии из списка активных аварий в список исторических аварий после погашения аварии (в миллисекундах).</p> <p>По умолчанию - 120000 - 2 минуты.</p>
server.notification_ buffering_period	<p>Период ожидания для сбора сообщений о смене состояний объектов и отправки группового уведомления (в миллисекундах).</p> <p>По умолчанию - 0 - буферизация отключена.</p> <p><i>Подробности об уведомлениях описаны в разделе 3.4 "Настройка уведомлений" на стр. 78.</i></p>

Параметры конфигурационного файла сервера (часть 17 из 23):

Секция/Параметр	Описание
server. retain_expired_stat	Включает хранение последних полученных данных после их устаревания; <ul style="list-style-type: none">• false - хранение выключено,• true - хранение включено. По умолчанию - false - хранение выключено.
server.script_ trigger_timeout	Максимальное время выполнения триггера (в миллисекундах). По умолчанию - 30000 - 30 секунд.
server.self_object_id	ID объекта, используемого для самомониторинга.
server.sms_script	Путь до скрипта, отправляющего SMS-уведомления.
server.stat_local_ timestamp_field_ name	Имя поля, где передается время, с которым нужно сохранять данные в OpenTSDB. По умолчанию - " localTimestamp ".
server. stat_scan_period	Период проверки актуальности пришедших данных (в миллисекундах). По умолчанию - 3000 - 3 секунды.
server. use_stat_timestamp	Сохраняет временную метку (поле timestamp) из данных агента; <ul style="list-style-type: none">• false - значение поля timestamp из данных агента заменяется на временную метку сервера,• true - используется значение поля timestamp из данных агента, оно не перезаписывается временем сервера. По умолчанию - false - временная метка из данных агента перезаписывается временем сервера.
server.voice_call_script	Путь до скрипта, осуществляющего голосовой вызов.

Параметры конфигурационного файла сервера (часть 18 из 23):

Секция/Параметр	Описание
server.email	<p>В этой подсекции задаются параметры доступа к почтовому серверу:</p> <pre>"email" : { "disabled" : false, "fields" : { "from" : "saymon@saas.saymon.info" }, "max_json_length": 1000, "transport" : { "auth" { "user" : "saymon@saas.saymon.info", "pass" : "P@ssw0rd" }, "host" : "smtp.gmail.com", "port" : 465, "secure" : true }, }</pre>
server.email.disabled	<p>Выключает отправку почтовых уведомлений;</p> <ul style="list-style-type: none"> • true - отправка выключена, • false - отправка включена. <p>По умолчанию - true - отправка выключена.</p>
server.email.max_json_length	<p>Ограничение размера письма с уведомлением (в символах). По умолчанию - 1000 - 1000 символов.</p>
server.email.fields	<p>Данные об отправителе уведомлений.</p>
server.email.fields.from	<p>Почтовый адрес отправителя.</p>
server.email.transport	<p>Данные почтового сервера.</p>
server.email.transport.host	<p>Адрес почтового сервера.</p>
server.email.transport.port	<p>Порт почтового сервера.</p>
server.email.transport.secure	<p>Включает использование TLS при подключении к серверу;</p> <ul style="list-style-type: none"> • false - использоване TLS выключено, • true - использоване TLS включено. <p>Значение по умолчанию зависит от порта.</p>
server.email.transport.service	<p>Встроенный в коннектор набор служб. При наличии задаёт host, port, secure автоматически. По умолчанию - "Gmail".</p>
server.email.transport.auth	<p>Данные для аутентификации пользователя.</p>

Параметры конфигурационного файла сервера (часть 19 из 23):

Секция/Параметр	Описание
server.email.transport.auth.pass	Пароль пользователя.
server.email.transport.auth.user	Логин пользователя.
server.user	<p>В этой подсекции задаются параметры пользователей:</p> <pre>"user" : { "auth_enabled": "true", "new_user_access": "all", "lang_default" : "ru", "template": { "permissions": ["manage-objects", "view-section-stat"], "objectPermissions": { "include": [], "exclude": ["5fb643ddf277b96c8401119b", "5f8dc28407e86603bfe281f8"] } }, "usersRoot": "5800d9aaac7bf0f90d3d520e" }</pre>
server.user.auth_enabled	<p>Включает самостоятельную регистрацию для пользователей;</p> <ul style="list-style-type: none"> • false - регистрация выключена, • true - регистрация включена. <p>По умолчанию - false - регистрация выключена.</p>
server.user.lang_default	<p>Язык пользователей по умолчанию;</p> <ul style="list-style-type: none"> • "en" - английский, • "it" - итальянский, • "ru" - русский. <p>По умолчанию - "en" - английский.</p>
server.user.new_user_access	<p>Права доступа к объектам для нового пользователя;</p> <ul style="list-style-type: none"> • "all" - есть доступ ко всем объектам, • "not" - нет доступа ни к одному объекту. <p>По умолчанию - "all" - доступ ко всем объектам.</p>
server.user.usersRoot	<p>Идентификатор корневого объекта для создаваемых новым пользователем объектов.</p> <p>По умолчанию - "1".</p>
server.user.template	<p>Шаблон прав нового пользователя.</p> <p>Данные параметры применяются только для пользователей, регистрирующихся самостоятельно.</p>

Параметры конфигурационного файла сервера (часть 20 из 23):

Секция/Параметр	Описание
server.user.template.permissions	Список прав на операции, доступных пользователю по умолчанию. <i>Список всех возможных прав доступен в Приложении А на стр.173.</i>
server.user.template.objectPermissions	Права пользователя на доступ к объектам.
server.user.template.objectPermissions.include	Список идентификаторов объектов, к которым пользователю по умолчанию доступ разрешён.
server.user.template.objectPermissions.exclude	Список идентификаторов объектов, к которым пользователю по умолчанию доступ запрещён.
SNMP	В этой секции задаются параметры обработки SNMP-трапов. <pre>"snmp": { "filter": "/users/admin/tmp/snmp-filter.js" }</pre>
snmp.filter	Путь к файлу с функцией фильтрации входящих SNMP Trap. Если функция возвращает значение false , сообщение отбрасывается. Пример функции фильтрации: <pre>module.exports = function(message, rawMessage) { rawMessage = String(rawMessage); // console.log(message, rawMessage); let filters = ['HLR Call Processing Message', 'AIR Rejected - No EPS Subscription', 'GPRS SIBB Processing Exception', 'AuC Call Processing Message', 'Received notification from CLIM', 'AuC Event Log Clean Up', 'SOFT 0006']; return !filters.some((filter) => rawMessage.includes(filter)); }</pre> Приведённый выше пример блокирует трапы, которые содержат любую строку, указанную в массиве <i>filters</i> .

Параметры конфигурационного файла сервера (часть 21 из 23):

Секция/Параметр	Описание
<p>Wetty</p>	<p>В этой секции задаются параметры логирования истории взаимодействия пользователей с системой через терминал Wetty. История каждой пользовательской сессии сохраняется в отдельный файл.</p> <p>Формат имени файла: YYYY-MM-DD_HH_MM_SS_PROTOCOL_IP_USERNAME.log, например, 2023-01-12_11-56-17_ssh_127.0.0.1_admin.log.</p> <pre>"wetty" : { "log_dir" : "/tmp", "raw_mode": true }</pre> <p>Если используется версия Центрального Пульта ниже 3.12.86, при переходе на новую версию необходимо:</p> <ol style="list-style-type: none"> Внести изменения в файл <code>/etc/nginx/sites-available/saymon</code>: <pre>location ~ /wetty/(.*) { # take path and query after wetty/ and append it to proxy_pass proxy_pass http://127.0.0.1:3001/wetty/\$1?\$query_string; proxy_http_version 1.1; proxy_set_header Upgrade \$http_upgrade; proxy_set_header Connection "upgrade"; }</pre> Перезапустить <code>nginx</code>: <pre>service nginx reload</pre>
<p>wetty.log_dir</p>	<p>Путь к папке для хранения log-файлов.</p>
<p>wetty.raw_mode</p>	<p>Включает режим записи логов с управляющими ANSI-символами;</p> <ul style="list-style-type: none"> • true - логи записываются с управляющими ANSI-символами; • false - логи записываются без управляющих ANSI-символов. <p>По умолчанию - true - логи записываются с ANSI-символами.</p>

Параметры конфигурационного файла сервера (часть 22 из 23):

Секция/Параметр	Описание
Zabbix	<p>В этой секции задаются параметры для импорта данных из системы Zabbix.</p> <pre data-bbox="564 387 1481 752">"zabbix" : [{ "url" : "http://192.168.1.215/zabbix/api_jsonrpc.php", "user" : "saymon", "password" : "saymon_user_password", "parent_id" : "58b586d5c3a2f96642e25537", "debug": true, "polling_period": 30000, "classes" : { "4" : "CPU", "619503be0ffb595aebe22222" : "Memory General" } }]</pre> <p><i>Подробности описаны в подразделе 3.5.1 "Интеграция с Zabbix" на стр. 84.</i></p>
zabbix.classes	<p>Массив соответствий идентификаторов классов и имён обнаруженных объектов. Объектам с указанными именами будут при создании присвоены соответствующие классы.</p>
zabbix.debug	<p>Включает вывод параметров и результатов запросов в лог;</p> <ul style="list-style-type: none"> • false - вывод выключен, • true - вывод включен. <p>По умолчанию - false - вывод выключен.</p>
zabbix.parent_id	<p>ID объекта, используемого в качестве родителя для объектов, импортируемых из Zabbix.</p>
zabbix.password	<p>Пароль пользователя Zabbix с правами на чтение хостов или групп хостов, данные с которых необходимо импортировать.</p>
zabbix.polling_period	<p>Период обновления данных (в миллисекундах).</p> <p>По умолчанию - 120000 - 2 минуты.</p>
zabbix.url	<p>Адрес файла <code>api_jsonrpc.php</code> требуемой инсталляции Zabbix.</p>
zabbix.user	<p>Имя пользователя Zabbix с правами на чтение хостов или групп хостов, данные с которых необходимо импортировать.</p>

Параметры конфигурационного файла сервера (часть 23 из 23):

Секция/Параметр	Описание
zabbix. request_options	<p>В этой подсекции можно задать изменения опций для запросов хостов, триггеров и данных.</p> <pre data-bbox="603 387 1485 909"> "request_options": { "hosts": { "filter": { ... } }, "triggers": { "filter": { ... } }, "data": { "filter": { ... } } } </pre>
zabbix.request_options.hosts	Параметры для запроса хостов.
zabbix.request_options.hosts.filter	<p>Поля фильтров для запроса хостов.</p> <p>Все возможные поля фильтров hosts представлены в документации по Zabbix API.</p>
zabbix.request_options.triggers	Параметры для запроса триггеров.
zabbix.request_options.triggers.filter	<p>Поля фильтров для запроса триггеров.</p> <p>Все возможные поля фильтров triggers представлены в документации по Zabbix API.</p>
zabbix.request_options.data	Параметры для запроса данных.
zabbix.request_options.data.filter	<p>Поля фильтров для запроса данных.</p> <p>Все возможные поля фильтров data представлены в документации по Zabbix API.</p>

Управление некоторыми настройками доступно в web-интерфейсе системы:

1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
2. Перейти в раздел "Опции конфигурации".

Изменённые параметры в интерфейсе приоритетнее настроек в конфигурационном файле.

Установленные значения параметров автоматически сохраняются в MongoDB, конфигурационный файл не перезаписывается.

Раздел "Опции конфигурации" окна конфигурации системы состоит из подразделов:

1. "Общие настройки" соответствуют параметрам секции **Server** (Рис. 3.1.3.1):

Общие настройки

Сохранять устаревшие данные от агента НЕТ

Период обновления истории, мс

Период обновления таблицы состояний, мс

Период проверки устаревания данных от агента, мс

Период обработки пассивных данных от агента, мс

Максимальный размер журнала событий, байты

Срок действия данных от агента по умолчанию, мс

Таймаут погашенной аварии, мс

Рис. 3.1.3.1. Общие настройки

2. "Настройки электронной почты" соответствуют параметрам подсекции **Server.Email** (Рис. 3.1.3.2):

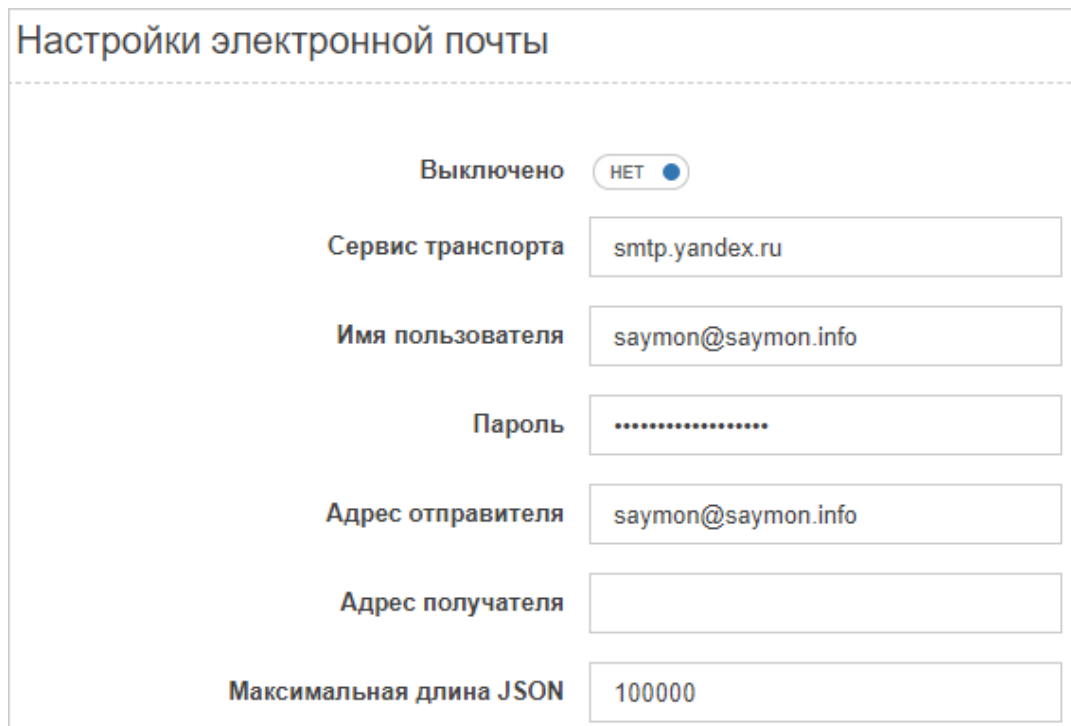


Рис. 3.1.3.2. Настройки электронной почты

3. "Настройки пользователей" соответствуют параметрам подсекции **Server.User** (Рис. 3.1.3.3):

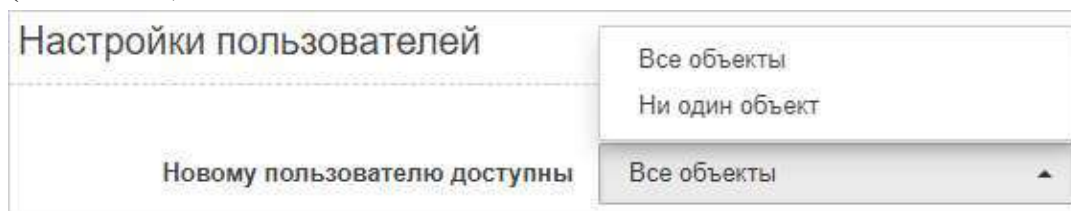


Рис. 3.1.3.3. Настройки пользователей

Просмотреть актуальные настройки сервера возможно при помощи REST API метода:


```
GET /node/api/configuration
```

Пример (bash):

```
login=<...>  
password=<...>  
saymon_hostname=<...>  
url=https://$saymon_hostname/node/api/configuration  
  
curl -X GET $url -u $login:$password
```

3.1.4 Настройка элементов web-интерфейса

Некоторые элементы web-интерфейса можно настроить в конфигурационном файле клиента `/etc/saymon/saymon-client.yaml`.

 *Настройки конфигурации клиента могут храниться в (в порядке снижения приоритета):*

- *MongoDB - настройки, измененные через rest-api;*
- `/etc/saymon/saymon-client.yaml` - конфигурация клиента в формате `yaml`;
- `/etc/saymon/saymon-client.yml` - конфигурация клиента в формате `yaml` (с расширением `yml`);
- `/etc/saymon/saymon-client.json` - конфигурация клиента в формате `json`;
- `/etc/saymon/client-config.js` - конфигурация клиента в старом формате;
- `./backend/server/saymon-client.yaml` - конфигурация клиента с настройками по умолчанию.

Примеры настроек приведены для файла `saymon-client.yaml`.

Параметры конфигурационного файла клиента (часть 1 из 11):

Секция/Параметр	Описание
<code>agentInstallerUrl</code>	Ссылка для скачивания установочного скрипта для агента.
<code>authEnabled</code>	Включает самостоятельную регистрацию для пользователей; <ul style="list-style-type: none"> • <code>false</code> - регистрация выключена, • <code>true</code> - регистрация включена. По умолчанию - false - регистрация выключена.
Authentication	В этой секции можно настроить методы аутентификации пользователей. <pre> authentication: availableMethods: - native - keycloak methodByDefault: keycloak services: keycloak: configUri: keycloak_frontend.json legacySupport: false </pre>
<code>authentication.availableMethods</code>	Список доступных для пользователей методов аутентификации: <ul style="list-style-type: none"> • native - вход по логину и паролю непосредственно на сервере Центрального Пульта; • keycloak - вход с использованием внешнего Keycloak-сервера. По умолчанию используется только native .

Параметры конфигурационного файла клиента (часть 2 из 11):

Секция/Параметр	Описание
authentication. methodByDefault	Метод аутентификации, предлагаемый пользователю при отображении формы аутентификации. По умолчанию - native .
authentication.services	Секция с настройками сервисов аутентификации.
authentication.services. keycloak	Секция с настройками аутентификации через Keycloak.
authentication.services. keycloak.configUri	Название файла настроек соединения, сгенерированного Keycloak-сервером для Frontend-клиента. <i>Файл необходимо разместить на сервере Центрального Пульта в каталоге <code>/etc/saymon</code>.</i>
authentication.services. keycloak.legacySupport	Включает поддержку работы с Keycloak-сервером версии ниже 19; <ul style="list-style-type: none">• false - поддержка работы с Keycloak-сервером версии ниже 19 выключена;• true - поддержка работы с Keycloak-сервером версии ниже 19 включена. По умолчанию - false - работа с Keycloak-сервером версии ниже 19 не поддерживается.
canEditObjectStyle	Включает возможность вручную настраивать CSS-стили для объектов и связей. При включении опции в разделе Параметры появляется подраздел Стили ; <ul style="list-style-type: none">• false - настройка стилей выключена,• true - настройка стилей включена. По умолчанию - true - настройка стилей включена.
collapseSections	Задаёт способ первоначального отображения секций и графиков; <ul style="list-style-type: none">• false – секции закреплены, графики раскрыты,• true – секции откреплены, графики свёрнуты. По умолчанию - true - секции откреплены, графики свёрнуты.

Параметры конфигурационного файла клиента (часть 3 из 11):

Секция/Параметр	Описание
Comet	Наряду с REST API, Центральный Пульт использует модель Comet для обмена данными между клиентом и сервером. <pre>comet: port: 8091 url: - "https://cpult.ru/ws" - "http://10.78.5.11:8092"</pre>
comet.port	Номер порта, по которому клиент подключается к Comet-серверу. По умолчанию - 8091 .
comet.url	Адреса для подключения клиентов к Comet-серверу из разных подсетей. <i>Параметр comet.port игнорируется при использовании параметра comet.url.</i>
DefaultClassImage	Позволяет задать стандартное изображение и его размер для объектов определённого класса. <pre>defaultClassImage: "29": img: /images/cloud.svg dim: - 100 - 75</pre>
defaultClassImage.<number>	Идентификатор класса, например, "29".
defaultClassImage.<number>.img	Путь до изображения относительно папки, где находится конфигурационный файл.
defaultClassImage.<number>.dim	Размер изображения (в пикселях, [ширина, высота]).
DefaultEmbeddableLink	Позволяет встраивать виджеты с информацией об объектах на сторонние ресурсы. <pre>defaultEmbeddableLink: url: http://saymon.info/ name: SAYMON</pre>
defaultEmbeddableLink.name	Имя виджета.
defaultEmbeddableLink.url	URL, на который ведёт виджет.

Параметры конфигурационного файла клиента (часть 4 из 11):

Секция/Параметр	Описание
defaultPieChartColors	<p>Цвета секторов по умолчанию для круговой диаграммы.</p> <pre>defaultPieChartColors: - "#a90329" - "#3276b1" - "#009F3D" - "#9868B8" - "#F2C001" - "#FF742C" - "#90574E" - "#EB77BE" - "#FF9796" - "#AAC6E5" - "#8BDE90" - "#FDB5D0"</pre>
disabledSections	<p>Позволяет удалить секции, которые показываются при подробном отображении объекта в верхней части экрана.</p> <p>Список всех доступных секций:</p> <ul style="list-style-type: none">• audit-log (История изменений),• config-log (Изменения конфигурации),• documents (Документы),• entity-incident-conditions (Условия генерации аварий),• entity-settings (Параметры),• entity-state-conditions (Условия перехода состояний),• history-graph (Графики),• monitoring (Мониторинг),• operations (Операции),• properties (Свойства),• stat (Данные),• stat-rules (Правила формирования данных),• state-history (История состояний),• state-triggers (Действия при смене состояний),• widgets (Виджеты).

Параметры конфигурационного файла клиента (часть 5 из 11):

Секция/Параметр	Описание
Documentation	<p>В этой секции можно настроить ссылки на различную документацию для Центрального Пульта.</p> <pre>documentation: main: root: https://wiki.saymon.info/display/SAYMONEN ru: https://wiki.saymon.info notificationTemplates: root: https://wiki.saymon.info/display/SAYMONEN/Notification+templates ru: https://wiki.saymon.info/pages/viewpage.action?pageId=45385140 restApi: root: https://api.saymon.tech</pre>
documentation.main	Ссылки на пользовательскую документацию.
documentation.main.root	Ссылка на англоязычную документацию.
documentation.main.ru	Ссылка на русскоязычную документацию.
documentation.notificationTemplates	Ссылки на шаблоны оповещений.
documentation.notificationTemplates.root	Ссылка на англоязычные шаблоны оповещений.
documentation.notificationTemplates.ru	Ссылка на русскоязычные шаблоны оповещений.
documentation.restApi	Ссылки на документацию по REST API.
documentation.restApi.root	Ссылка на документацию по REST API.
enableAnalytics	<p>Включает функционал модуля аналитики;</p> <ul style="list-style-type: none"> • false - функционал выключен, • true - функционал включен. <p>По умолчанию - false - функционал выключен.</p>
enableConditionalIncidents	<p>Включает функционал генерации аварий;</p> <ul style="list-style-type: none"> • false - функционал выключен, • true - функционал включен. <p>По умолчанию - false - функционал выключен.</p>
enableSmsTrigger	<p>Включает использование SMS-уведомлений;</p> <ul style="list-style-type: none"> • false - SMS-уведомления выключены, • true - SMS-уведомления включены. <p>По умолчанию - false - SMS-уведомления выключены.</p>

Параметры конфигурационного файла клиента (часть 6 из 11):

Секция/Параметр	Описание
enableSnmpTranslate	<p>Включает трансляцию SNMP OID в текстовый формат;</p> <ul style="list-style-type: none"> • false - трансляция выключена, • true - трансляция включена. <p>По умолчанию - false - трансляция выключена.</p>
enableVoiceCallTrigger	<p>Включает использование голосовых вызовов;</p> <ul style="list-style-type: none"> • false - голосовые вызовы выключены, • true - голосовые вызовы включены. <p>По умолчанию - false - голосовые вызовы выключены.</p>
ForceEmptyStandardView	<p>При выборе объекта, в том числе не содержащего вложенных объектов, Центральный Пульт по умолчанию показывает для него подробную информацию.</p> <p>В параметре задаётся список идентификаторов классов, при выборе пустых объектов которых Центральный Пульт переходит в стандартный вид.</p> <p>По умолчанию:</p> <ul style="list-style-type: none"> • 1 (Root), • 3 (Host), • 13 (Node), • 43 (Dashboard).
GeoMap	<p>Центральный Пульт позволяет привязывать объекты к их геоположению и просматривать их на карте.</p> <pre> geoMap: serverName: openstreetmap.org initialPosition: - 30.341306 - 59.930089 initialZoom: 8 </pre>
geoMap.initialPosition	<p>Начальная позиция на карте в формате [долгота, широта].</p> <p>По умолчанию - Россия, Санкт-Петербург.</p>
geoMap.initialZoom	<p>Начальный масштаб карты.</p> <p>По умолчанию - 8.</p>
geoMap.serverName	<p>Имя сервера, отвечающего за отображения карты.</p> <p>По умолчанию - openstreetmap.org.</p> <p>Также можно использовать локальный OSM-сервер.</p>






Параметры конфигурационного файла клиента (часть 7 из 11):

Секция/Параметр	Описание
Grid	<p>В этой секции задаются настройки сетки для выравнивания объектов в стандартном виде.</p> <pre>grid: dim: 20 color: rgba(128, 128, 128, 0.3) border: 4</pre>
grid.border	<p>Максимальное значение отступа границы объекта от границы сетки (в пикселях).</p> <p>По умолчанию - 4.</p>
grid.color	<p>Цвет сетки в формате RGBA.</p> <p>По умолчанию - rgba(128, 128, 128, 0.3).</p>
grid.dim	<p>Размер сетки (в пикселях).</p> <p>По умолчанию - 20.</p>
GridView	<p>В этой секции задаются параметры отображения объектов в виде сетки.</p> <pre>gridView: cols: 6 colWidth: 240 rowHeight: 90 gutterSize: 5</pre>
gridView.cols	<p>Количество объектов в строке сетки.</p> <p>При gridView.cols > 0 ширина объектов меняется автоматически.</p> <p>При gridView.cols = 0 число объектов в строке сетки подстраивается под ширину экрана.</p> <p>По умолчанию - 6.</p>
gridView.colWidth	<p>Ширина объектов при gridView.cols = 0 (в пикселях).</p> <p>По умолчанию - 240.</p>
gridView.gutterSize	<p>Величина отступа между объектами (в пикселях).</p> <p>По умолчанию - 5.</p>
gridView.rowHeight	<p>Высота объектов (в пикселях).</p> <p>По умолчанию - 90.</p>

Параметры конфигурационного файла клиента (часть 8 из 11):

Секция/Параметр	Описание
hideConnectionStatusNotifications	<p>Скрывает оповещения о статусе соединения с Comet-сервером;</p> <ul style="list-style-type: none"> • false - оповещения выводятся в web-интерфейс, • true - оповещения выводятся в консоль. <p>По умолчанию - false - оповещения о статусе соединения с Comet-сервером выводятся в web-интерфейс.</p>
hideResponseErrorNotifications	<p>Скрывает оповещения об ошибках, возникающих при отправке автоматических запросов на сервер;</p> <ul style="list-style-type: none"> • false - оповещения выводятся в web-интерфейс, • true - оповещения скрыты. <p>По умолчанию - false - оповещения выводятся в web-интерфейс.</p> <p><i>Ошибки, возникающие при участии пользователя, например сохранение каких-либо данных в формах, будут выводиться в web-интерфейс в любом случае.</i></p>
History	<p>В этой секции задаются параметры, отвечающие за отображение данных на графиках, а также активируются некоторые дополнительные элементы интерфейса.</p> <pre> history: slider: false, downsampling: - period: 1-hours dsp: 15s-avg - period: 1-days dsp: 5m-avg - period: 1-weeks dsp: 1h-avg - dsp: 1d-avg modelChangeAnnotations: false </pre>
history.downsampling	<p>Параметры уменьшения размера выборки данных - downsampling.</p>
history.modelChangeAnnotations	<p>Включает смену аннотаций на графиках;</p> <ul style="list-style-type: none"> • false - смена аннотаций выключена, • true - смена аннотаций включена. <p>По умолчанию - false - смена аннотаций выключена.</p>
history.slider	<p>Включает ползунок, который используется для задания интервала времени отображения данных;</p> <ul style="list-style-type: none"> • false - ползунок выключен, • true - ползунок включен. <p>По умолчанию - false - ползунок выключен.</p>

Параметры конфигурационного файла клиента (часть 9 из 11):

Секция/Параметр	Описание
Incidents	<p>В этой секции настраиваются дополнительные поля для списков активных аварий и исторических аварий.</p> <pre>incidents: additionalFields: - properties.address, additionalFieldNames: - IP-address</pre>
incidents. additionalFieldNames	Имена дополнительных полей, отображаемые в интерфейсе.
incidents.additionalFields	Источники данных для дополнительных полей.
Languages	<p>В этой секции происходит управление предустановленными языками web-интерфейса.</p> <pre>languages: en: short: us long: English ru: short: ru long: Русский it: short: it long: Italiano</pre>
languages.<id>	<p>Идентификатор языка. Доступны три языка:</p> <ul style="list-style-type: none"> • en - английский, • it - итальянский, • ru - русский.
languages.<id>.long	<p>Полное название языка.</p> <p>Это название отображается в меню текущего пользователя Центрального Пульта при выборе языка интерфейса.</p>
languages.<id>.short	<p>Идентификатор иконки флага.</p> <p>Иконка отображается в меню текущего пользователя Центрального Пульта при выборе языка интерфейса.</p>  - es,  - gb,  - it,  - ru,  - us.

Параметры конфигурационного файла клиента (часть 10 из 11):

Секция/Параметр	Описание
millisecondMonitoring	<p>Включает обновление данных каждую миллисекунду;</p> <ul style="list-style-type: none"> • false - обновление выключено, • true - обновление включено. <p>По умолчанию - false - обновление выключено.</p>
Monitoring	<p>В этой секции настраивается скрытие стандартных мониторинговых сенсоров из интерфейса.</p> <pre>monitoring: standardTasks: - ping - snmpGet</pre> <p><i>Механизм скрытия стандартных сенсоров описан в подразделе 3.3.1 "Скрытие неиспользуемых сенсоров" на стр. 75.</i></p>
monitoring.standardTasks	<p>Массив идентификаторов отображаемых стандартных сенсоров.</p>
pollInterval	<p>Интервал между запросами данных с REST-сервера, если соединение между клиентом и Comet-сервером недоступно (в миллисекундах).</p> <p>По умолчанию - 5000 - 5 секунд.</p>
pollIntervalSocket	<p>Интервал между запросами данных с Comet-сервера, если соединение между клиентом и Comet-сервером доступно (в миллисекундах).</p> <p>По умолчанию - 60000 - 1 минута.</p>
title	<p>Заголовок для вкладок, а также имя, отображаемое в левом верхнем углу web-интерфейса.</p> <p>По умолчанию - SAYMON.</p>
Tree	<p>В этом разделе задаются настройки для дерева объектов.</p> <pre>tree: filterSubmit: true</pre>
tree.filterSubmit	<p>Включает кнопку применения фильтра и отключает его автоматическое применение при вводе символов;</p> <ul style="list-style-type: none"> • false - кнопка выключена, • true - кнопка включена. <p>По умолчанию - false - кнопка выключена.</p>

Параметры конфигурационного файла клиента (часть 11 из 11):

Секция/Параметр	Описание
themes	<p>Этот параметр отвечает за настройку тем.</p> <p>По умолчанию используется тема Light. Также доступна тема Dark.</p> <p>CSS-файлы с темами находятся в директории <code>\$\$SAYMON_ROOT/target/client/css</code>.</p> <p><code>\$\$SAYMON_ROOT</code> - директория, где установлен Центральный Пульт.</p> <pre>themes: default: name: Light dark: name: Dark</pre>
useNaturalSort	<p>Включает сортировку объектов с помощью библиотеки javascript-natural-sort:</p> <ul style="list-style-type: none">• <code>false</code> - объекты сортируются с помощью нативных функций браузера,• <code>true</code> - объекты сортируются с помощью библиотеки javascript-natural-sort. <p>По умолчанию - false - объекты сортируются с помощью нативных функций браузера.</p> <p><i>При установленном <code>useNaturalSort = true</code> возможно замедление работы web-интерфейса при большом количестве объектов в системе (от 100 000).</i></p>

3.1.5 Служба "saymon-server"

Узнать состояние, запустить, перезапустить и остановить службу сервера можно следующими командами соответственно:

```
sudo service saymon-server status  
sudo service saymon-server start  
sudo service saymon-server restart  
sudo service saymon-server stop
```

3.1.6 Просмотр websocket-нотификаций

Центральный пульт использует гибкий механизм оповещений, который позволяет пользователю оперативно реагировать на возникающие ситуации.

Чтобы просмотреть пришедшие websocket-уведомления, необходимо:

1. Запустить Chrome.
2. Авторизоваться на сервере Центрального Пульта.
3. Перейти по ссылке `https://<your_server>/incidents.html?debug=comet`
4. Открыть в Chrome Инструменты разработчика.
5. Открыть вкладку Консоль (Console) в Инструментах разработчика.
6. В качестве примера нажать правой кнопкой мыши на строке с аварией и выбрать пункт "Подтвердить".

В консоли отобразится websocket-нотификация.

3.1.7 Увеличение количества обработчиков SNMP-Trap

Для поддержания бесперебойного наблюдения за объектами и оповещения администратора Центральный Пульт использует SNMP-Trap.

Если на сервер поступает большое количество SNMP-Trap, то возможно увеличить количество их обработчиков. Для этого необходимо:

1. Открыть в текстовом редакторе файл настроек акторов:

```
sudo nano /usr/local/saymon/backend/server/actors.json
```

2. Добавить следующую секцию:

```
"snmpTrapMessageHandlerActor": {  
  "mode": "forked",  
  "clusterSize": 3,  
  "onCrash": "respawn"  
}
```

3. Перезапустить сервер:

```
sudo service saymon-server restart
```

Для проверки корректности выполненной операции необходимо выполнить команду:

```
ps ax | grep node
```

В выводе должно отображаться число процессов **SnmptTrapMessageHandlerActor**, которое было указано в параметре **clusterSize** выше (в этом примере - 3):

```
5793 ? Rsl 10:23 /usr/bin/nodejs --  
harmony /usr/local/saymon/backend/server/saymon-server.js  
  
5857 ? Sl 3:18 /opt/nodejs/bin/node --  
harmony /usr/local/saymon/backend/server/actors/forked-actor-worker.js RestServerActor  
  
5862 ? Sl 0:37 /opt/nodejs/bin/node --  
harmony /usr/local/saymon/backend/server/actors/forked-actor-worker.js  
ResourceServerActor  
  
5867 ? Sl 1:43 /opt/nodejs/bin/node --  
harmony /usr/local/saymon/backend/server/actors/forked-actor-worker.js  
HistoryWriterActor  
  
5872 ? Sl 0:45 /opt/nodejs/bin/node --  
harmony /usr/local/saymon/backend/server/actors/forked-actor-worker.js  
SnmptTrapMessageHandlerActor  
  
5877 ? Sl 0:42 /opt/nodejs/bin/node --  
harmony /usr/local/saymon/backend/server/actors/forked-actor-worker.js  
SnmptTrapMessageHandlerActor  
  
5882 ? Sl 0:42 /opt/nodejs/bin/node --  
harmony /usr/local/saymon/backend/server/actors/forked-actor-worker.js  
SnmptTrapMessageHandlerActor
```

3.1.8 Сброс системы к заводским настройкам

Администратор может в любой момент сбросить настройки Центрального Пульта, чтобы восстановить настройки по умолчанию.

Для этого необходимо выполнить следующий скрипт:

```
#!/bin/bash
#
#Script deletes instance-specific data from MongoDB, Redis and OpenTSDB.
# Let's stop SAYMON Server and begin.
service saymon-server stop

mongo saymon --eval 'db.dropDatabase()'

echo flushall | redis-cli

docker stop opentsdb
docker rm opentsdb
docker run -d -p 127.0.0.1:4242:4242 --restart=always --name=opentsdb
rossinno/opentsdb

# Purges logs also.
rm /var/log/saymon/* /var/log/nginx/saymon*

# Forward to new monitoring adventures!
service saymon-server start
```


3.1.9 Включение функционала генерации аварий

Функционал генерации аварий опционален и выключен по умолчанию. Для его активации необходимо:

1. В секции **Server** конфигурационного файла сервера `/etc/saymon/saymon-server.conf` установить параметру **conditional_incidents_enabled** значение **true**:

```
{  
  ...  
  "server" : {  
    ...  
    "conditional_incidents_enabled ": true,  
  },  
  ...  
}
```

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

2. В конфигурационном файле клиента `/etc/saymon/saymon-client.yaml` установить параметру **enableConditionallncidents** значение **true**:

```
enableConditionallncidents: true
```

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

3.1.10 Передача аварий в сторонние сервисы

Для передачи аварийных сообщений в системы верхнего уровня необходимо выполнить следующие действия:

1. Включить функционал генерации аварий в секции **Server** конфигурационного файла сервера `/etc/saymon/saymon-server.conf` и там же указать путь к скрипту, который будет отправлять данные:

```
"server" : {  
  "conditional_incidents_enabled" : true,  
  "conditional_incidents_script": "/home/saymon/scripts/send_incident.sh",  
  ...  
}
```

2. Добавить в MongoDB триггеры по авариям для классов или отдельных объектов:

```
mongo saymon  
  
db.incidentTriggers.insert({ "ownerId" : 1042, "ownerType" : 4, "body" : [ {  
  "type" : "conditional_incidents_script", "payload" : { }, "states" : [ 1,2,4 ] } ] })
```

где

- `ownerId` - идентификатор сущности, к которой добавляется триггер;
- `ownerType` - тип сущности, для которой добавляется триггер (4 - класс, 1 - объект);
- `states` - уровень критичности аварий, при которых запускается триггер.

В указанном выше примере скрипт триггера будет вызываться при возникновении аварии любой критичности у объектов класса 1042.

В скрипт передается два аргумента:


- `$1` - тело аварии;
- `$2` - свойства объекта, к которому относится авария.

3.1.11 Работа со свойствами аварий

Добавить/изменить или удалить свойства аварий можно с помощью REST API.

При желании можно добавлять в списки активных и исторических аварий дополнительные поля из свойств аварий, значения которых будут отражены в списках. Для этого необходимо указать нужные свойства аварий в разделе **Incidents** конфигурационного файла клиента `/etc/saymon/saymon-client.yaml`.

```
incidents:  
  additionalFields:  
    - properties.address,  
  additionalFieldNames:  
    - IP-address
```

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

REST API метод для добавления или изменения свойств аварии:

POST /node/api/incidents/:id/props

Пример (bash) добавления аварии свойств **foo** со значением **1** и **bar** со значением **second**:

```
login=<...>  
password=<...>  
saymon_hostname=<...>  
incident_id=<...>  
url=https://$saymon_hostname/node/api/incidents/$incident_id/props  
  
curl -X POST $url -u $login:$password \  
-H "Content-Type: application/json" \  
-d @- <<EOF  
{  
  "foo": 1,  
  "bar": "second"  
}  
EOF
```

REST API метод для удаления свойств аварии:

```
DELETE /node/api/incidents/:id/props
```

Пример (bash) удаления свойства **foo** аварии:

```
login=<...>  
password=<...>  
saymon_hostname=<...>  
incident_id=<...>  
url=https://$saymon_hostname/node/api/incidents/$incident_id/props  
  
curl -X DELETE $url -u $login:$password \  
-H "Content-Type: application/json" \  
-d @- <<EOF  
{  
  "foo"  
}  
EOF
```


 *Пустой запрос удаляет все свойства аварии.*

3.1.12 Перевод SNMP OID в текстовый формат

По умолчанию в результатах проверки SNMP Trap OID отображается в числовом формате. Для перевода OID в "человекочитаемый" текстовый формат необходимо:

1. В секции **rest_server** конфигурационного файла сервера `/etc/saymon/saymon-server.conf` задать адрес сервера для трансляции OID в текстовый формат в параметре **snmp_mib_url**:

```
{  
  ...  
  "rest_server" : {  
    ...  
    "snmp_mib_url": "http://192.168.1.189:5550",  
  },  
  ...  
}
```

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

2. В конфигурационном файле клиента `/etc/saymon/saymon-client.yaml` установить параметру **enableSnmpTranslate** значение **true**:

```
enableSnmpTranslate: true
```

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

3.1.13 Выполнение скриптов при создании и удалении объектов

При создании или удалении объектов того или иного класса система способна выполнять скрипты и передавать им аргументы, настраиваемые через web-интерфейс.


Для применения изменений достаточно обновить страницу в браузере.

Чтобы настроить скрипты, необходимо:

1. Задать каталог для хранения скриптов:


- 1.1. Открыть конфигурационный файл сервера `/etc/saymon/saymon-server.conf` и добавить в него секцию **custom_scripts**:

```
{
  ...
  "custom_scripts": {
    "entity_triggers_path": "/opt/saymon-extensions/entity-triggers-path"
  },
  ...
}
```

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

- 1.2. В параметре **entity_triggers_path** указать полный путь до каталога.

2. Поместить исполняемый файл в указанный каталог.


 Исполняемые файлы скриптов могут располагаться в любом количестве подпапок. Поиск производится рекурсивно.

3. Задать настройки скрипта в конфигурационном файле.

Параметры скрипта определяются в JSON-файле, именуемом как **имя_исполняемого_файла + .conf**. Располагаться этот файл должен в том же каталоге, что и исполняемый файл.

Пример:

```
/opt/saymon-extensions/entity-triggers-path/myscript.sh
/opt/saymon-extensions/entity-triggers-path/myscript.sh.conf
```

 Возможные поля файла настроек параметров и пример конфигурационного файла представлены в Приложении Б на стр. 178.

3.1.14 Автоматическое обнаружение объектов


Агент сканирует локальную подсеть и отправляет на сервер информацию обо всех IP-адресах, доступных для TCP-соединения либо доступных по PING. Для обнаруженных хостов объекты класса **Host** с соответствующими адресами создаются в Центральном Пульте и отображаются на карте инфраструктуры. Внутри каждого из этих объектов автоматически создаётся объект класса **Ping**, в котором включается мониторинг с помощью агента, выполнившего автообнаружение, и сенсора **Ping**.

IP-адрес обнаруженного объекта автоматически записывается в свойство **IP**, что можно использовать для перехода по этому адресу в браузере или доступа к объекту по SSH или Telnet через контекстное меню.

Чтобы настроить автообнаружение объектов, необходимо:

1. В конфигурационном файле агента `.../saymon-agent/conf/agent.properties` установить параметру **agent.discoveryEnabled** значение **true**:


```
agent.discoveryEnabled=true
```

 Подробную информацию о файле `.../saymon-agent/conf/agent.properties` см. в подразделе 3.1.2 "Конфигурация агента" на стр. 21.

2. Указать ID родительского объект для обнаруживаемых объектов в параметре **server.discovery_parent_id** конфигурационного файла сервера `/etc/saymon/saymon-server.conf`:

 По умолчанию обнаруженные объекты помещаются в корневой объект.

```
...
  "server": {
    ...
    "discovery_parent_id": "632aae8b1a687b43378c0657",
    ...
  },
  ...
```

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

3. Перезапустить службы `saymon-agent` и `saymon-server`:

```
sudo service saymon-agent restart
sudo service saymon-server restart
```

Заключительные действия:


Не требуются.

3.2 Модуль аналитики

По умолчанию модуль аналитики, используемый для прогнозирования и определения всплесков, не включен в ISO-образ Центрального Пульта. Чтобы установить модуль аналитики, необходимо:

1. Скачать скрипт [analytics-create-and-run.sh](#) и разместить его в файловой системе на виртуальной машине, где установлен ISO-образ Центрального Пульта.
2. Запустить скрипт командой

```
sudo ANALYTICS_BRANCH=x.y.z ./analytics-create-and-run.sh
```

 *x.y.z - версия модуля аналитики, совместимая с вашей версией Центрального Пульта.*

Проверить, что контейнер **saymon-analytics** запустился и работает, можно с помощью команды


```
docker ps -a
```


3.2.1 Подключение модуля аналитики к Центральному Пульту

Чтобы подключить модуль аналитики, потребуется внести изменения в конфигурацию Центрального Пульта:

1. В секции **Server** конфигурационного файла сервера `/etc/saymon/saymon-server.conf` добавить или изменить следующие параметры:

```
{  
  ...  
  "server" : {  
    ...  
    "analytics_enabled": true,  
    "analytics_processes": 2 # количество логических ядер для аналитики  
  },  
  ...  
}
```

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

2. В конфигурационном файле клиента `/etc/saymon/saymon-client.yaml` установить параметру **enableAnalytics** значение **true**:

```
enableConditionallncidents: true,
```

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

3. Перезапустить сервер Центрального Пульта:

```
sudo service saymon-server restart
```

3.2.2 Мониторинг работы модуля аналитики

Чтобы мониторить работу модуля аналитики можно использовать логи контейнера **saymon-analytics**. Для этого необходимо:

1. Подключиться к контейнеру командой

```
docker exec -ti saymon-analytics bash
```

2. Открыть файл логов модуля командой

```
tail -f /opt/analytics/analytics.log
```

В логах модуля содержится информация о:

- настройках, с которыми запущен модуль (слушающий сокет и количество задействованных в пуле обработчика процессов),
- обрабатываемых метриках,
- результатах обработки метрик,
- ошибках, возникающих в процессе работы модуля.

3.3 Управление сенсорами мониторинга

Системой предусмотрена возможность скрывать в интерфейсе неиспользуемые мониторинговые сенсоры, а также настраивать пользовательские сенсоры и внедрять их в интерфейс.

3.3.1 Скрытие неиспользуемых сенсоров


Для того, чтобы неиспользуемые сенсоры не отображались в пользовательском интерфейсе, необходимо:

1. Открыть конфигурационный файл клиента `/etc/saymon/saymon-client.yaml` и добавить в него секцию **monitoring**:

```
monitoring:  
standardTasks:  
- ping  
- snmpGet
```

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

2. В переменной **monitoring.standardTasks** указать идентификаторы сенсоров, отображаемых в web-интерфейсе.

 Идентификаторы сенсоров чувствительны к регистру символов.

Список идентификаторов стандартных сенсоров:

- binaryProtocol (бинарный протокол),
- configFile (конфигурационный файл / директория),
- databaseQuery (запрос в базу данных),
- exec (выполнение программы / скрипта),
- external (внешняя проверка - записанные через API данные),
- ftp (FTP-сенсор),
- httpRequest (HTTP-запрос),
- jmx (jmx-сенсор),
- localNetworkPort (локальный порт),
- mqtt (mqtt-сенсор),
- ping (пинг-сенсор),
- processInfo (процесс по имени),
- remoteNetworkPort (удалённый порт),
- snmpGet (SNMP Get-сенсор),
- snmpTrap (SNMP Trap-сенсор),
- wmi (WMI-сенсор).

3.3.2 Настройка пользовательских сенсоров

В качестве сенсора можно использовать собственноручно написанный скрипт и передавать ему в качестве аргументов значения параметров через удобный web-интерфейс.


Для применения изменений достаточно обновить страницу в браузере.

Чтобы сделать пользовательский скрипт мониторинговым сенсором, необходимо:

1. Задать каталог для хранения пользовательских сенсоров:


1.1. Открыть конфигурационный файл сервера `/etc/saymon/saymon-server.conf` и добавить в него секцию **monitoring**:

```
{
  ...
  "monitoring": {
    "custom_tasks_path": "/opt/saymon-agent/custom_tasks"
  },
  ...
}
```


 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.


1.2. В параметре **monitoring.custom_tasks_path** указать полный путь до каталога.

2. Поместить исполняемый файл в указанный каталог.

 Исполняемые файлы пользовательских сенсоров могут располагаться в любом количестве подпапок. Поиск производится рекурсивно.

3. Проверить идентификатор пользовательского сенсора. Идентификатор сенсора создаётся автоматически и эквивалентен имени исполняемого файла с относительным путём (если есть). Например: **utils/network/ping**.

 Идентификатор пользовательского сенсора не должен совпадать с идентификатором стандартного, иначе пользовательский сенсор будет проигнорирован.


 С перечнем идентификаторов стандартных сенсоров можно ознакомиться в подразделе 3.3.1 "Скрытие неиспользуемых сенсоров" на стр. 75.


4. Задать настройки сенсора в конфигурационном файле.

Параметры сенсора определяются в JSON-файле, именуемом как **имя_исполняемого_файла + .conf**. Располагаться этот файл должен в том же каталоге, что и исполняемый файл.

Пример:

```
/opt/saymon-agent/custom_tasks/mytask.sh  
/opt/saymon-agent/custom_tasks/mytask.sh.conf
```

 *Возможные поля файла настроек параметров и пример конфигурационного файла представлены в Приложении Б на стр. 178.*

 *Пользовательские сенсоры выполняются агентами локально, поэтому необходимо скопировать исполняемые файлы в одну и ту же папку на все хосты, на которых предполагается их запускать. Конфигурационные файлы достаточно разместить на хостах с сервером системы.*

3.4 Настройка уведомлений

При переходе объектов в определенные состояния система может:

- отправлять email-уведомления,
- автоматически запускать программу или скрипт с параметрами,
- отправлять сообщения в Telegram,
- показывать визуальное уведомление в браузере, сопровождающееся звуком,
- создавать задачи в JIRA,
- запускать операции,
- отправлять SMS,
- совершать голосовые вызовы.

Уведомления настраиваются в виде подробной информации об объекте в секции "Действия при смене состояния" (Рис. 3.4.1):

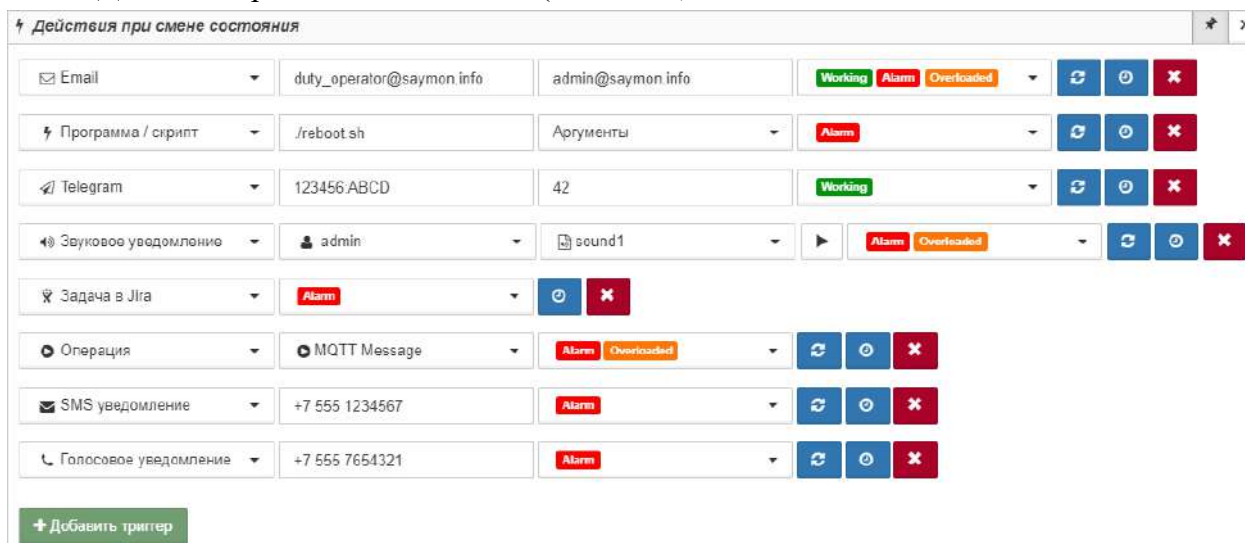


Рис. 3.4.1. Действия при смене состояния

3.4.1 Активация функционала отправки SMS и голосовых вызовов

Для активации функционала необходимо выполнить описанные ниже действия:

1. В файле конфигурации клиента `/etc/saymon/saymon-client.yaml` установить параметрам `enableSmsTrigger` и `enableVoiceCallTrigger` значение `true`:

```
enableVoiceCallTrigger: true
enableSmsTrigger: true
```

📘 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

2. В секции **Server** конфигурационного файла сервера `/etc/saymon/saymon-server.conf` задать путь до скриптов, осуществляющих отправку SMS-уведомлений и голосовые вызовы:

```
{
  ...
  "server" : {
    ...
    "sms_script" : "путь до скрипта, отправляющего sms-уведомления",
    "voice_call_script" : "путь до скрипта, осуществляющего голосовые
    вызовы",
    ...
  },
  ...
}
```


📘 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

3. Для применения изменений перезапустить службу "saymon-server":

```
sudo service saymon-server restart
```


3.4.2 Отправка почтовых уведомлений

Для настройки отправки почтовых уведомлений требуется настроить необходимые параметры доступа к почтовому серверу в подсекции **Email** секции **Server** файла `/etc/saymon/saymon-server.conf`.

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

Пример настройки подсекции **Email**:

```
"email" : {
  "disabled" : false,
  "fields" : {
    "from" : "saymon@saas.saymon.info"
  },
  "max_json_length": 1000,
  "transport" : {
    "auth" {
      "user" : "saymon@saas.saymon.info",
      "pass" : "P@ssw0rd"
    },
    "host" : "smtp.gmail.com",
    "port" : 465,
    "secure" : true
  },
}
```

3.4.3 Настройка уведомлений в Telegram

Для настройки отправки уведомлений с помощью Telegram необходимо:

1. Задать бота, от которого будут поступать уведомления:
 - 1.1. Создать нового бота:
 - 1.1.1. Найти в приложении Telegram контакт **BotFather**.
 - 1.1.2. Отправить ему сообщение **/newbot**.
 - 1.1.3. Задать боту отображаемое имя (**name**, позже возможно изменить).
 - 1.1.4. Задать боту уникальное имя (**username**, изменить будет невозможно).
 - 1.1.5. Скопировать токен бота вида
`210979209:AAFfT2mt3oW4EK1gYqE_d3OjAJSIRLSrAL`.
 - 1.1.6. Отправить контакту **BotFather** сообщение **/setprivacy**.
 - 1.1.7. Выбрать созданного бота по его **username**.
 - 1.1.8. Выбрать опцию **Disable**.
 - 1.2. Использовать существующего бота:
 - 1.2.1. Найти в приложении Telegram контакт **BotFather**.
 - 1.2.2. Отправить ему сообщение **/mybots**.
 - 1.2.3. Выбрать нужного бота.
 - 1.2.4. Выбрать опцию **API Token**.
 - 1.2.5. Скопировать токен бота вида
`210979209:AAFfT2mt3oW4EK1gYqE_d3OjAJSIRLSrAL`.
2. Настроить канал, чат или группу:
 - 2.1. Создать приватный канал (рекомендуется):
 - 2.1.1. В приложении Telegram создать новый канал.
 - 2.1.2. Открыть настройки канала, добавить бота в список администраторов.
 - 2.1.3. Отправить сообщение в канал.
 - 2.1.4. Перейти по ссылке в любом web-браузере, вставив в неё токен своего бота (без пробелов и знаков <>):
`https://api.telegram.org/bot<токен_бота>/getUpdates`
 - 2.1.5. Найти текст со словами **chat** и **id**, например
`... "channel_post": {"message_id": 4, "chat": {"id": -1001156346945, "title": "SAYMON" ...`
Здесь **-1001156346945** - искомый ID канала.
 - 2.2. Создать чат:
 - 2.2.1. Отправить боту любое сообщение.
 - 2.2.2. Перейти по ссылке в любом web-браузере, вставив в неё токен своего бота (без пробелов и знаков <>):
`https://api.telegram.org/bot<токен_бота>/getUpdates`
 - 2.2.3. Найти текст со словами **chat** и **id**, например
`... ": "К"}, "chat": {"id": 121399918, "first_ ...`
Здесь **121399918** - искомый ID чата.
 - 2.3. Настроить группу:

2.3.1. Добавить бота в группу.

2.3.2. Отправить боту в группу любое сообщение, начав его со знака @.

2.3.3. Перейти по ссылке в любом web-браузере, вставив в неё токен своего бота (без пробелов и знаков <>):

```
https://api.telegram.org/bot<токен_бота>/getUpdates
```

2.2.4. Найти текст со словами **chat** и **id**, например

```
... "К" }, "chat": { "id": -209194473, "first_ ...
```

Здесь **-209194473** - искомый ID группы.

3. В настройках Telegram-уведомлений ввести токен (ID) бота и ID канала/чата/группы в соответствующие поля.

3.5 Интеграция со сторонними системами

Система предусматривает возможность импортировать данные с других мониторинговых платформ и экспортировать метрики в платформы для визуализации данных.

3.5.1 Интеграция с Zabbix

Для импорта данных из Zabbix необходимо:

1. Проверить доступ от сервера Центрального Пульта до сервера Zabbix, выполнив команду (в одну строку), заменив **http://192.168.1.215** на адрес файла `api_jsonrpc.php` вашей инсталляции Zabbix:

```
curl -H "Content-Type: application/json" -X POST -d  
'{"jsonrpc":"2.0","method":"apiinfo.version","id":1,"auth":null,"params"  
{}}' http://192.168.1.215/zabbix/api_jsonrpc.php
```

При наличии доступа сервер Zabbix ответит похожим сообщением:


```
{"jsonrpc":"2.0","result":"3.2.1","id":1}
```

2. Добавить в Zabbix пользователя с правами на чтение необходимых хостов или групп хостов.
3. На сервере системы создать объект, в который будут импортироваться данные о хостах из Zabbix, и запомнить его ID.
4. Открыть конфигурационный файл сервера `/etc/saymon/saymon-server.conf` и добавить в него секцию **zabbix**:

```
"zabbix": [  
  {  
    "url" : "http://192.168.1.215/zabbix/api_jsonrpc.php",  
    "user" : "saymon",  
    "password" : "saymon_user_password",  
    "parent_id" : "58b586d5c3a2f96642e25537"  
  },  
  ...  
]
```

где:

- **url** - адрес файла `api_jsonrpc.php` вашей инсталляции Zabbix, который был использован на шаге 1, например, **http://192.168.1.215/zabbix/api_jsonrpc.php**;
- **user** - имя пользователя, добавленного в Zabbix на шаге 2;
- **password** - пароль пользователя, добавленного в Zabbix на шаге 2;
- **parent_id** - ID объекта, созданного на шаге 3.

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

5. Для каждого дополнительного сервера Zabbix добавить новый JSON-документ с его данными в массив:

```
"zabbix" : [  
  {  
    "url" : "http://192.168.1.215/zabbix/api_jsonrpc.php",  
    "user" : "saymon",  
    "password" : "saymon_user_password",  
    "parent_id" : "58b586d5c3a2f96642e12345"  
  },  
  {  
    "url" : "http://192.168.1.180:8020/zabbix/api_jsonrpc.php",  
    "user" : "saymon",  
    "password" : "saymon_user_password",  
  }  
]
```

Для применения изменений необходимо перезапустить службу **saymon-server**:

```
sudo service saymon-server restart
```

По умолчанию данные на сервере системы обновляются каждые 2 минуты. Для изменения периода обновления данных необходимо добавить в конфигурационный файл сервера `/etc/saymon/saymon-server.conf` параметр **polling_period** со значением периода обновления данных в миллисекундах:

```
"zabbix" : [  
  {  
    "url" : "http://192.168.1.215/zabbix/api_jsonrpc.php",  
    "user" : "saymon",  
    "password" : "saymon_user_password",  
    "parent_id" : "58b586d5c3a2f96642e12345"  
    "polling_period": 30000  
  }  
]
```

Возможно изменять опции для запросов

- хостов (hosts),
- триггеров (triggers),
- данных (data).

i Все возможные поля фильтров представлены в документации по Zabbix API:

- [hosts](#),
- [triggers](#),
- [data](#).

```
"zabbix" : [{
  ...
  "request_options": {
    "hosts": {
      "filter": {
        ...
      }
    },
    "triggers": {
      "filter": {
        ...
      }
    },
    "data": {
      "filter": {
        ...
      }
    }
  }
}
...
}]
```

Чтобы убрать фильтр из опции запроса, необходимо указать параметру **filter** значение **null**.

Пример (убрать поле **filter** из опций запроса триггеров Zabbix):

```
"zabbix" : [{
  ...
  "triggers": {
    "filter": null
  }
}
...
}]
```

Обнаруженным объектам по умолчанию присваивается класс **Info**. Чтобы присвоить новым объектам другие классы, необходимо задать массив **zabbix.classes** и указать в нём соответствия идентификаторов классов и имён объектов:

```
"zabbix" : [{  
  ...  
  "classes" : {  
    "4" : "CPU",  
    "619503be0ffb595aebe22222" : "Memory|General"  
  },  
  ...  
}]
```

! *Порядок применения правил привязки не гарантируется. Если назначить двум разным классам одинаковые регулярные выражения или использовать выражение `".*"` (любой текст), то нет гарантии, что сначала будет применено правило, указанное выше в списке.*

Для каждого Zabbix-подключения массив настраивается индивидуально. Регулярное выражение по имени объекта нечувствительно к регистру символов.

! *При необходимости связать класс с несколькими именами необходимо указать все имена в одном регулярном выражении с использованием оператора **ИЛИ**, в противном случае применится только одно соответствие.*
Пример:
`"619503be0ffb595aebe22222": "Memory|General"`

Чтобы выводить параметры и результаты запросов в лог, необходимо задать параметр **zabbix.debug** со значением **true**:

```
"zabbix" : [{  
  ...  
  "debug": true,  
  ...  
}]
```


3.5.2 Интеграция с Grafana

⚠ Все действия, связанные с интеграцией, осуществляются в интерфейсе Grafana.

Для экспорта метрик в Grafana необходимо:

1. Авторизоваться в Grafana.
2. С главной страницы рабочего пространства перейти в **Configurations - Data Sources** через боковое меню и добавить data source (источник данных) нажатием на соответствующую кнопку (Рис. 3.5.2.1):

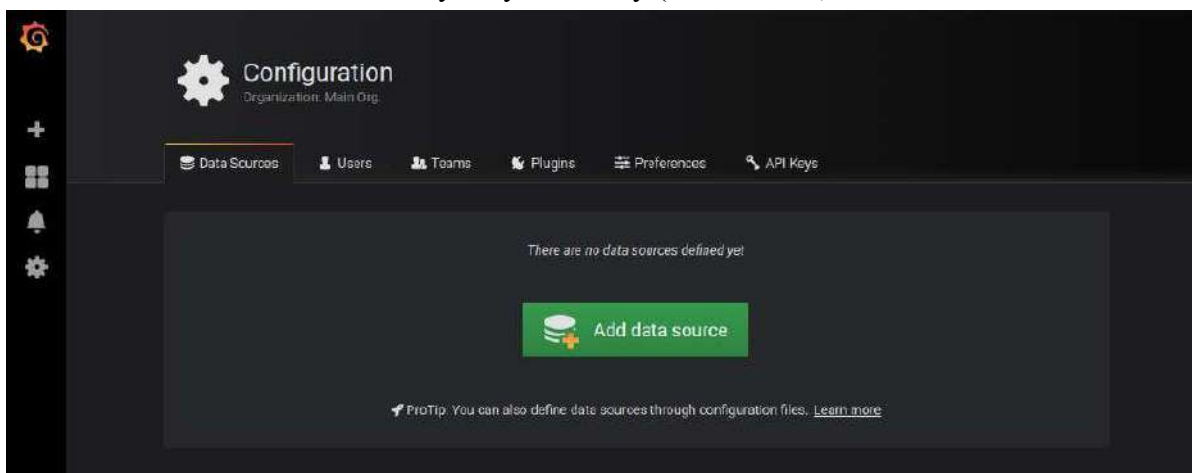


Рис. 3.5.2.1. Добавление источника данных в Grafana

3. В открывшемся окне типов источников данных выбрать **SAYMON** (Рис. 3.5.2.2):

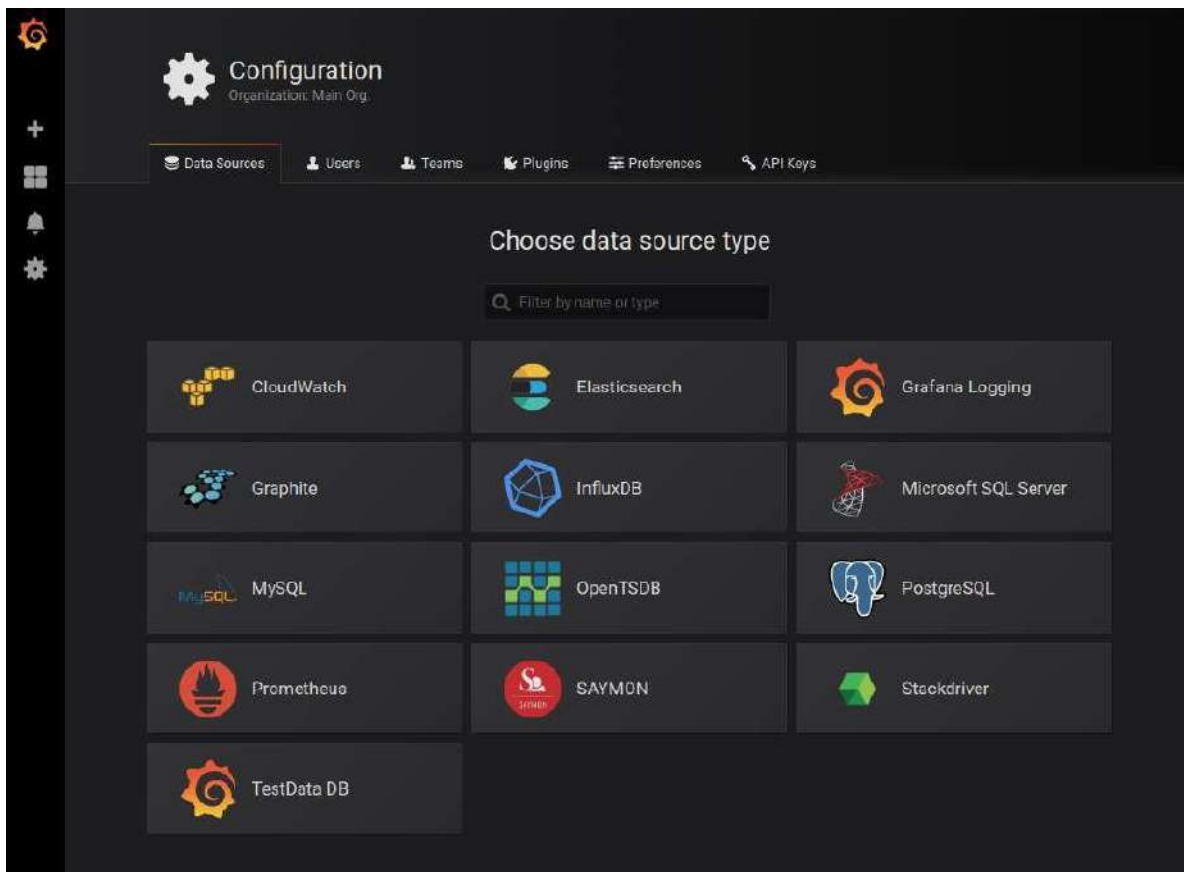


Рис. 3.5.2.2. Выбор источника данных в Grafana

4. В окне настроек необходимо указать (Рис. 3.5.2.3):
- имя источника данных;
 - URL-адрес, откуда будут собираться данные;
 - режим доступа, как будут обрабатываться запросы к источнику данных: **server** или **browser**;
 - имена cookies-файлов, которые должны быть перенаправлены в источник данных;
 - тип аутентификации;
 - логин и пароль, используемые в Центральном Пульте.

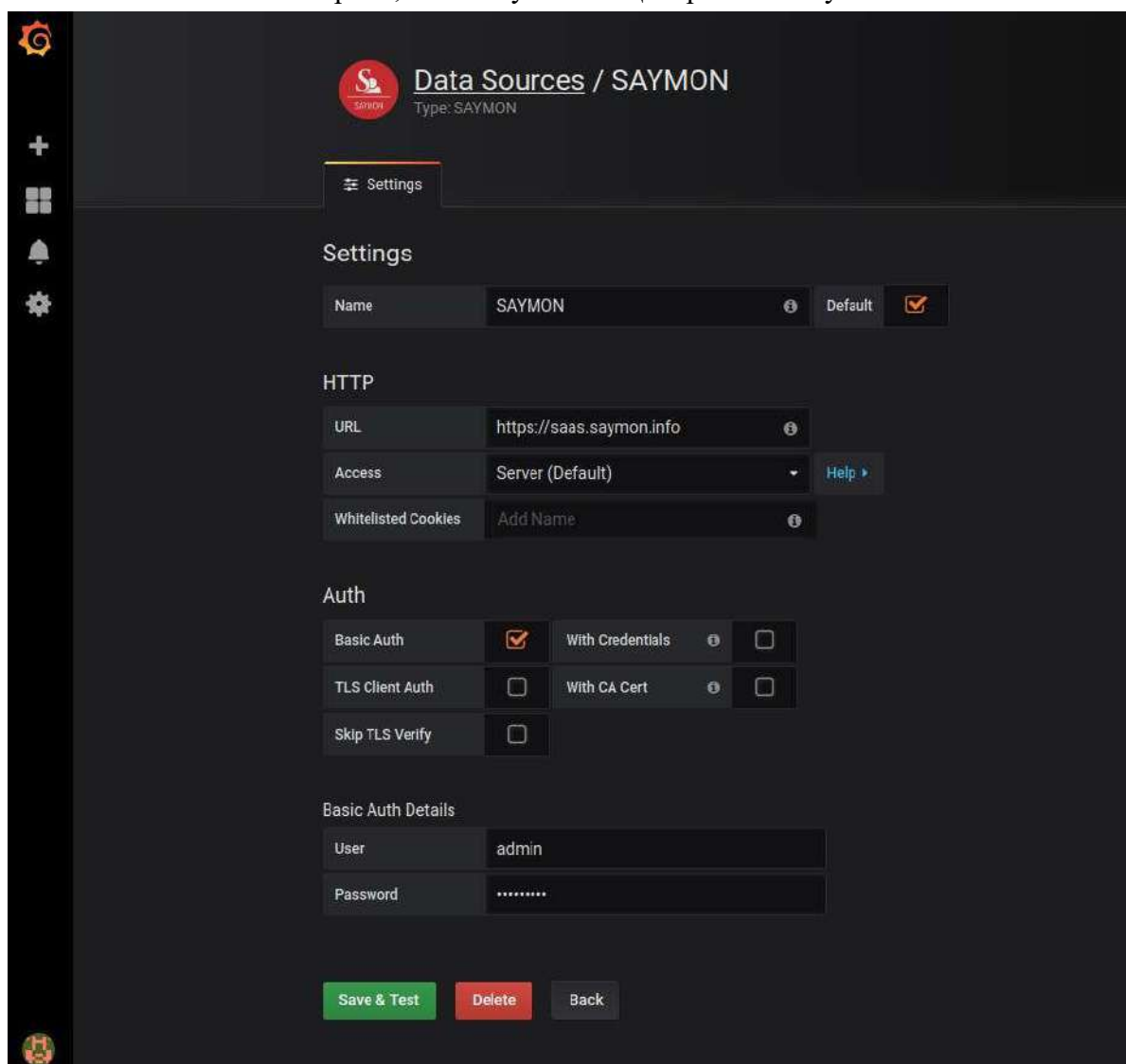


Рис. 3.5.2.3. Настройка источника данных в Grafana

5. Через боковое меню перейти в окно управления дашбордами (**dashboards - manage**) и приступить к созданию нового дашборда нажатием соответствующей кнопки (Рис. 3.5.2.4):

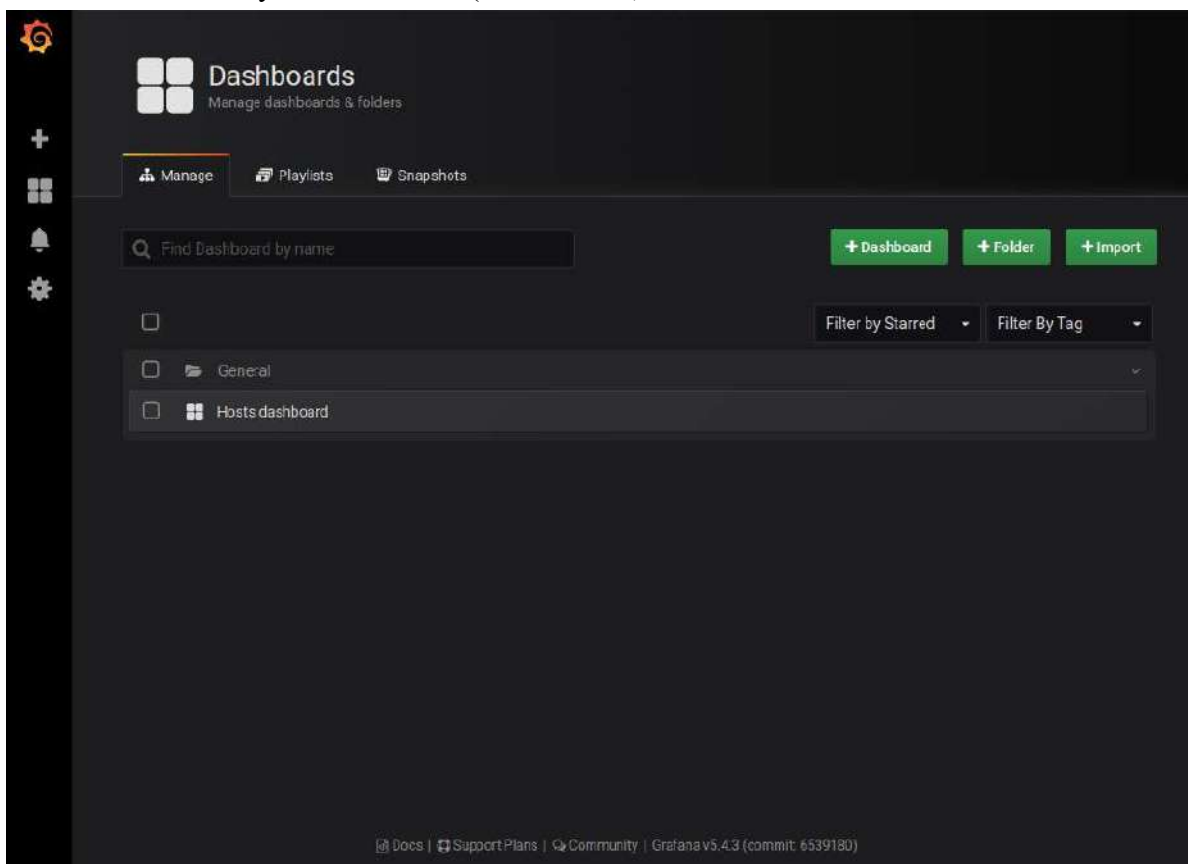


Рис. 3.5.2.4. Создание нового дашборда в Grafana

6. Выбрать тип отображения дашборда. Например, график (Рис. 3.5.2.5):



Рис. 3.5.2.5. Выбор типа отображения дашборда в Grafana

7. Вызвать контекстное меню нажатием на стрелку рядом с заголовком панели и перейти в режим редактирования.

- В окне редактирования перейти во вкладку **Metrics** и добавить объекты, к которым у пользователя, под чьей учётной записью совершён вход, есть доступ в Центральном Пульте (Рис. 3.5.2.6). Указать:
 - имя или ID объекта;
 - метрику, которую необходимо отобразить на графике;
 - отображать ли путь до объекта.

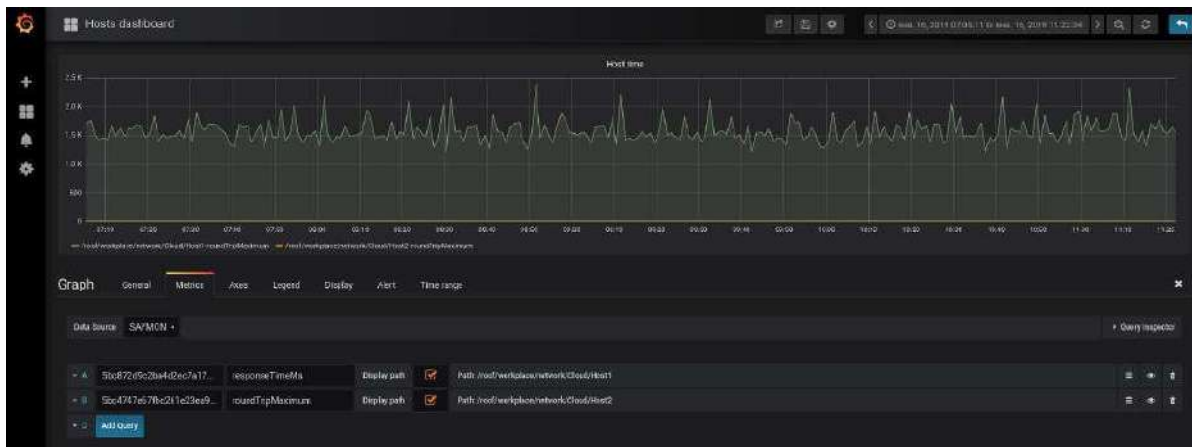


Рис. 3.5.2.6. Отображение дашборда в Grafana

- Настроить временной период, за который данные отображаются на графике, и интервал их обновления.

3.5.3 Интеграция с Keycloak

Для пользователей Центрального Пульта предусмотрена возможность авторизации посредством сервера Keycloak.

Клиенты в Keycloak - это параметры соединения с Keycloak-сервером для внешних приложений, которые авторизуют пользователей.


Главной особенностью Backend-клиента является наличие собственной аутентификации: такой клиент получает конфиденциальный доступ по секретному ключу.

Главной особенностью Frontend-клиента является отсутствие собственной аутентификации: данный клиент получает публичный доступ.

Для настройки взаимодействия между сервером Центрального Пульта и внешним сервером Keycloak необходимо получить хотя бы один из параметров:

- Realm Certificate, которым сервер Keycloak подписывает пользовательские токены,
- файл настроек соединения для Backend-клиента.

Для возможности авторизации пользователей посредством Keycloak через web-интерфейс Центрального Пульта необходимо получить файл настроек соединения Frontend-клиента.

 *Настройка клиентов и получение параметров осуществляются в консоли администратора Keycloak.*

3.5.3.1 Настройка сервера

Для получения Realm Certificate необходимо:

1. Выбрать требуемую область (Realm) из списка (Рис. 3.5.3.1.1; здесь **SAYMON**):

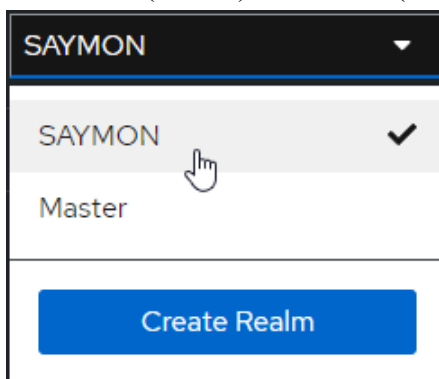


Рис. 3.5.3.1.1. Выбор области Keycloak

2. В секции **Realm settings** на вкладке **Tokens** уточнить алгоритм подписи токенов в поле **Default Signature Algorithm** (Рис. 3.5.3.1.2; здесь **RS256**):

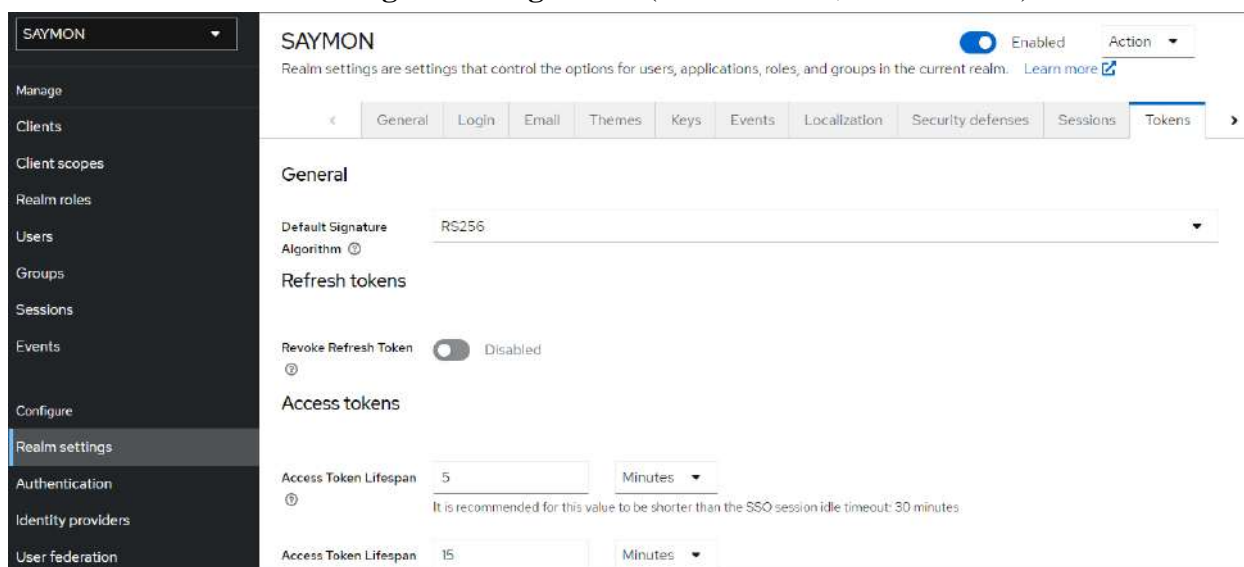


Рис. 3.5.3.1.2. Проверка алгоритма подписи токенов

3. На вкладке **Keys** найти сертификат для данного алгоритма (Рис. 3.5.3.1.3):

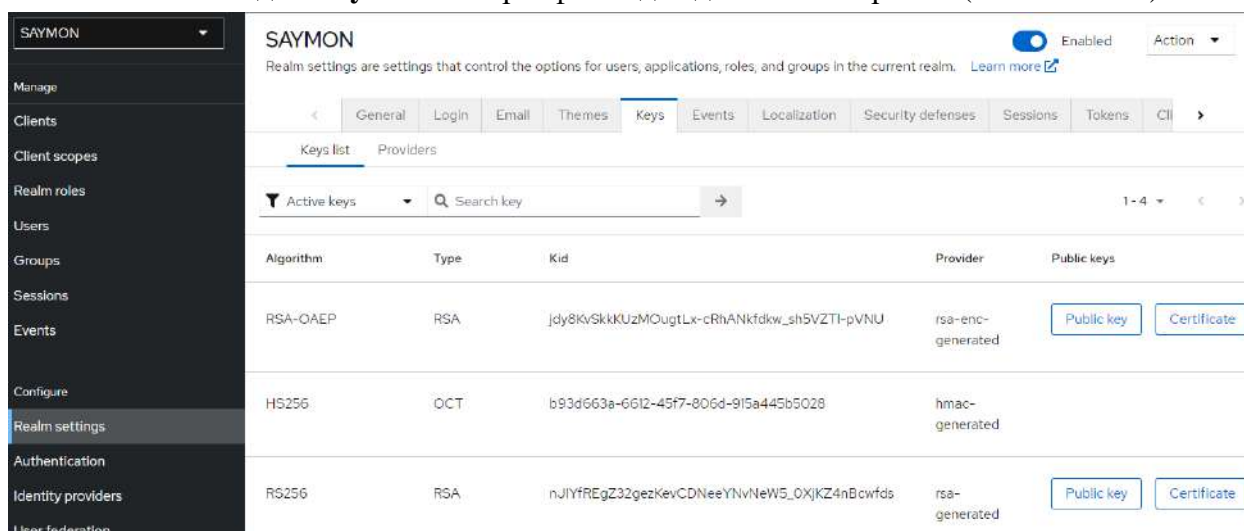
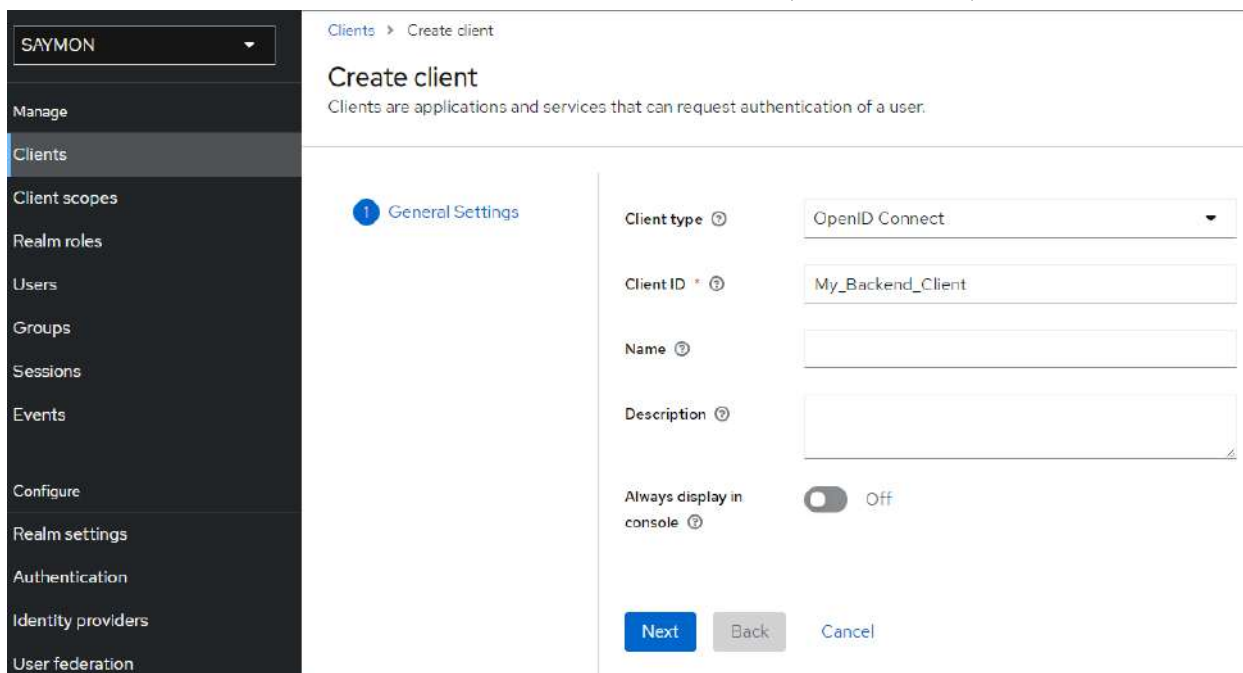


Рис. 3.5.3.1.3. Получение сертификата

3. Ввести имя Backend-клиента в поле **Client ID** (Рис. 3.5.3.1.6):

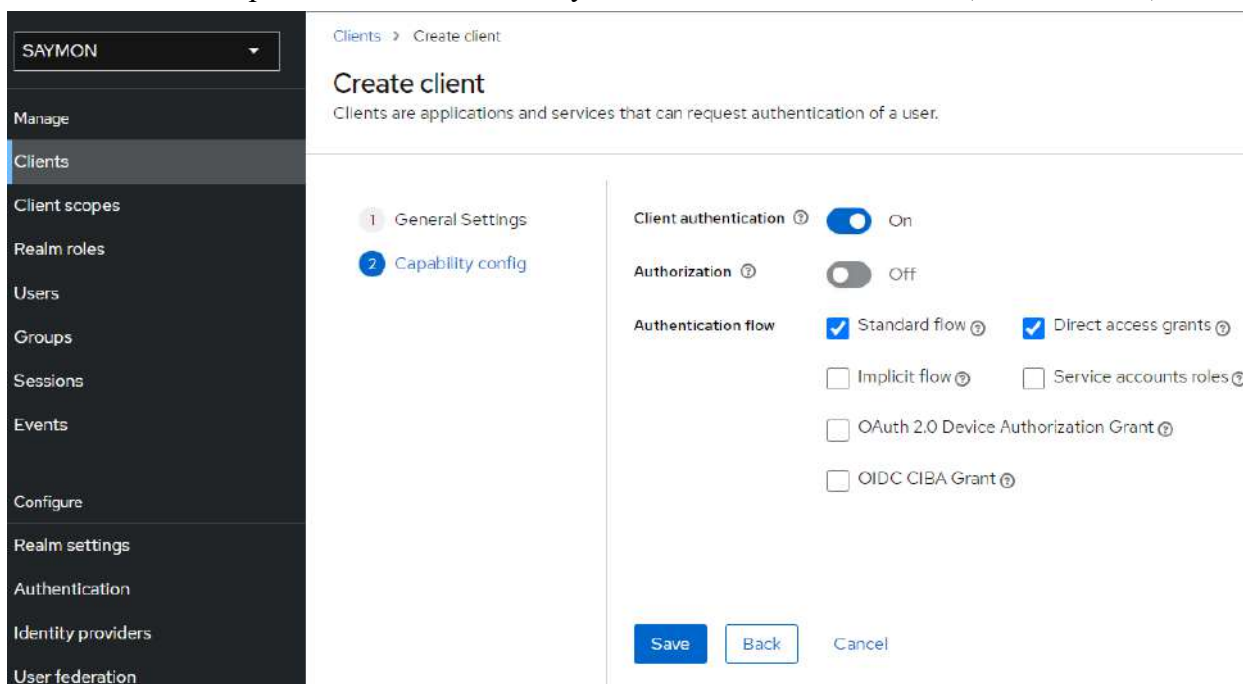


The screenshot shows the 'Create client' interface. On the left is a navigation menu with 'Clients' selected. The main area has a breadcrumb 'Clients > Create client' and a title 'Create client'. Below the title is a sub-header 'Clients are applications and services that can request authentication of a user.' A progress indicator shows '1 General Settings' selected. The form fields are: 'Client type' (OpenID Connect), 'Client ID *' (My_Backend_Client), 'Name' (empty), 'Description' (empty), and 'Always display in console' (Off). At the bottom are 'Next', 'Back', and 'Cancel' buttons.

Рис. 3.5.3.1.6. Ввод имени Backend-клиента

и нажать кнопку .

4. Слайдер **Client authentication** установить в положение **On** (Рис. 3.5.3.1.7):



The screenshot shows the 'Create client' interface at the 'Capability config' step. The progress indicator shows '2 Capability config' selected. The form fields are: 'Client authentication' (On), 'Authorization' (Off), 'Authentication flow' (Standard flow and Direct access grants checked), 'Implicit flow' (unchecked), 'Service accounts roles' (unchecked), 'OAuth 2.0 Device Authorization Grant' (unchecked), and 'OIDC CIBA Grant' (unchecked). At the bottom are 'Save', 'Back', and 'Cancel' buttons.

Рис. 3.5.3.1.7. Включение клиентской аутентификации

и нажать кнопку .

5. В списке **Action** выбрать **Download adapter config** (Рис. 3.5.3.1.8):

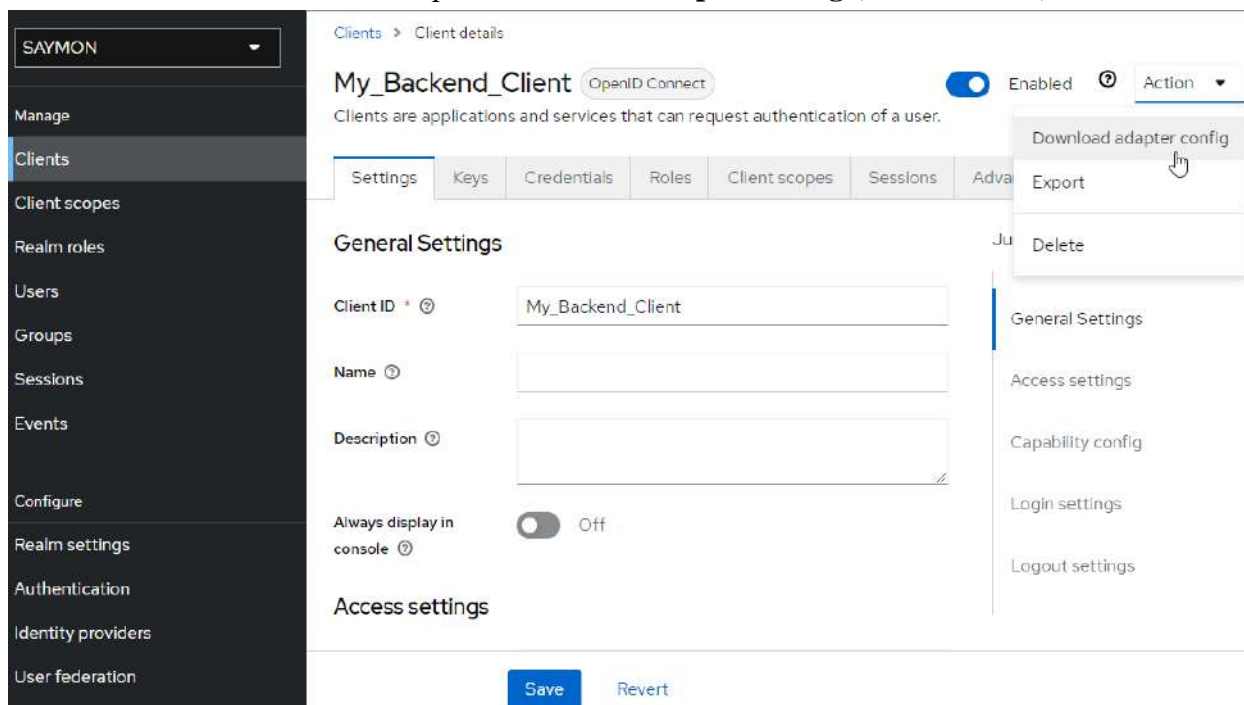


Рис. 3.5.3.1.8. Получение файла конфигурации Backend-клиента

6. Нажать кнопку **Download**, чтобы получить файл настроек соединения для Backend-клиента в формате JSON (Рис. 3.5.3.1.9):

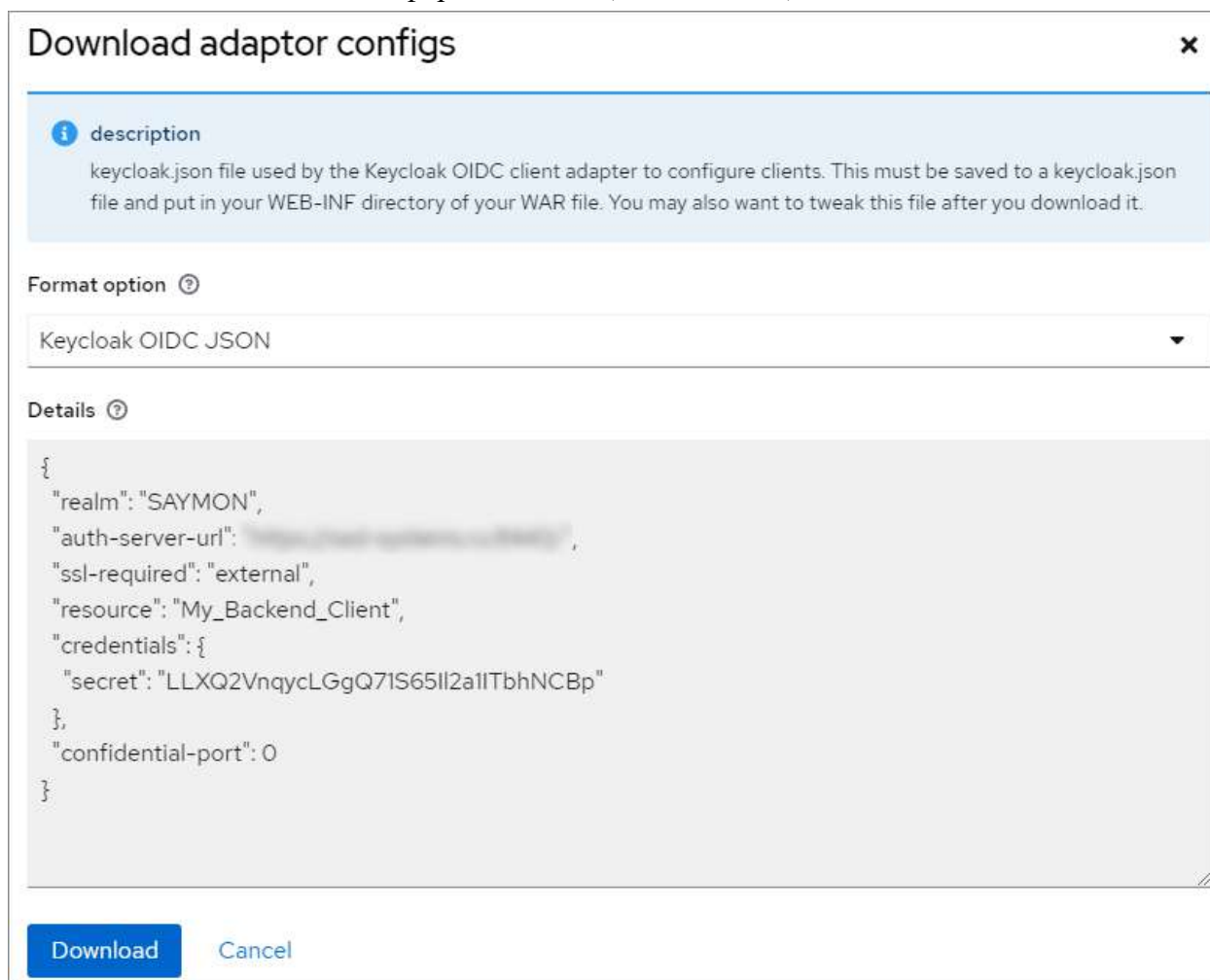


Рис. 3.5.3.1.9. Пример данных файла конфигурации Backend-клиента

Для взаимодействия с сервером Keycloak на сервере Центрального Пульта необходимо:

1. Добавить раздел **keycloak** в конфигурационный файл сервера


`/etc/saymon/saymon-server.conf` :

```
"keycloak": {  
  "realm_certificate": "<данные keycloak_realm_certificate>",  
  "realm_certificate_file": "/etc/saymon/keycloak_realm_certificate",  
  "config_file": "/etc/saymon/keycloak_backend.json"  
}
```

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

где:

- **realm_certificate** - данные Keycloak Realm Certificate;
- **realm_certificate_file** - путь к файлу с Keycloak Realm Certificate;
- **config_file** - путь к файлу конфигурации, сгенерированному Keycloak-сервером (для backend-клиента).

 Параметры перечислены в порядке понижения приоритета при одновременном указании. Для работы с Keycloak достаточно указать один из параметров.

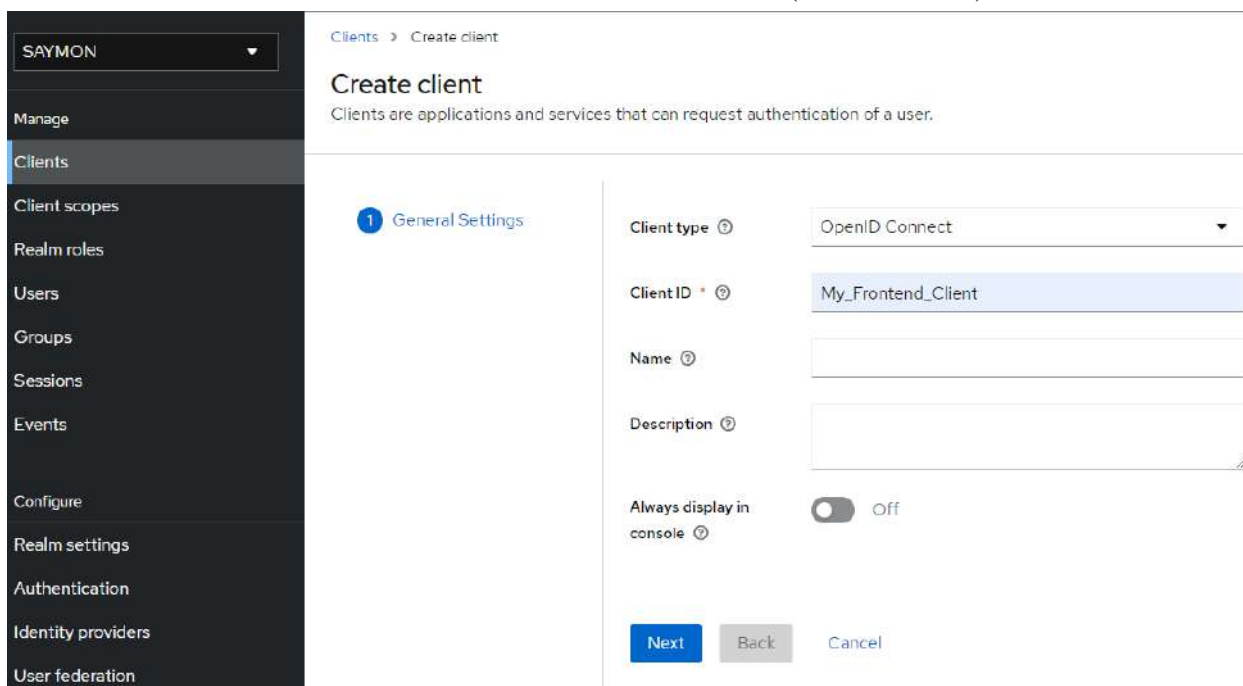
2. Перезапустить службу saymon-server:

```
sudo service saymon-server restart
```

3.5.3.2 Настройка web-интерфейса

Для настройки Frontend-клиента необходимо:

1. Выбрать требуемую область (Realm) из списка (Рис. 3.5.3.1.1 на стр. 93).
2. В секции **Clients** нажать кнопку **Create client** (Рис. 3.5.3.1.5 на стр. 94).
3. Ввести имя Frontend-клиента в поле **Client ID** (Рис. 3.5.3.2.1):

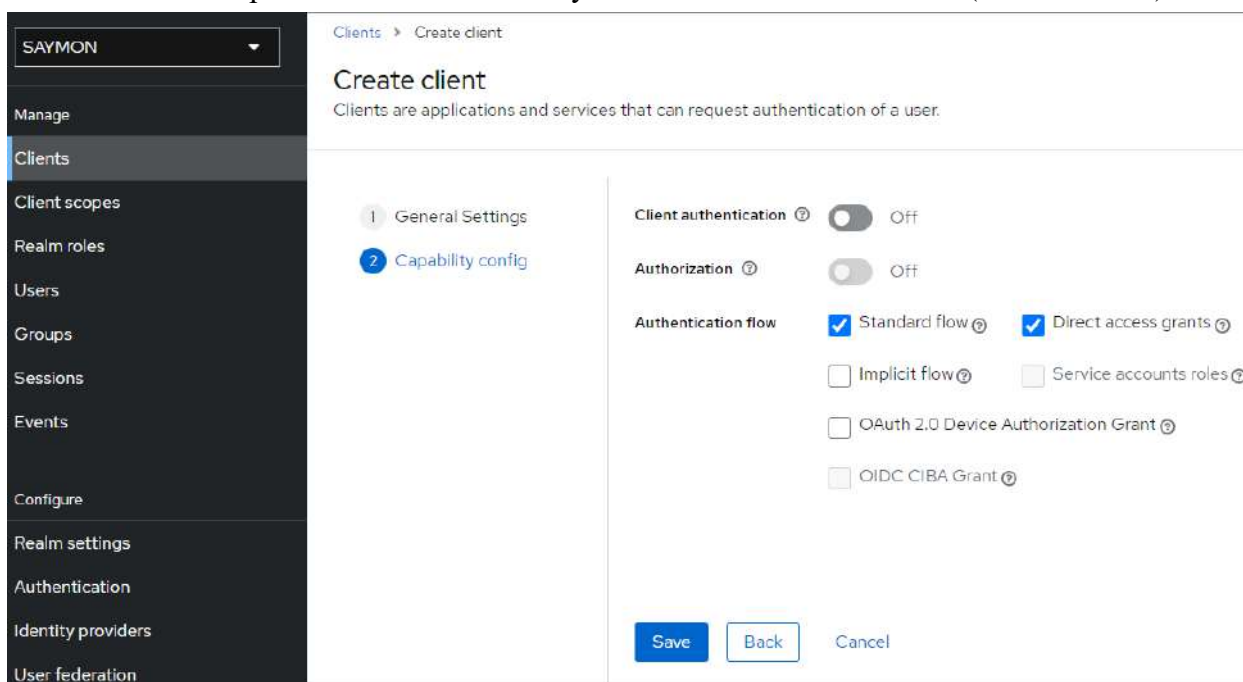


The screenshot shows the 'Create client' interface. On the left is a navigation menu with 'Clients' selected. The main area has a breadcrumb 'Clients > Create client' and a title 'Create client'. Below the title is a sub-header 'Clients are applications and services that can request authentication of a user.' The 'General Settings' step is active, indicated by a blue circle with the number '1'. The 'Client type' dropdown is set to 'OpenID Connect'. The 'Client ID' field is highlighted with a blue selection box and contains the text 'My_Frontend_Client'. The 'Name' and 'Description' fields are empty. The 'Always display in console' toggle is turned off. At the bottom, there are three buttons: 'Next' (highlighted in blue), 'Back', and 'Cancel'.

Рис. 3.5.3.2.1. Ввод имени Frontend-клиента

и нажать кнопку **Next**.

4. Слайдер **Client authentication** установить в положение **Off** (Рис. 3.5.3.2.2):



The screenshot shows the 'Create client' interface. The breadcrumb is 'Clients > Create client'. The title is 'Create client'. Below the title is a sub-header 'Clients are applications and services that can request authentication of a user.' The 'General Settings' step is completed, and the 'Capability config' step is active, indicated by a blue circle with the number '2'. The 'Client authentication' toggle is turned off. The 'Authorization' toggle is also turned off. The 'Authentication flow' section has 'Standard flow' and 'Direct access grants' checked. The 'Implicit flow', 'Service accounts roles', 'OAuth 2.0 Device Authorization Grant', and 'OIDC CIBA Grant' are unchecked. At the bottom, there are three buttons: 'Save' (highlighted in blue), 'Back', and 'Cancel'.

Рис. 3.5.3.2.2. Отключение клиентской аутентификации

и нажать кнопку **Save**.

5. На вкладке **Settings** в разделе **Access settings** указать корректные URI-адреса, с которых будет осуществляться доступ к Keycloak-серверу, и на которые будут перенаправляться пользователи после успешной аутентификации и выхода (Рис. 3.5.3.2.3):

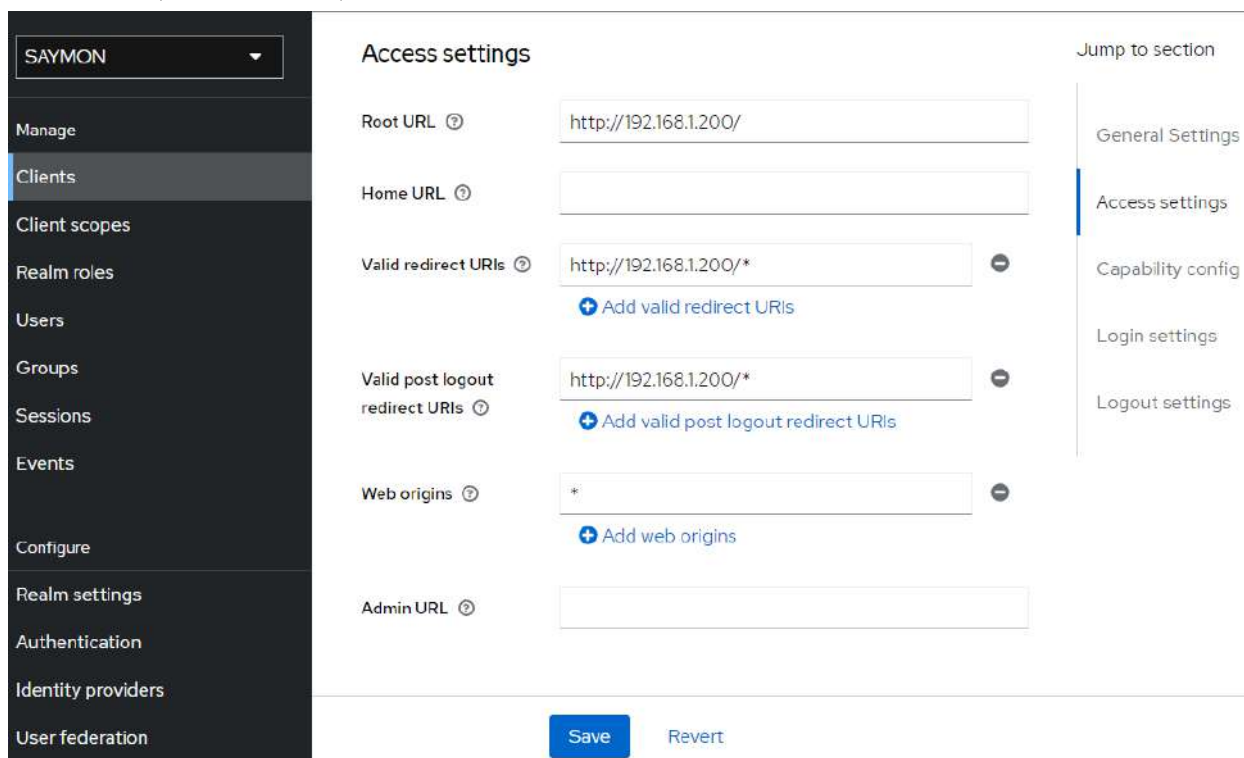


Рис. 3.5.3.2.3. Отключение клиентской аутентификации

и нажать кнопку 

6. В списке **Action** выбрать **Download adapter config** (Рис. 3.5.3.2.4):

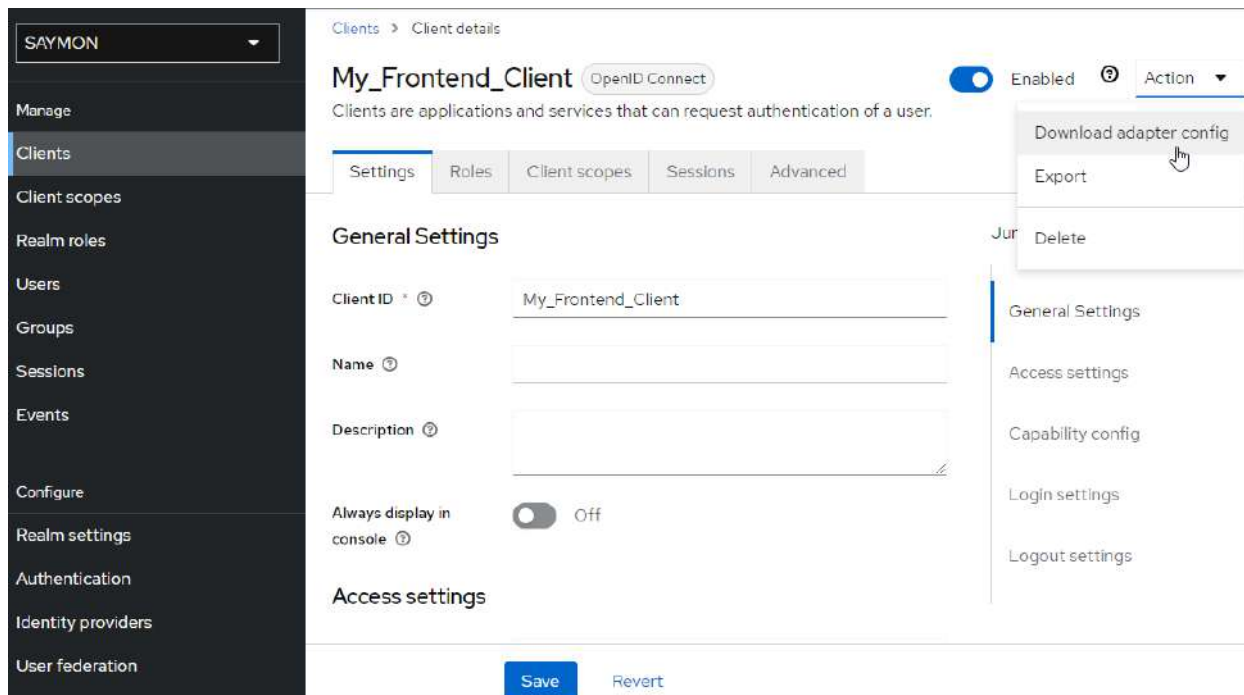


Рис. 3.5.3.2.4. Отключение клиентской аутентификации

7. Нажать кнопку **Download**, чтобы получить файл настроек соединения для Frontend-клиента в формате JSON (Рис. 3.5.3.2.5):

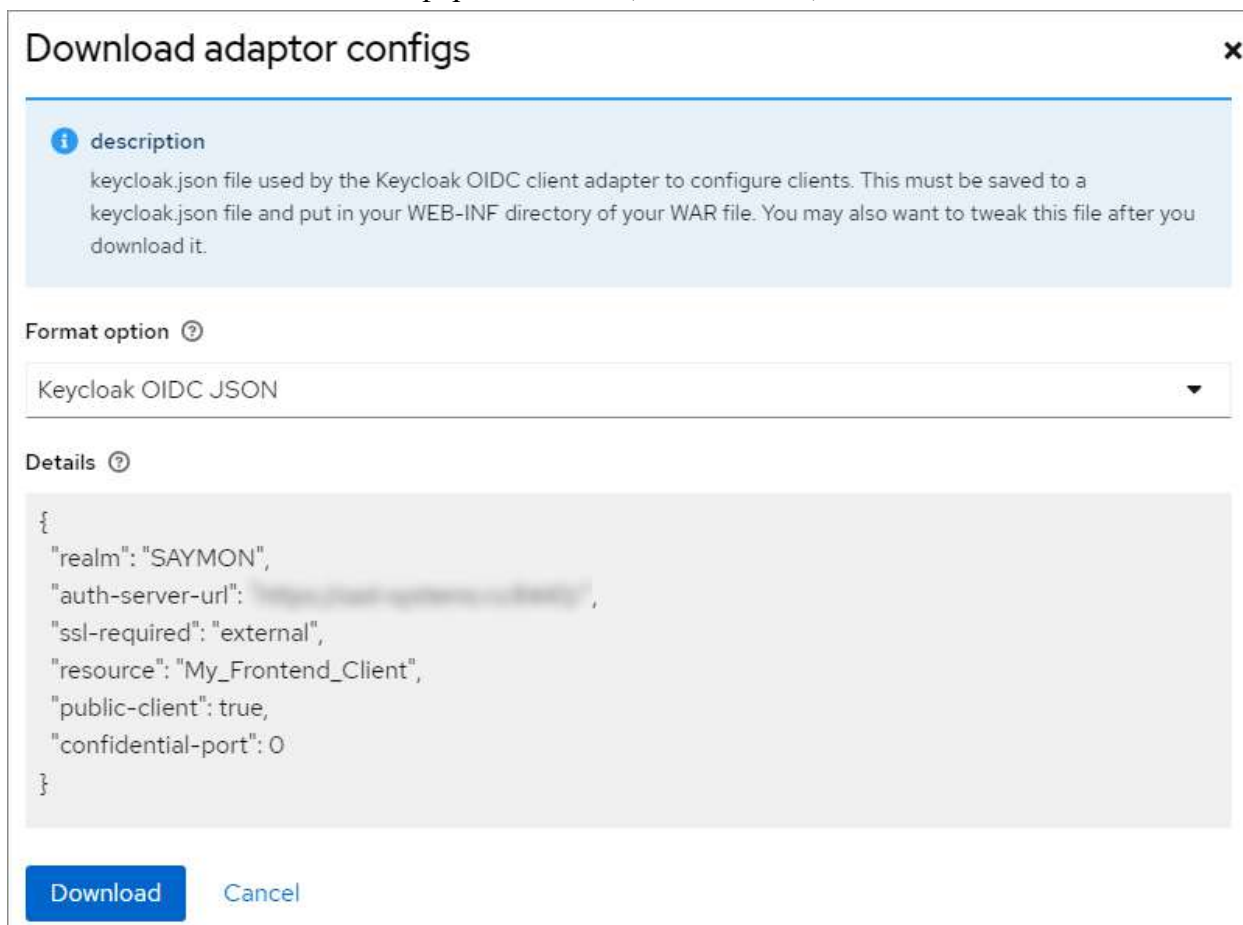


Рис. 3.5.3.2.5. Отключение клиентской аутентификации

Для активации формы авторизации через Keycloak в web-интерфейсе системы необходимо:


1. Добавить на сервере Центрального Пульта раздел **authentication** в конфигурационный файл клиента `/etc/saymon/saymon-client.yaml`

```
authentication:  
  availableMethods:  
    - native  
    - keycloak  
  methodByDefault: keycloak  
  services:  
    keycloak:  
      configUri: keycloak_frontend.json  
      legacySupport: false
```

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

где:

- **availableMethods** - список доступных для пользователей методов аутентификации;
- **methodByDefault** - метод аутентификации, который будет предложен пользователю сразу при отображении аутентификационной формы;
- **configUri** - файл настроек соединения с Keycloak-сервером (для frontend-клиента).

 Файл необходимо поместить в каталог с конфигурационным файлом клиента.

2. Обновить страницу Центрального Пульта в web-браузере.

3.6 Управление логированием

Для хранения и дальнейшего анализа изменений в системной работе агента Центральный Пульт использует логирование.

Логи агента хранятся в папках:

- Linux, Wiren Board 6 - `/var/log/saymon`;
- Mac OS X - `/opt/saymon-agent/log`;
- Windows - `папка_установки_агента\log`.

Также в журналы записывается информация о следующих событиях:

- дата и время удачных и неудачных попыток входа пользователей в систему;
- причина и время выхода пользователей из системы;
- дата, время и инициатор выполнения операций;
- факт использования прав администратора;
- факт доступа пользователей к основным конфигурационным данным платформы;
- запуск и остановка сервисов аудита действий пользователя.

Все записи имеют временной штамп, признак инициатора (ID пользователя или процесса) и признак сессии, если событие было инициировано пользователем.

3.6.1 Конфигурация log-файлов агента

Конфигурация log-файлов агента выполняется в файле

- `<PROGRAMFILES>/SAYMON Agent/conf/logback-winservice.xml` (Windows).
- `/opt/saymon-agent/conf/logback-daemon.xml` (Linux/MacOS).

Логирование выполняется на уровне INFO. При необходимости возможно дополнительно настроить debug-режим.

Агент выполняет ротацию логов раз в день, старые логи архивируются.

i *Архивация происходит в момент поступления в лог новой информации от агента. Если новых записей нет, архивация не выполняется.*

Пример секции настроек базового логирования:

```
<appender name="FILE-INFO" class="RollingFileAppender">
  <file>log/saymon-agent.info.log</file>
  <rollingPolicy class="TimeBasedRollingPolicy">
    <!-- Daily rollover -->
    <fileNamePattern>log/saymon-agent.info.%d{yyyy-MM-dd}.log.zip
</fileNamePattern>
    <!-- Keep 10 days' worth of history -->
    <maxHistory>10</maxHistory>
    <!-- Limit total size of all archive logs to 50 MB. -->
    <totalSizeCap>50MB</totalSizeCap>
  </rollingPolicy>
  <encoder class="PatternLayoutEncoder">
    <pattern>%d{dd.MM.yyyy HH:mm:ss.SSS} [%-15thread] %-5level
%logger{36} - %msg %kvp%n%rootException</pattern>
  </encoder>
</appender>
```

где:

- `<file>log/saymon-agent.info.log</file>` — размещение log-файла;
- `<fileNamePattern>... .zip</fileNamePattern>` — указание на архивацию файлов в формат .zip;
- `<maxHistory>10</maxHistory>` — длительность хранения файлов в днях;
- `<totalSizeCap>50MB</totalSizeCap>` — ограничение дискового пространства для хранения логов.

i *Полная информация о настройках доступна в [документации по Logback](#).*


Для активации debug-режима необходимо:

1. Заменить содержимое файла конфигурации log-файлов агента содержимым файла

- `logback-winservice-debug.xml` (Windows);
- `logback-daemon-debug.xml` (Linux/Mac OS).

В этом файле находится секция настроек debug-режима:

```
<appender name="FILE-DEBUG" class="RollingFileAppender">  
...  
</appender>
```

 *Файл с секцией настроек debug-режима находится в той же папке, что и файл конфигурации log-файлов агента.*

2. Перезапустить агента:
 - служба **SaymonAgent** (Windows);
 - служба **saymon-agent** (Linux/Mac OS).

3.6.2 Конфигурация ротации log-файлов сервера

Конфигурация ротации log-файлов сервера выполняется в файле `/etc/logrotate.d/saymon`.

Параметры файла конфигурации ротации log-файлов:

Параметр	Описание
<code>/var/log/saymon/saymon-rest-server.log</code> <code>/var/log/saymon/saymon-server.log</code>	Размещение log-файлов.
<code>daily</code>	Ежедневная ротация.
<code>missingok</code>	Продолжать ротацию без ошибки, если отсутствует один из файлов.
<code>rotate N</code>	Длительность хранения файлов в днях.
<code>compress</code>	Архивация файлов в формат <code>.gzip</code> .
<code>notifempty</code>	Не производить ротацию лога, если он пуст.
<code>copytruncate</code>	Писать лог в один файл, урезая его после каждого шага ротации.

3.6.3 Просмотр информации о Журнале событий

Информацию о содержании журнала событий возможно просмотреть с помощью REST API метода:

```
GET /node/api/event-log/info
```


Пример (bash):

```
login=<...>  
password=<...>  
saymon_hostname=<...>  
url=https://$saymon_hostname/node/api/event-log/info  
curl -X GET $url -u $login:$password
```

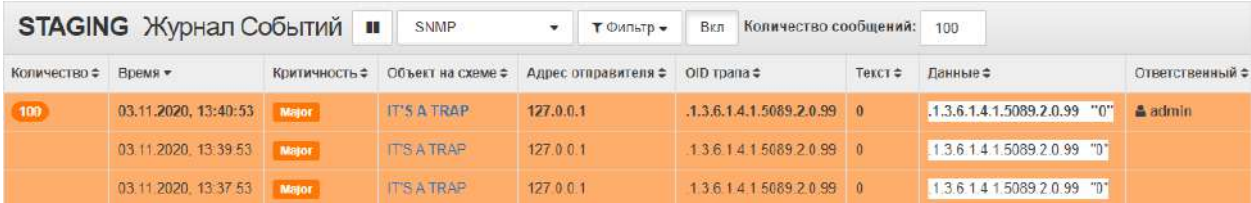
3.6.4 Назначение ответственного за событие

При возникновении критической ситуации возможно установить ответственного за неё пользователя двумя способами:

1. Через Web UI:

- 1.1. В панели режимов отображения открыть Журнал событий кнопкой .
- 1.2. Нажать правой кнопкой мыши на требуемое событие, затем выбрать пункт "Назначить ответственного".
- 1.3. Выбрать ответственного за событие из выпадающего списка.

Имя ответственного пользователя отобразится в соответствующем столбце (Рис. 3.6.4.1):



Количество	Время	Критичность	Объект на схеме	Адрес отправителя	ОID трапа	Текст	Данные	Ответственный
100	03.11.2020, 13:40:53	Мажор	IT'S A TRAP	127.0.0.1	.1.3.6.1.4.1.5089.2.0.99	0	.1.3.6.1.4.1.5089.2.0.99 "0"	admin
	03.11.2020, 13:39:53	Мажор	IT'S A TRAP	127.0.0.1	.1.3.6.1.4.1.5089.2.0.99	0	.1.3.6.1.4.1.5089.2.0.99 "0"	
	03.11.2020, 13:37:53	Мажор	IT'S A TRAP	127.0.0.1	.1.3.6.1.4.1.5089.2.0.99	0	.1.3.6.1.4.1.5089.2.0.99 "0"	

Рис. 3.6.4.1. Журнал событий

2. REST API методом:

PATCH /node/api/event-log/:id/assignee

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
record_id=<...>
url=https://$saymon_hostname/node/api/event-log/$record_id/assignee
curl -X PATCH $url -u $login:$password -H "Content-Type: application/json" \
--data '{"userId": "..."}'
```

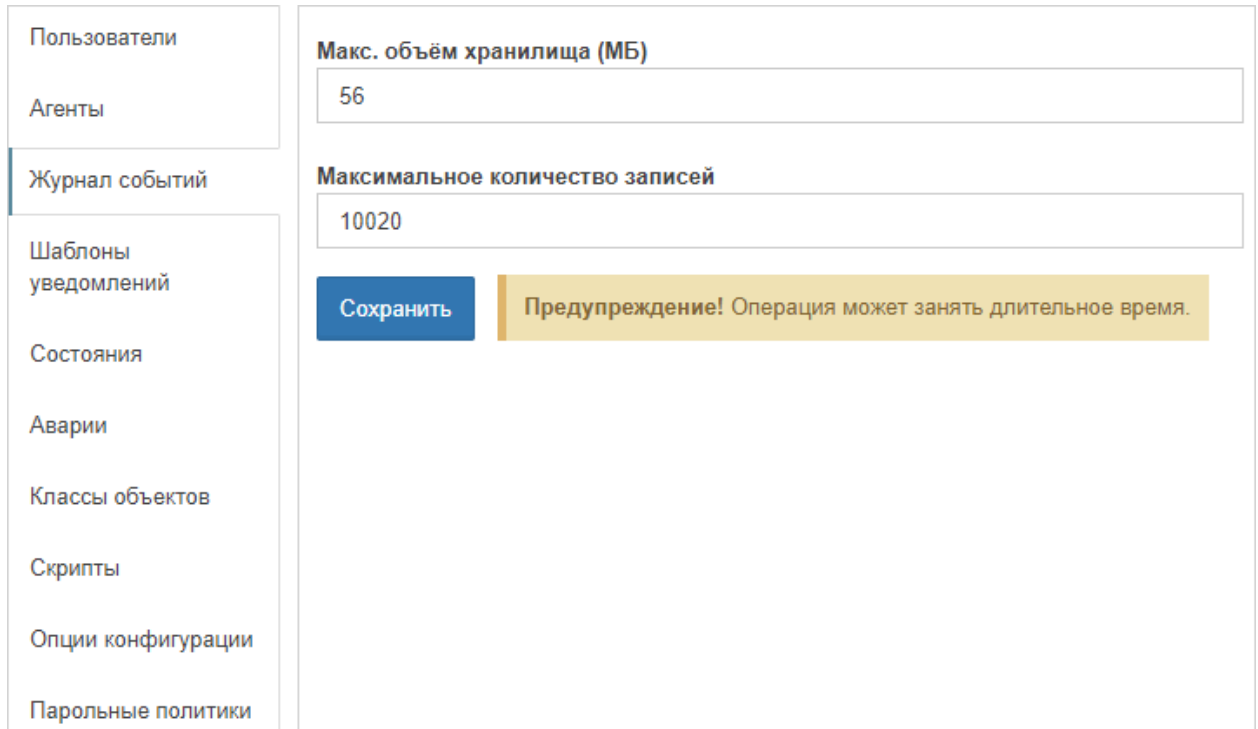
3.6.5 Установка ограничения для логирования

Центральный Пульт позволяет установить максимальный объём хранилища двумя способами:

1. Через Web UI:

1.1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".

1.2. Перейти в раздел "Журнал событий" (Рис. 3.6.5.1):



Пользователи

Агенты

Журнал событий

Шаблоны уведомлений

Состояния

Аварии

Классы объектов

Скрипты

Опции конфигурации

Парольные политики

Макс. объём хранилища (МБ)

56

Максимальное количество записей

10020

Сохранить

Предупреждение! Операция может занять длительное время.

Рис. 3.6.5.1. Журнал событий

1.3. Заполнить поля требуемыми значениями.

1.4. Сохранить изменения.

2. Через REST API метод:

PUT /node/api/event-log/limits

Пример (bash):

login=<...>

password=<...>

saymon_hostname=<...>

url=https://\$saymon_hostname/node/api/event-log/limits

```
curl -X PUT $url -u $login:$password -H "Content-Type: application/json" \  
--data '{"maxBytes": 1024, "maxRecords": 100}'
```

3.6.6 Удаление всех SNMP-Трап'ов из Журнала событий

Для очистки Журнала событий необходимо:

1. Выполнить в терминале следующие команды:

```
mongo saymon
>db.eventLog.drop()
```

2. После сброса проверить создание новой коллекции командой:

```
>db.eventLog.stats()
```

3. Если ответ выглядит следующим образом, необходимо создать новую коллекцию:

```
{ "ok" : 0, "errmsg" : "ns not found" }
```

- создание новой коллекции с лимитом по объёму в байтах:

```
>db.createCollection("eventLog", {capped:true, size: 100000000})
```

- создание новой коллекции без лимита:

```
>db.createCollection("eventLog")
```

4. Повторно проверить создание коллекции командой:

```
>db.eventLog.stats()
```

Ответ должен выглядеть примерно следующим образом:

```
{
  "ns" : "saymon.eventLog",
  "count" : 0,
  "size" : 0,
  "storageSize" : 100003840,
  "numExtents" : 1,
  "nindexes" : 1,
  "lastExtentSize" : 100003840,
  "paddingFactor" : 1,
  "systemFlags" : 1,
  "userFlags" : 0,
  "totalIndexSize" : 8176,
  "indexSizes" : {
    "_id_" : 8176
  },
  "capped" : true,
  "max" : NumberLong("9223372036854775807"),
  "ok" : 1
}
```

3.6.7 Удаление логов

Удаление логов осуществляется следующей командой в консоли:

```
sudo rm -rf /var/log/upstart/*
```

Также возможно удалить логи с помощью REST API:

```
DELETE /node/api/event-log/:id
```

Пример (bash):

```
login=<...>
```

```
password=<...>
```

```
saymon_hostname=<...>
```

```
record_id=<...>
```

```
url=https://$saymon_hostname/node/api/event-log/$record_id
```

```
curl -X DELETE $url -u $login:$password
```

3.7 Управление учётными записями пользователей

Раздел содержит информацию об администрировании пользовательских учётных записей.

Группы пользователей позволяют упростить настройку и редактирование прав пользователей. При необходимости настроить нескольким пользователям идентичные


- права на операции,
- доступы к объектам,
- права на просмотр событий в Журнале событий,


достаточно создать группу пользователей, настроить ей необходимые права и добавить в эту группу нужных пользователей. В дальнейшем возможно редактировать права группы. Пользователь может принадлежать к неограниченному числу групп.


Права пользователя и его групп суммируются. Чтобы пользователь мог выполнять те или иные действия в системе, нужно, чтобы соответствующие права были либо у самого пользователя, либо у какой-то из его групп.

3.7.1 Авторизация пользователей через LDAP

Для авторизации пользователей с помощью сервера службы каталогов (Active Directory, OpenLDAP, и т.д.) необходимо добавить секцию LDAP в конфигурационный файл сервера `/etc/saymon/saymon-server.conf`.

 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

При первом входе пользователя, аутентифицированного через LDAP, для него автоматически создаётся учётная запись в системе. У таких пользователей на вкладке "Общие" есть поле "Источник" со значением "LDAP", в списке пользователей они отмечаются иконкой .


 Если логин LDAP-пользователя совпадает с логином другого пользователя, уже зарегистрированного в системе, LDAP-пользователь авторизоваться не сможет.

Пользователям из LDAP, у которых ещё нет учётной записи в Центральном Пульте, можно ограничить вход в систему, подготовив группы для нужных пользователей. Чтобы учётная запись создавалась только для пользователей, у которых имя группы на LDAP-сервере совпадает с именем существующей (созданной ранее) группы в Центральном Пульте, в конфигурационном файле сервера необходимо указать параметр `ldap.create_user_for_existing_group_only` со значением `true`:

```
"ldap" : {  
  ...  
  "create_user_for_existing_group_only": true,  
  ...  
}
```

При использовании протокола LDAP во время авторизации пользователя в системе могут быть автоматически созданы группы с именами, эквивалентными именам групп из LDAP, которые отсутствуют в Центральном Пульте. Авторизовавшийся пользователь автоматически добавляется в импортированные группы. В конфигурационном файле сервера для этого необходимо указать параметр `ldap.import_non_existing_groups` со значением `true`:

```
"ldap" : {  
  ...  
  "import_non_existing_groups": true,  
  ...  
}
```

LDAP-группы - группы, созданные при авторизации LDAP-пользователей - обозначаются в списке иконкой . Для таких групп недоступна смена имени, в качестве источника указан LDAP.

Группы, созданные в Центральном Пульте, имена которых совпадают с именами групп из LDAP, можно обновить до LDAP-групп. В конфигурационном файле сервера для этого необходимо указать параметр **ldap.update_existing_groups** со значением **true**:

```
"ldap" : {  
  ...  
  "update_existing_groups": true,  
  ...  
}
```

В этом случае при авторизации LDAP-пользователя те группы в Центральном Пульте, для которых есть одноимённые группы среди групп пользователя в LDAP, будут обновлены до LDAP-групп.




Если пользователь был исключён из группы в Центральном Пульте - аналога своей группы в LDAP, при следующем входе в систему пользователь автоматически будет возвращён в эту группу.


3.7.2 Авторизация пользователей через Keycloak


Для авторизации пользователей с помощью внешнего сервера Keycloak необходимо:


- выполнить настройку клиентов и получить необходимые параметры в консоли администратора Keycloak;

 *Описание необходимых действий в консоли администратора Keycloak приведено в подразделе 3.5.3 "Интеграция с Keycloak" на стр. 92.*

- добавить секцию **Keycloak** в конфигурационный файл сервера `/etc/saymon/saymon-server.conf`;

 *Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.*

При первом входе пользователя, аутентифицированного через Keycloak, для него автоматически создаётся учётная запись в системе. У таких пользователей на вкладке "Общие" есть поле "Источник" со значением " Keycloak", в списке пользователей они отмечаются иконкой .

 *Если логин Keycloak-пользователя совпадает с логином другого пользователя, уже зарегистрированного в системе, Keycloak-пользователь авторизоваться не сможет.*

3.7.3 Создание учётной записи

При создании пользователей и групп в именах и паролях допускаются любые символы, кроме символа @.

Создание учётных записей пользователей осуществляется двумя способами:

1. Через Web UI:
 - 1.1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
 - 1.2. Перейти в раздел "Журнал событий" (Рис. 3.7.3.1):

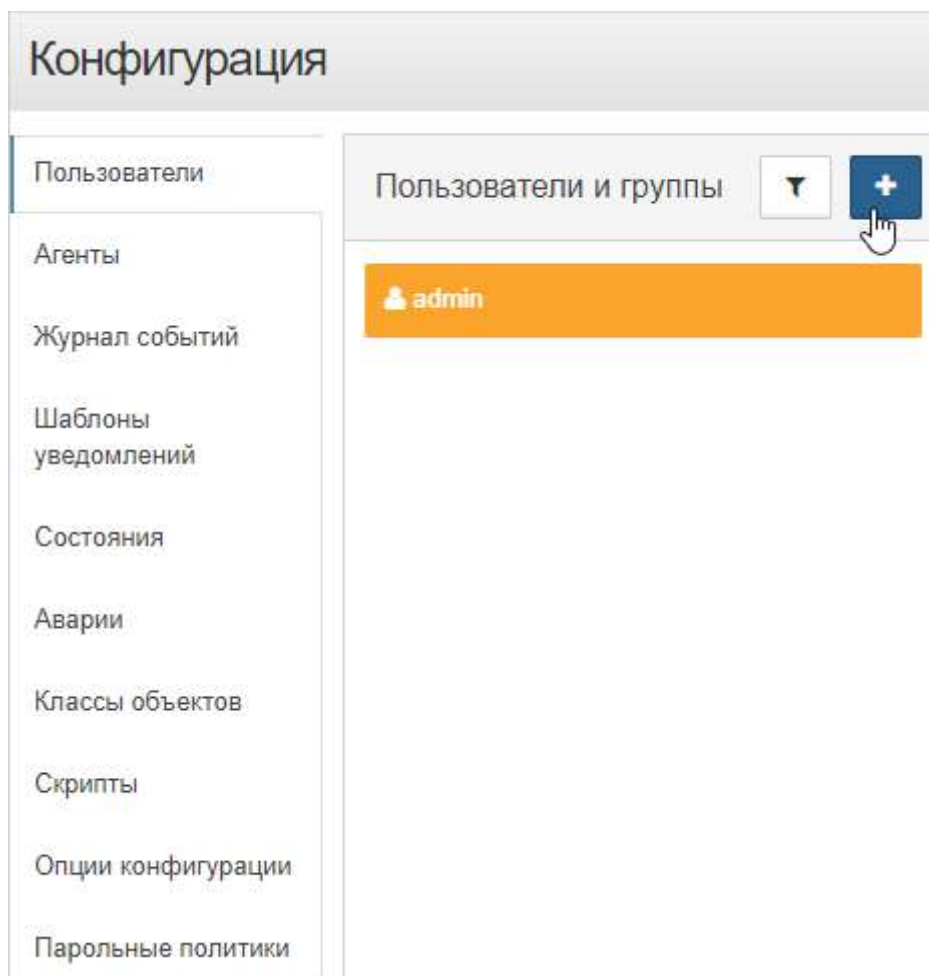




Рис. 3.7.3.1. Журнал событий

- 1.3. Нажать кнопку  и выбрать добавление пользователя.
- 1.4. Ввести логин пользователя, пароль и подтверждение.
- 1.5. Нажать кнопку .

2. Через REST API:

POST /node/api/users

Пример (bash)

```
login=<...>
password=<...>
saymon_hostname=<...>
url=https://$saymon_hostname/node/api/users

curl -X POST $url -u $login:$password -H "Content-Type: application/json" \
-d @- <<EOF
{
  "login": "Bob",
  "password": "qwerty",
  "permissions": [
    "manage-objects",
    "manage-links"
  ]
}
EOF
```

3.7.4 Назначение пользователям прав доступа

i Список операций с подробным описанием содержится в Приложении А на стр. 173.

Настройка прав пользователей осуществляется двумя способами:

1. Через Web UI:

- 1.1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
- 1.2. Перейти в раздел "Пользователи".
- 1.3. Выбрать нужного пользователя или группу из списка.
- 1.4. Открыть вкладку "Права на операции" (Рис. 3.7.4.1):

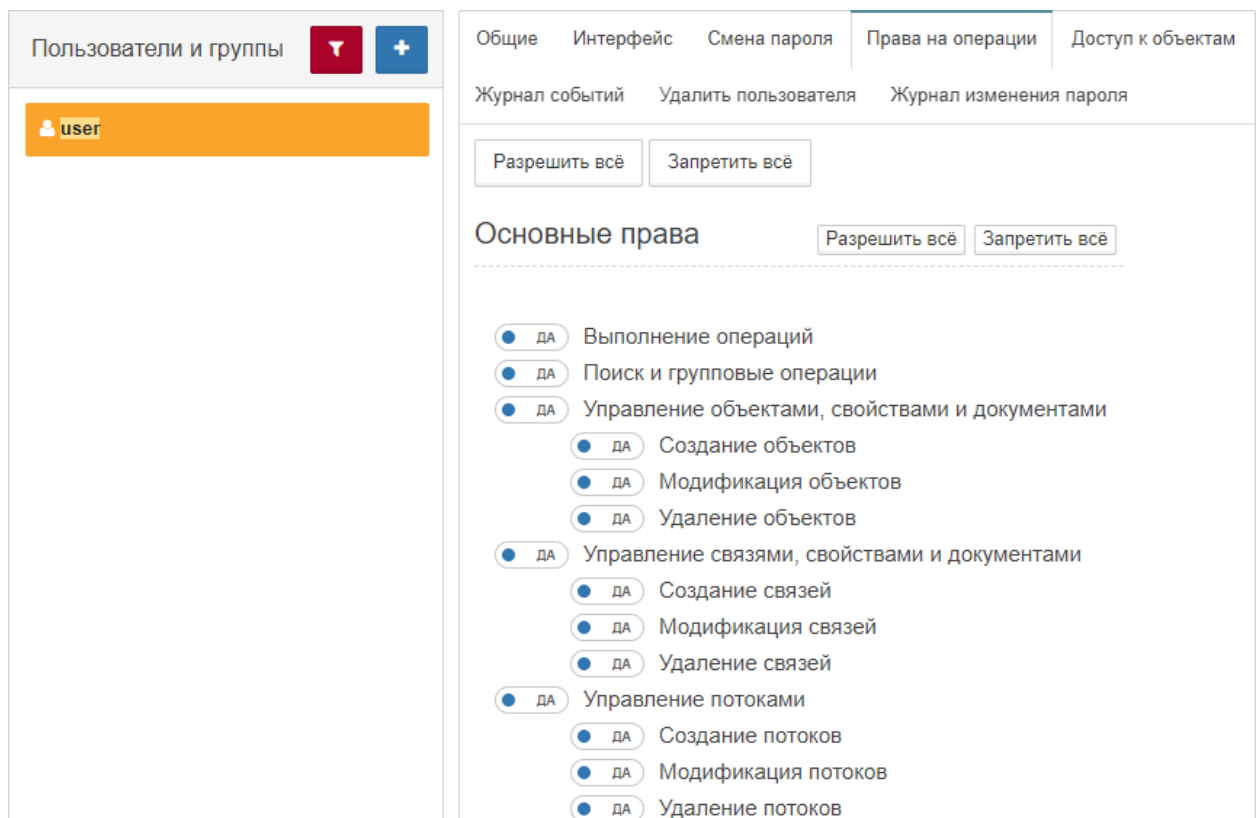


Рис. 3.7.4.1. Права на операции

1.5. Отредактировать права пользователя или группы.

⚠ Если пользователь принадлежит к группам, права пользователя и его групп суммируются.

2. Через REST API:

PATCH /node/api/users/:id

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
user_id=<...>
url=https://$saymon_hostname/node/api/users/$user_id
curl -X PATCH $url -u $login:$password -H "Content-Type: application/json" \
-d @- <<EOF
{
  "login": "Bob",
  "password": "qwerty",
  "permissions": [
    "manage-objects",
    "manage-links"
  ]
}
EOF
```

3.7.5 Назначение парольных политик

Настройка парольных политик осуществляется через Web UI.

1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
2. Перейти в раздел "Парольные политики" (Рис. 3.7.5.1):

Конфигурация		
Пользователи	Парольные политики	Редактирование политики
Журнал сессий	По умолчанию	Имя: По умолчанию
Агенты		Минимальное количество символов: <input checked="" type="radio"/> ДА 8
Журнал событий		Минимальное количество символов нижнего регистра: <input checked="" type="radio"/> ДА 1
Шаблоны уведомлений		Минимальное количество символов в верхнем регистре: <input checked="" type="radio"/> ДА 1
Состояния		Минимальное количество цифр: <input checked="" type="radio"/> ДА 1
Аварии		Минимальное количество специальных символов: <input checked="" type="radio"/> ДА 1
Классы объектов		Количество уникальных паролей: <input checked="" type="radio"/> ДА 1
Скрипты		Пользователь должен сменить пароль при первом входе: <input checked="" type="radio"/> ДА
Опции конфигурации		Срок действия пароля (дни): <input checked="" type="radio"/> ДА 180
Парольные политики		Период, за который пользователя необходимо уведомить об окончании срока действия его пароля (дни): <input checked="" type="radio"/> ДА 1
		<input checked="" type="button" value="Применить"/>

Рис. 3.7.5.1. Парольные политики

3. Установить необходимые требования к паролям пользователей.
4. Нажать кнопку .

3.7.6 Изменение пароля от учётной записи

Смена пароля пользователей осуществляется двумя способами:

1. Через Web UI:
 - 1.1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
 - 1.2. Перейти в раздел "Пользователи".
 - 1.3. Выбрать нужного пользователя из списка.
 - 1.4. Открыть вкладку "Смена пароля" (Рис. 3.7.6.1):

The screenshot shows the 'Users and Groups' management interface. On the left, a list of users is shown with 'user' selected. The main panel has several tabs: 'Общие', 'Интерфейс', 'Смена пароля' (selected), 'Права на операции', and 'Доступ к объектам'. Below these are sub-tabs: 'Журнал событий', 'Удалить пользователя', and 'Журнал изменения пароля'. The 'Смена пароля' tab contains a form with two input fields: 'Новый пароль' and 'Подтверждение пароля'. Below the fields, it displays 'Текущие требования парольной политики:' with a bullet point: '• количество уникальных паролей - 2'. A blue 'Сохранить' button is positioned below the form. At the bottom, there is a toggle switch for 'Сменить пароль при следующем входе:' which is currently set to 'НЕТ'.

Рис. 3.7.6.1. Смена пароля пользователя

- 1.5. Ввести новый пароль пользователя и подтверждение.

⚠ При смене собственного пароля необходимо также ввести текущий пароль.

- 1.6. Нажать кнопку

Сохранить

2. Через REST API:

```
PUT /node/api/users/:id/password
```

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
user_id=<...>
url=https://$saymon_hostname/node/api/users/$user_id/password
curl -X PUT $url -u $login:$password -H "Content-Type: application/json" \
-d @- <<EOF
{
  "currentPassword": "qwerty",
  "newPassword": "qwerty_qwerty"
}
EOF
```

3.7.7 Настройка доступа к объектам

Настройка доступа к объектам осуществляется через Web UI.

1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
2. Перейти в раздел "Пользователи".
3. Выбрать нужного пользователя или группу из списка.
4. Открыть вкладку "Доступ к объектам" (Рис. 3.7.7.1):

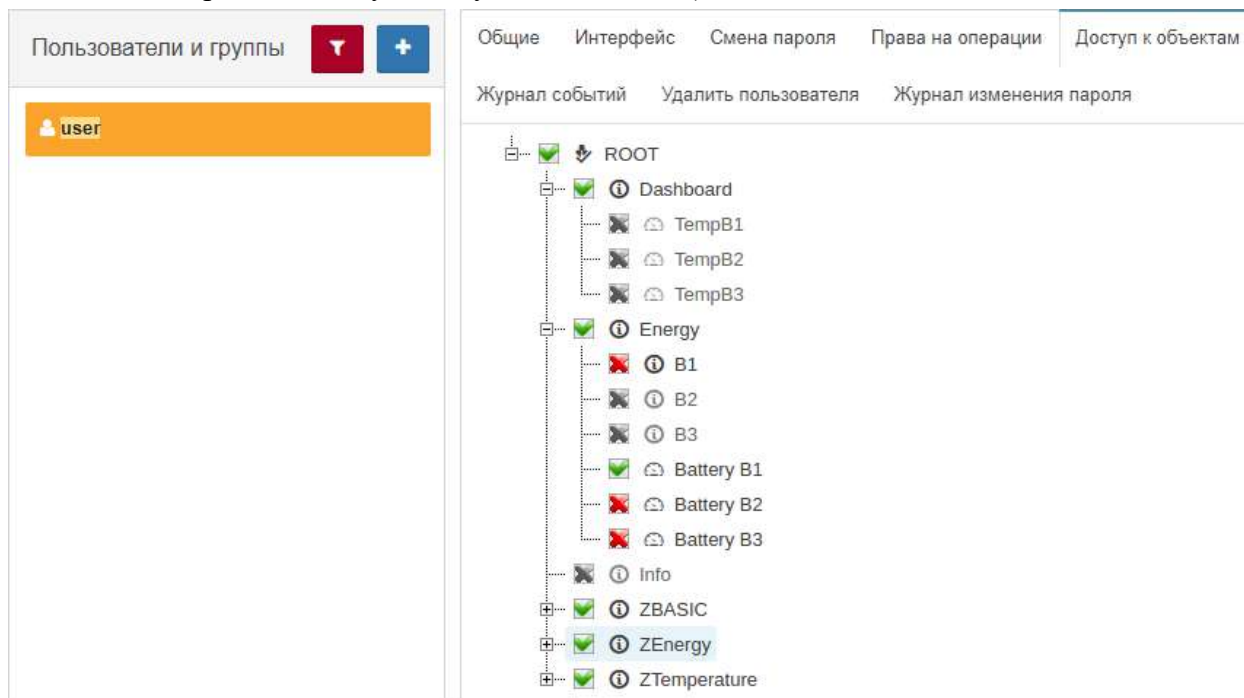



Рис. 3.7.7.1. Доступ к объектам

5. Отметить объекты, к которым необходимо предоставить/заблокировать доступ.

 *Объекты, недоступные для группы, становятся недоступными для всех членов группы.*

3.7.8 Блокировка учётной записи

Блокировка учётных записей пользователей осуществляется двумя способами:

1. Через Web UI:
 - 1.1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
 - 1.2. Перейти в раздел "Пользователи".
 - 1.3. Выбрать нужного пользователя из списка.
 - 1.4. Открыть вкладку "Общие" (Рис. 3.7.8.1):

Общие	Интерфейс	Смена пароля	Права на операции	Доступ к объектам	Журнал событий								
Удалить пользователя		Журнал изменения пароля											
ID	58048d843bddd07007607034												
Логин	demo												
Email	<input type="text"/>												
Язык	English												
Статус	Активен												
Активен до	DD.MM.YYY <input type="text"/> <input type="text"/>												
Группа	-- Не выбрано --												
Ссылка для авторизации	<input type="text"/>												
Активность	<table border="1"><thead><tr><th>⌚ Время</th><th>⚡ Действие</th><th>* Тип</th><th>Разница</th></tr></thead><tbody><tr><td>07.12.2022, 15:58:39</td><td>Удалено</td><td>Session</td><td><pre>↑ {"id": "09d30aed-583e-4e6b-82e5-f97187627db9", "userId": "58048d843bddd07007607034", "tokenId": "a6060167-61b1-4e78-ba79-daaa9eeefba0"} ↓</pre></td></tr></tbody></table>					⌚ Время	⚡ Действие	* Тип	Разница	07.12.2022, 15:58:39	Удалено	Session	<pre>↑ {"id": "09d30aed-583e-4e6b-82e5-f97187627db9", "userId": "58048d843bddd07007607034", "tokenId": "a6060167-61b1-4e78-ba79-daaa9eeefba0"} ↓</pre>
⌚ Время	⚡ Действие	* Тип	Разница										
07.12.2022, 15:58:39	Удалено	Session	<pre>↑ {"id": "09d30aed-583e-4e6b-82e5-f97187627db9", "userId": "58048d843bddd07007607034", "tokenId": "a6060167-61b1-4e78-ba79-daaa9eeefba0"} ↓</pre>										

Рис. 3.7.8.1. Общие параметры пользователя

- 1.5. В выпадающем списке "Статус" выбрать "Заблокирован".

В поле **Активен до** можно задать дату и время блокировки учётной записи. При наступлении указанного времени статус учётной записи будет автоматически изменён на **Заблокирован**.

⚠ В случае если указанное время меньше текущего, статус учётной записи немедленно изменяется на **Заблокирован.**

2. Через REST API:

PATCH /node/api/users/:id

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
user_id=<...>
url=https://$saymon_hostname/node/api/users/$user_id/password
curl -X PATCH $url -u $login:$password -H "Content-Type: application/json" \
-d @- <<EOF
{
  "status": "3",
}
EOF
```

3.7.9 Удаление учётной записи

Удаление учётных записей осуществляется двумя способами:

1. Через Web UI:

- 1.1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
- 1.2. Перейти в раздел "Пользователи".
- 1.3. Выбрать нужного пользователя из списка.
- 1.4. Открыть вкладку "Удалить пользователя" (Рис. 3.7.9.1):

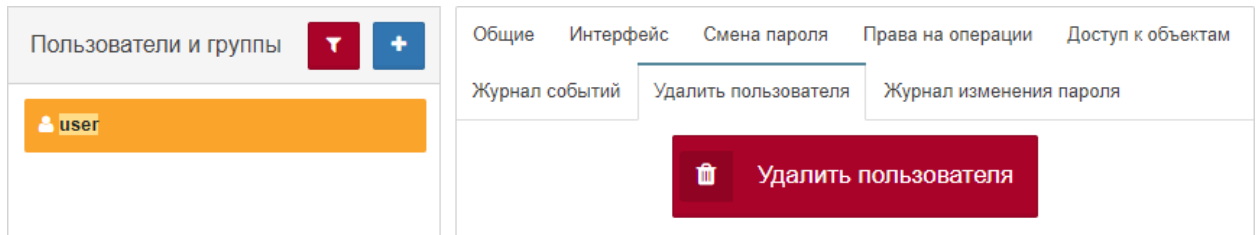


Рис. 3.7.9.1. Удаление пользователя

- 1.5. Нажать кнопку удаления пользователя.
 - 1.6. Подтвердить удаление во всплывающем окне.
2. Через REST API:

```
DELETE /node/api/users/:id
```

Пример (bash):

```
login=<...>  
password=<...>  
saymon_hostname=<...>  
user_id=<...>  
url=http://$saymon_hostname/node/api/users/$user_id  
curl -X DELETE $url -u $login:$password
```



После удаления учётной записи пользователя LDAP/Keycloak с сервера системы пользователь по-прежнему сможет войти в систему под своими учётными данными, авторизовавшись через LDAP/Keycloak. Учётная запись при этом будет создана заново с правами по умолчанию; права, полученные через группы, останутся прежними.

Чтобы заблокировать такому пользователю доступ к данным, достаточно сменить его статус на **Заблокирован**.

3.8 Работа с объектами и связями

Вся управляемая инфраструктура в системе представлена в виде объектов и связей между ними.

Все метрики, характеризующие текущее состояние платформы, связываются с отдельными объектами мониторинга. Контроль загрузки и наличия свободных ресурсов осуществляется стандартными средствами платформы.

3.8.1 Создание объекта

Создать объект можно двумя способами:

1. Через Web UI:

1.1. Нажать кнопку  на панели инструментов.

1.2. В окне "Новый объект" ввести имя объекта и выбрать класс объекта (Рис. 3.8.1.1):

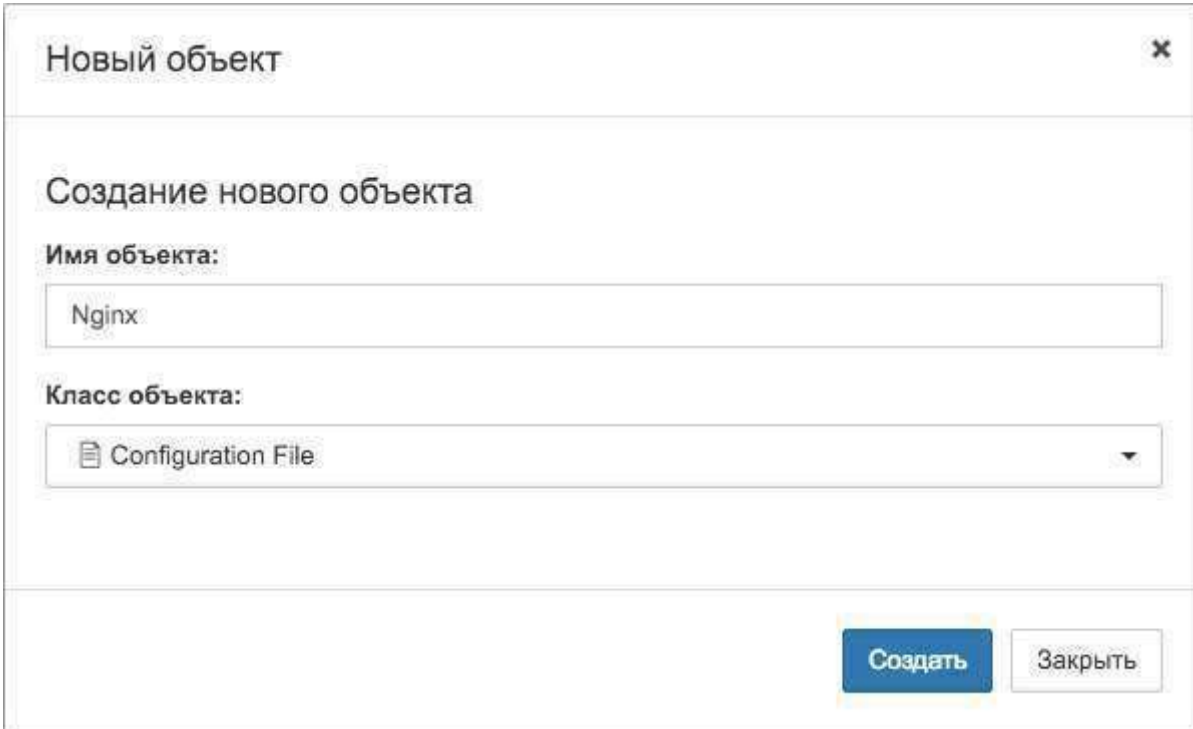


Рис. 3.8.1.1. Окно создания нового объекта

1.3. Нажать кнопку .

2. Через REST API:

POST /node/api/objects

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
url=https://$saymon_hostname/node/api/objects
curl -X POST $url -u $login:$password -H "Content-Type: application/json" \
-d @- <<EOF
{
  "name": "New Object",
  "parent_id": "1",
  "class_id": "3"
}
EOF
```

 "parent_id" - ID родительского объекта для создаваемого.

3.8.2 Клонирование объекта

Объект клонируется со всеми своими документами, параметрами, свойствами дочерними объектами и связями.

Клонировать объект можно двумя способами:

1. Через Web UI:
 - 1.1. Вызвать контекстное меню клонируемого объекта щелчком правой кнопкой мыши.
 - 1.2. Выбрать пункт меню "Клонировать".
2. Через REST API:


POST /node/api/objects/:id/clone

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
object_id=<...>
url=https://$saymon_hostname/node/api/objects/$object_id/clone
curl -X POST $url -u $login:$password
```


3.8.3 Удаление объекта

Удалить объект можно тремя способами:

1. Через Web UI (контекстное меню объекта):
 - 1.1. Вызвать контекстное меню удаляемого объекта щелчком правой кнопкой мыши.
 - 1.2. Выбрать пункт меню "Удалить".
 - 1.3. Подтвердить удаление объекта во всплывающем окне.
2. Через Web UI (режим удаления элементов):
 - 2.1. Нажать кнопку  на панели хлебных крошек.
 - 2.2. Нажать на такую же иконку на удаляемом объекте.
 - 2.3. Подтвердить удаление объекта во всплывающем окне.
3. Через REST API:

DELETE /node/api/objects/:id

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
object_id=<...>
url=https://$saymon_hostname/node/api/objects/$object_id
curl -X DELETE $url -u $login:$password
```

3.8.4 Создание ссылки на объект

Ссылка представляет собой особый тип объекта и служит для отображения уже настроенных в инфраструктуре объектов в других её частях, например, в дашбордах.

С помощью ссылок можно создавать связи и потоки между объектами, которые находятся в разных частях инфраструктуры.

Создать ссылку можно двумя способами:

1. Через Web UI:

1.1. Нажать кнопку  на панели инструментов.

1.2. В появившемся всплывающем окне **Новая ссылка** (Рис. 3.8.4.1) выбрать из выпадающего списка объект, на который создаётся ссылка:

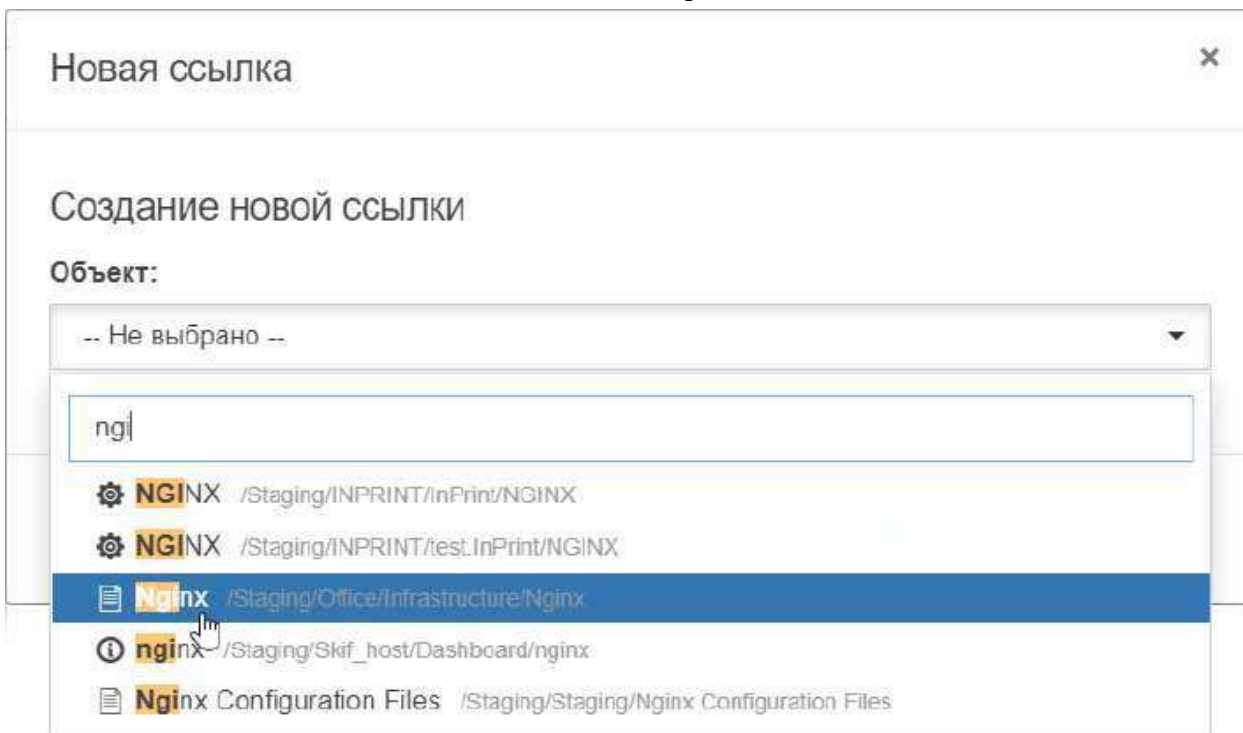


Рис. 3.8.4.1. Окно создания нового объекта

1.3. Нажать кнопку .

2. Через REST API:

POST /node/api/refs

Пример (bash):

```
login=<...>
password=<...>
saymon_hostname=<...>
url=https://$saymon_hostname/node/api/refs
curl -X POST $url -u $login:$password -H "Content-Type: application/json" \
--data '{"target": "5e60d9db630502472925fe9f", "owner": "1"}
```


3.8.5 Создание связи


Связь может отражать как физическое соединение между объектами (например, соединение сервера с маршрутизатором с помощью Ethernet-кабеля), так и логическое отношение (например, поток данных от одного программного компонента к другому).

Связи между объектами также могут являться объектами мониторинга.

Создать связь можно двумя способами:

1. Через Web UI:

1.1. Перейти в режим создания связей, нажав кнопку  на панели инструментов.

1.2. После того, как на всех объектах появится соответствующий символ , нажать на него на исходном объекте и, удерживая, переместить курсор на целевой объект (Рис. 3.8.5.1):

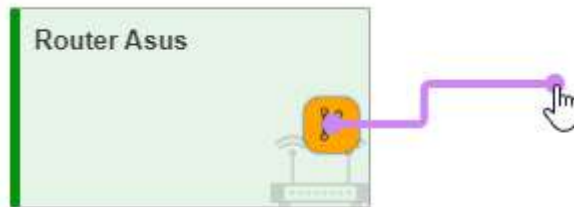


Рис. 3.8.5.1. Создание связи

Созданная связь отобразится между выбранными объектами (Рис. 3.8.5.2):

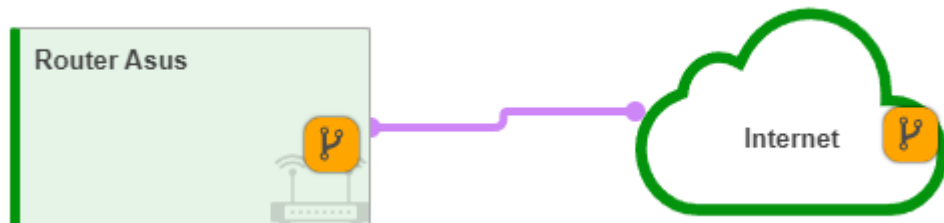



Рис. 3.8.5.2. Связь между объектами

1.3. Нажать кнопку  в верхней части главного экрана для выхода из режима создания связей.

2. Через REST API:

POST /node/api/links

Пример (bash):


```
login=<...>
password=<...>
saymon_hostname=<...>
source_obj_id=<...>
target_obj_id=<...>
url=https://$saymon_hostname/node/api/links

curl -X POST $url -u $login:$password -H "Content-Type: application/json" \
-d @- <<EOF
{
  "source": "$source_obj_id",
  "target": "$target_obj_id"
}
EOF
```

3.8.6 Удаление связи

Удалить связь можно двумя способами:

1. Через Web UI:

- 1.1. Нажать кнопку  на панели хлебных крошек.
- 1.2. Нажать на такую же иконку на удаляемой связи.
- 1.3. Подтвердить удаление связи во всплывающем окне.

2. Через REST API:

```
DELETE /node/api/links/:id
```

Пример (bash):


```
login=<...>  
password=<...>  
saymon_hostname=<...>  
link_id=<...>  
url=https://$saymon_hostname/node/api/links/$link_id  
curl -X DELETE $url -u $login:$password
```

3.9 Настройка интерфейса


В разделе описаны механизмы настройки элементов интерфейса для лучшей визуализации данных.

3.9.1 Выравнивание/расстановка объектов в стандартном виде

Выравнивание объектов в стандартном виде происходит благодаря сетке.

Для отображения/скрытия сетки необходимо нажать кнопку  на панели "хлебных крошек".

Настройки сетки выполняется в файле `/etc/saymon/saymon-client.yaml`

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

В секции **Grid** этого файла можно задать параметры:

- **border** - максимальный отступ границы объекта от границы сетки (в пикселях).
- **color** - цвет сетки в формате RGBA.
- **dim** - размер сетки (в пикселях).


```
grid:  
  dim: 20  
  color: rgba(128, 128, 128, 0.3)  
  border: 4
```

После внесения изменений в файл необходимо обновить страницу в браузере.

3.9.2 Настройка заголовка web-интерфейса

Для изменения заголовка в web-интерфейсе:

1. Открыть файл `/etc/saymon/saymon-client.yaml`.

 Подробную информацию о файле `/etc/saymon/saymon-client.yaml` см. в подразделе 3.1.4 "Настройка элементов web-интерфейса" на стр. 49.

2. В строке **title** ввести желаемое имя:

```
title: <your-new-name>
```

3. Обновить страницу браузера.

3.9.3 Перемещение/отключение фоновой иконки объекта

Все предустановленные классы объектов имеют индивидуальную фоновую иконку. При необходимости переместить иконку, в секции **Параметры** во вкладке **Стили** объекта необходимо добавить:

```
.object-background {  
background-position: 9px 8px !important;  
background-size: 15px;  
opacity: 1;  
}  
  
.object-caption-panel {  
padding-left: 15px;  
}
```

Для отключения иконки требуется добавить в ту же секцию:

```
.background-component {  
display: none  
}
```

3.9.4 Вертикальное отображение имени объекта

По умолчанию имя объекта отображается в его левом верхнем углу горизонтально. При необходимости отображать имя вертикально, в секции "Параметры" во вкладке "Стили" объекта необходимо добавить:

```
.js-caption {  
  writing-mode: vertical-lr;  
  text-orientation: upright;  
  text-transform: uppercase;  
  letter-spacing: 1px;  
}
```

3.9.5 Редактирование стилей состояний

В процессе мониторинга в зависимости от данных, получаемых от агента, объект может менять состояние.

Каждое состояние имеет цвет. Цвет и стиль состояний можно изменить двумя способами:


1. Через Web UI:
 - 1.1. В панели инструментов нажать на имя пользователя и выбрать в меню пункт "Конфигурация".
 - 1.2. Перейти в раздел "Состояния".
 - 1.3. В списке состояний выбрать то, которое требуется изменить.
 - 1.4. При необходимости изменить имя в соответствующем поле.
 - 1.5. Настроить основной цвет, цвет тени, цвет строки таблицы и фон при помощи цветовой палитры или методом ввода номера цвета.
2. Через файл конфигурации:
 - 2.1. Создать файл: `/usr/local/saymon/saymon.local/css/saymon.local.css`.
 - 2.2. Открыть его в текстовом редакторе и вставить код для изменения цвета состояния или его фона. Например:

```
.state-4
{
  background-color: rgba(255, 122, 0, 0.46);
  box-shadow: 2px 5px 10px rgba(253, 118, 7, 0.5);
  border-left: 5px solid #FD7607;
}
.state-bg-4
{
  background-color: #FD7607;
}
.view-screen-element ul li.state-4
{
  border-left: 5px solid #FD7607;
}
.view-screen-element ul li .badge.state-4
{
  background-color: #FD7607;
}
```

Номер состояния соответствует его ID.

3.10 Настройка мониторинга

Платформа "Центральный Пульт" позволяет осуществлять мониторинг с использованием различных типов проверок. Проверки настраиваются в web-интерфейсе системы.

 Подробную информацию о каждом типе проверок см. в "Руководстве пользователя" в подразделе. 4.2.1 "Настройка процесса мониторинга и типов проверок" на стр. 43.

Далее рассмотрены несколько примеров процесса мониторинга.

3.10.1 Мониторинг основных параметров ПК

Для мониторинга основных параметров работы сервера или ПК: CPU, File System, Memory и Network IO, достаточно выполнить несколько действий:

1. Установить агента на наблюдаемый ПК или сервер.
2. Создать объект, например, класса **Host**, в web-интерфейсе.
3. Перейти в созданный объект и добавить внутри него объекты классов:
 - **Saymon Agent**,
 - **CPU**,
 - **File System**,
 - **Memory**,
 - **Network IO**.
4. Сконфигурировать и запустить агента.

Через некоторое время информация об основных параметрах работы компьютера начнёт поступать на сервер и отображаться в web-интерфейсе системы.

3.10.2 Мониторинг процесса памяти

Для настройки мониторинга процесса памяти необходимо:

1. Установить, сконфигурировать и запустить агента на наблюдаемом ПК или сервере.
2. Создать объект, например, класса **Process**, в web-интерфейсе.
3. Перейти в созданный объект и в его секции **Мониторинг**:
 - выбрать агента, установленного ранее на данный компьютер;
 - выбрать тип проверки **Процесс по имени**;
 - заполнить необходимые поля.

Через некоторое время информация о проверяемом процессе начнёт поступать на сервер и отображаться в web-интерфейсе системы.

3.10.3 Мониторинг изменения файлов и папок

Для настройки мониторинга изменения файлов и папок сервера или ПК необходимо:

1. Установить, сконфигурировать и запустить агента на наблюдаемом ПК или сервере.
2. Создать объект, например, класса **Configuration File**, в web-интерфейсе.
3. Перейти в созданный объект и в его секции **Мониторинг**:
 - выбрать агента, установленного ранее на данный компьютер;
 - выбрать тип проверки **Конфигурационный файл / директория**;
 - указать путь к проверяемому файлу/директории.

Через некоторое время информация о проверяемом файле/директории начнёт поступать на сервер и отображаться в web-интерфейсе системы.

3.10.4 Проверка доступности web-ресурса

Данный тип мониторинга позволяет убедиться не только в работоспособности web-сайта (статус 200 ОК), но и в ограничении доступа к таким ресурсам, как панель администрирования баз данных. В этом случае статус "403 Forbidden" или "404 Not Found" будет говорить о правильности настройки системы, а иной статус - о возможной угрозе безопасности системы.

Для проверки доступности и скорости отклика web-ресурса необходимо:

1. Установить, сконфигурировать и запустить агента на наблюдаемом ПК или сервере.
2. Создать объект, например, класса **Address**, в web-интерфейсе.
3. Перейти в созданный объект и в его секции **Мониторинг**:
 - выбрать агента, который будет выполнять проверку;
 - выбрать тип проверки **HTTP-запрос**;
 - выбрать тип запроса **GET**;
 - в поле **URL** указать адрес web-сайта.

Через некоторое время информация о доступности и скорости отклика наблюдаемого ресурса начнёт поступать на сервер и отображаться в web-интерфейсе системы.

3.10.5 Безагентный мониторинг web-сервера

Существует ряд случаев, при которых установка агента на сервере невозможна. В таких случаях рекомендуется написать скрипт, который с заданной периодичностью будет выполняться на сервере, собирать необходимые данные и генерировать текстовый файл с результатами в формате JSON по ссылке, доступной извне.

Для мониторинга параметров web-сервера, на который невозможно поставить агента, необходимо:

1. Написать локальный скрипт, выполняющий подготовку данных (например, в папке загрузок: `.../downloads/scripts/webserver_stat.sh`):

```
#!/bin/bash
# Сбор параметров работы web-сервера.

# использование Memory
memUsage=$(free -m | grep Mem | perl -pe 's/Mem:\s+\S+\s+(\S+).*/$1/')

# использование Swap
swapUsage=$(free -m | grep Swap | perl -pe 's/Swap:\s+\S+\s+(\S+).*/$1/')

# загрузка CPU
cpuUsage=$(uptime | awk '{print $10}' | perl -pe 's/,//')

# проверка выполнения какого-либо скрипта, например, webserver_stat.sh
scriptExec=$(ps -ef | grep webserver_stat.sh | grep -v grep | wc -l)

# Write JSON response
echo "{\"memUsageMB\":\"$memUsage\", \"swapUsageMB\":\"$swapUsage\",
\"cpuUsage\":\"$cpuUsage\", \"scriptExec\":\"$scriptExec\"}" >
webserver_stat.json
```

2. Добавить выполнение скрипта в планировщик заданий cron.
3. Установить, сконфигурировать и запустить хотя бы одного агента в инфраструктуре.
4. Создать объект, например, класса **Info**, в web-интерфейсе.
5. Перейти в созданный объект и в его секции **Мониторинг**:
 - выбрать агента, который будет выполнять проверку;
 - выбрать тип проверки **HTTP-запрос**;
 - выбрать тип запроса **GET**;
 - в поле **URL** указать адрес JSON-файла.

Через некоторое время информация о параметрах работы web-сервера начнёт поступать на сервер и отображаться в web-интерфейсе системы.

3.11 Страницы для внедрения в IFrame

Виджет IFrame, предназначенный для внедрения в интерфейс содержимого сторонних ресурсов, можно также использовать и со специально настроенными информационными страницами внутри Центрального Пульта.

3.11.1 Страница с авариями

В адресной строке страницы аварий возможно указать дополнительные URL-параметры, влияющие на представление панели элементов управления и отображение данных в таблице.

Пример для отключения всех элементов управления, кроме кнопки экспорта данных в Excel, и применения ранее сохранённого фильтра **Major** (вместо **127.0.0.1** указать адрес нужного сервера Центрального Пульта):

`http://127.0.0.1/incidents.html?header=off&exportSection=on&filterName=Major`

Параметры элементов управления (часть 1 из 2):

Параметр	Описание
header	Включает/выключает отображение панели, содержащей элементы управления фильтрацией данных в таблицах; <ul style="list-style-type: none">• on - отображение панели включено,• off - отображение панели выключено. По умолчанию - on - отображение панели включено. <i>При выключенном отображении панели элементов управления выключаются все описанные в таблице элементы. В этом случае, при необходимости включить отдельный элемент, нужно отдельно вписать его в адресную строку со значением on.</i>
cache	Включает/выключает загрузку сделанных пользователем настроек из кэша браузера: будут ли настройки сохраняться при обновлении страницы браузера; <ul style="list-style-type: none">• on - загрузка настроек включена,• off - загрузка настроек выключена.
entityHref	Включает/выключает отображение ссылок на аварийные элементы в столбце Объект/связь; <ul style="list-style-type: none">• on - отображение ссылок включено,• off - отображение ссылок выключено.
exportSection	Включает/выключает отображение кнопки экспорта данных в Excel; <ul style="list-style-type: none">• on - отображение кнопки экспорта данных включено,• off - отображение кнопки экспорта данных выключено.
filterSection	Включает/выключает отображение расширенного фильтра; <ul style="list-style-type: none">• on - отображение секции фильтра включено,• off - отображение секции фильтра выключено.

Параметры элементов управления (часть 2 из 2):

Параметр	Описание
logo	Включает/выключает отображение логотипа; <ul style="list-style-type: none">• on - отображение логотипа включено,• off - отображение логотипа выключено.
presetSection	Включает/выключает отображение секции представлений; <ul style="list-style-type: none">• on - отображение секции представлений включено,• off - отображение секции представлений выключено.
propertyFieldsSection	Включает/выключает отображение секции с выбором полей свойств; <ul style="list-style-type: none">• on - отображение секции с выбором полей свойств включено,• off - отображение секции с выбором полей свойств выключено.
typeSelect	Включает/выключает отображение селектора выбора типа данных - выбор между активными авариями и историей аварий; <ul style="list-style-type: none">• on - отображение селектора включено,• off - отображение селектора выключено.

Параметры фильтра:

Параметр	Описание
filterName	Имя сохранённого фильтра, который сразу будет применён к отображаемым данным.
timeFilter	Включает/выключает отображение дополнительного фильтра по временному диапазону; <ul style="list-style-type: none">• on - временной фильтр включен,• off - временной фильтр выключен. По умолчанию - off - временной фильтр выключен.
type	Выбор типа отображаемых данных – список активных или исторических аварий; <ul style="list-style-type: none">• active - отображать список активных аварий,• history - отображать список исторических аварий. По умолчанию отображается последний выбранный тип.

3.11.2 Страница с графиками

В системе возможно настроить специальную страницу с набором графиков из одного или нескольких объектов (Рис. 3.11.2.1):

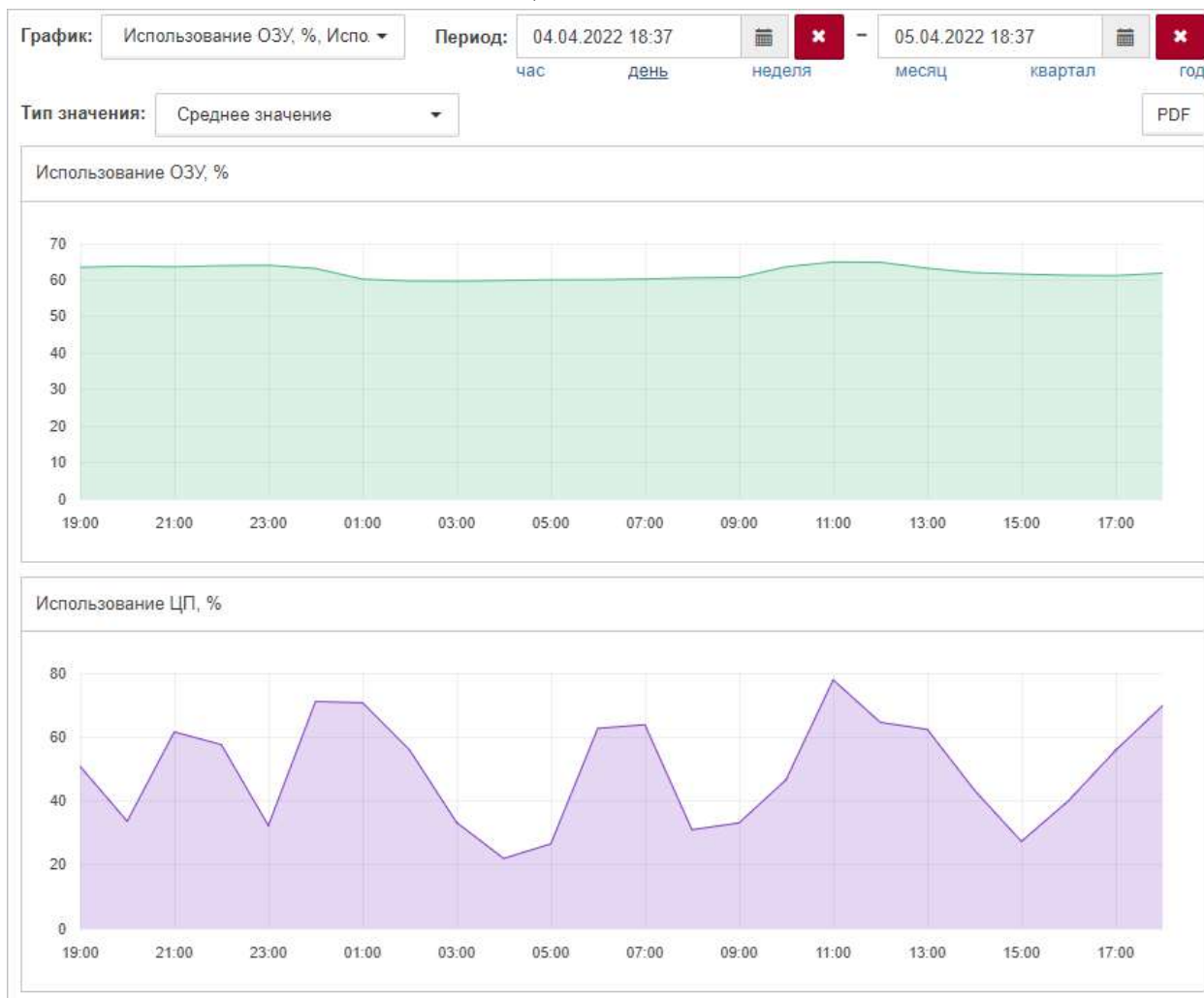


Рис. 3.11.2.1. Пример настроенной страницы графиков

В верхней части страницы представлены элементы управления (Рис. 3.11.2.2):

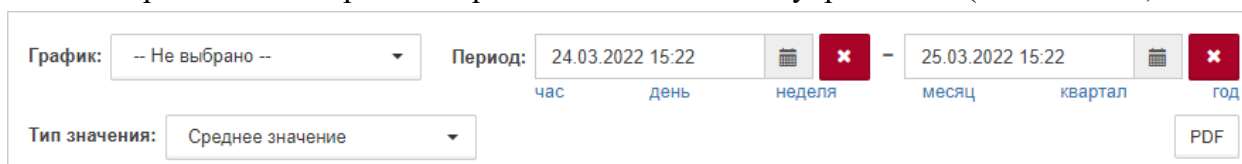


Рис. 3.11.2.2. Элементы управления страницы графиков

Элементы управления страницы графиков:

Параметр	Описание
График	Выпадающий список, где можно отметить отображаемые графики подключенных метрик.
Период	Временной период для отображения графиков. При необходимости можно быстро ввести период за последние <ul style="list-style-type: none">• час,• день,• неделю,• месяц,• квартал,• год, нажав соответствующую кнопку под полями выбора периода.
Тип значения	Способ вычисления значений точек графиков при достаточно коротком периоде обновления данных: <ul style="list-style-type: none">• среднее значение - значения точек графика рассчитываются как среднее арифметическое значений метрики;• минимальное значение - значения точек графиков соответствуют минимальным значениям метрики;• максимальное значение - значения точек графиков соответствуют максимальным значениям метрики.
PDF	Кнопка сохранения страницы в PDF-формате.

Страница с графиками доступна по ссылке вида

<http://<адрес сервера Центрального Пульта>/iframe-widgets.html?#widget/selectable-chart/<ID основного объекта>/<дополнительные параметры>>

где

- **<адрес сервера Центрального Пульта>** - IP-адрес или FQDN инсталляции Центрального Пульта;
- **<ID основного объекта>** - идентификатор объекта, в свойствах которого хранится список метрик и их отображаемые названия;
- **<дополнительные параметры>** - настройки, которые определяют первоначальный вид страницы при её загрузке.

Пример:

`http://127.0.0.1/iframe-widgets.html?#widget/selectable-chart/5fcc9a4de0a5393f45fb99f3/
chart=61a662bdde9e7970b38b340c:percentageUsage.combined&
chart=TOTAL.percentUsed&period=last-24hours`

В данном примере:

- сервер работает на локальной машине и доступен по адресу **127.0.0.1**;
- основным объектом указан объект с идентификатором **5fcc9a4de0a5393f45fb99f3**;
- при загрузке страницы отображаются график метрики **percentageUsage.combined** объекта с идентификатором **61a662bdde9e7970b38b340c** и график метрики **TOTAL.percentUsed** основного объекта за прошедшие сутки.

Возможные метрики для построения графиков необходимо указать в свойствах основного объекта.

В имени свойства указывается имя метрики в формате:

chart:<имя метрики>

При необходимости добавить метрику из другого объекта нужно добавить идентификатор объекта:

chart:<ID внешнего объекта>:<имя метрики>

В значении свойства задаётся отображается имя графика:

<желаемое название отображаемого графика>

Примеры:

Имя свойства: chart:TOTAL.percentUsed

Значение свойства: Использование ОЗУ, %

Описание: График метрики *TOTAL.percentUsed* основного объекта

Имя свойства: chart:61a662bdde9e7970b38b340c:percentageUsage.combined

Значение свойства: Использование ЦП, %

Описание: График метрики *percentageUsage.combined* объекта с ID *61a662bdde9e7970b38b340c*

Дополнительные параметры страницы графиков:

Параметр	Возможные значения	Описание
aggregate	<p>aggregate=avg - выбираются средние значения,</p> <p>aggregate=max - выбираются максимальные значения,</p> <p>aggregate=min - выбираются минимальные значения.</p>	<p>Тип значения, применяемый при загрузке страницы.</p> <p>По умолчанию применяется функция усреднения.</p>
chart	<p>chart:<имя метрики основного объекта> chart:packetsTransmitted</p> <p>chart:<ID нужного объекта>:<имя метрики нужного объекта> chart:61a662bdde9e7970b38b340c:freeMemory</p> <p><i>Используемые в URL метрики должны быть заранее настроены в свойствах основного объекта.</i></p>	<p>Графики, которые будут отображаться при загрузке страницы.</p> <p>Если не указать данный параметр, то по умолчанию откроется страница без графиков.</p>
period	<p>period=last-hour - за последний час,</p> <p>period=last-24hours - за последний день,</p> <p>period=last-7days - за последнюю неделю,</p> <p>period=last-30days - за последний месяц,</p> <p>period=last-90days - за последний квартал,</p> <p>period=last-365days - за последний год.</p>	<p>Период времени для построения графиков, выбираемый при загрузке страницы.</p> <p>По умолчанию отображаются графики за последний час.</p>
widget-instance-id	<p>Значение параметра - имя представления, уникальное в рамках основного объекта. В качестве значения может быть использован любой набор символов.</p> <p>Примеры:</p> <ul style="list-style-type: none"> widget-instance-id=1 - сохранение настроек в представлении с именем 1; widget-instance-id=example - сохранение настроек в представлении с именем example. 	<p>Сохранение настроек страницы в отдельном представлении с уникальным именем.</p> <p>По умолчанию настройки не записываются в представление.</p>

Параметр **widget-instance-id** позволяет сохранять все производимые пользователем настройки в представлении с соответствующим именем.

Имена представлений задаются пользователями произвольно.

✔ *Функционал будет полезен при необходимости одновременного просмотра графиков одних и тех же метрик с различными настройками отображения.*

Если встроить одну и ту же страницу с графиками в несколько IFrame-виджетов, то все изменения, вносимые через элементы управления на одном из виджетов, будут применяться и к остальным. Изменения с настройками отображения страницы можно зафиксировать в отдельном представлении с помощью параметра **widget-instance-id**. Имя представления соответствует значению параметра.

При указании **widget-instance-id** в дополнительных параметрах, изменения, вносимые через другие IFrame-виджеты с той же страницей с графиками, не будут влиять на настройки, сохранённые в представлении.

В настройках IFrame-виджета можно менять значение параметра **widget-instance-id**, чтобы создать еще одно представление или восстановить настройки из ранее сохранённого.

Пример ссылки на страницу с графиками с использованием **widget-instance-id**:

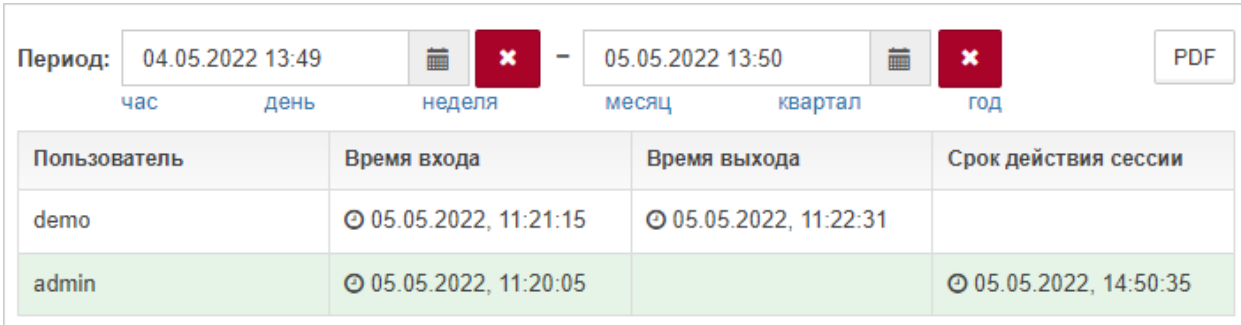
<http://127.0.0.1/iframe-widgets.html?#widget/selectable-chart/5fcc9a4de0a5393f45fb99f3/widget-instance-id=default>

В данном примере:

- сервер работает на локальной машине и доступен по адресу 127.0.0.1;
- основным объектом указан объект с идентификатором **5fcc9a4de0a5393f45fb99f3**;
- настройки отображения страницы сохраняются в представлении с именем **default**.

3.11.3 Страница с журналом сессий

Журнал пользовательских сессий можно открывать по прямой ссылке, которая также может быть использована для встраивания в виджет IFrame:



The screenshot shows a web interface for session logs. At the top, there is a date range filter labeled 'Период:' with two date pickers. The first date is '04.05.2022 13:49' and the second is '05.05.2022 13:50'. Below the dates are labels for time units: 'час', 'день', 'неделя', 'месяц', 'квартал', and 'год'. There are also calendar icons and red 'X' buttons. To the right of the date range is a 'PDF' button. Below the filter is a table with the following data:

Пользователь	Время входа	Время выхода	Срок действия сессии
demo	⌚ 05.05.2022, 11:21:15	⌚ 05.05.2022, 11:22:31	
admin	⌚ 05.05.2022, 11:20:05		⌚ 05.05.2022, 14:50:35

Рис. 3.11.3.1. Пример настроенной страницы с журналом сессий

Ссылка имеет следующую структуру:

<https://<адрес сервера Центрального Пульта>/iframe-widgets.html?#widget/session-log/1/<дополнительные параметры>>

где:

- **<адрес сервера Центрального Пульта>** - IP-адрес или FQDN инсталляции Центрального Пульта;
- **<дополнительные параметры>** - настройки, которые определяют вид страницы.

Пример:

<https://127.0.0.1/iframe-widgets.html?#widget/session-log/1/period=last-30days&limit=10>

В данном примере:

- сервер работает на локальной машине и доступен по адресу 127.0.0.1;
- при загрузке страницы устанавливается временной период за последний месяц;
- выдача ограничена 10 записями.

Дополнительные параметры страницы журнала сессий:

Параметр	Описание
limit	Максимальное количество возвращаемых записей. По умолчанию выдача ограничена 30 записями.
period	Период времени для отображения журнала сессий при загрузке страницы. По умолчанию отображаются сессии за последний час. Параметр может принимать следующие значения: <ul style="list-style-type: none">• period=last-hour - за последний час,• period=last-24hours - за последний день,• period=last-7days - за последнюю неделю,• period=last-30days - за последний месяц,• period=last-90days - за последний квартал,• period=last-365days - за последний год.

3.12 Открытие терминала удалённого доступа

Для объектов класса **Host**, а также для объектов с хотя бы одним из заданных свойств

- **address** (приоритетнее);
- **IP**,

в контекстном меню доступны дополнительные пункты:

- **Открыть SSH терминал**,
- **Открыть telnet терминал**.

Если IP-адрес указан в свойствах объекта, при выборе соответствующего пункта меню происходит подключение к терминалу.

По умолчанию используются следующие порты:

- **22** для SSH;
- **23** для telnet.

При необходимости использовать другой порт номер порта указывается в свойствах объекта для соответствующего протокола:


- **ssh_port**
- **telnet_port**

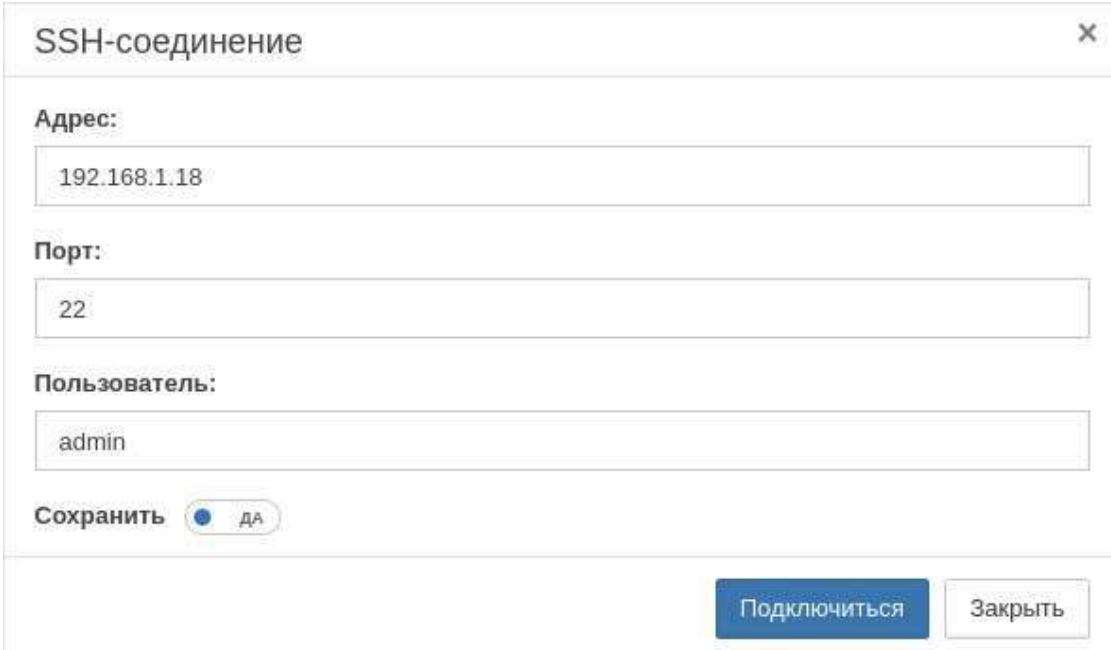
Логин пользователя также можно заранее указать в свойствах для соответствующего протокола:

- **ssh_login**
- **telnet_login**

Для объектов класса **Host**, если в свойствах объекта IP-адрес не задан, при выборе соответствующего пункта меню открывается окно (Рис. 3.12.1), в котором необходимо:

- ввести IP-адрес объекта в поле "Адрес";
- указать номер порта в поле "Порт";
- ввести логин пользователя в поле "Пользователь".

 При установленном слайдере "Сохранить" - "Да" введённые данные сохраняются в свойствах объекта.



SSH-соединение

Адрес:
192.168.1.18

Порт:
22

Пользователь:
admin

Сохранить ДА

Подключиться Заккрыть

Рис. 3.12.1. Пример окна подключения к SSH-терминалу

После ввода данных необходимо нажать кнопку .

3.13 Переход к web-интерфейсу устройства

Для объектов с хотя бы одним из следующих свойств (в порядке уменьшения приоритета)

- web_link,
- address,
- IP,

в контекстном меню доступен пункт "Переход по ссылке". При выборе данного пункта происходит переход по указанному в значении свойства IP-адресу или URL.

3.14 Резервное копирование и восстановление данных

Система предусматривает возможность создания резервных копий, восстановления и переноса основных данных между различными инсталляциями.

Экспорт данных из MongoDB

Для экспорта данных из MongoDB в архив на существующей инсталляции системы необходимо создать и выполнить следующий скрипт:

```
sudo /opt/saymon-scripts/mongodump.sh
```

Пример текста скрипта (необходимо указать HOST, LOGIN, PASS):

```
#!/bin/bash
BACKUP=/backups/mongo/mongodump-$(date +%F-%H-%M).gz
HOST='10.130.0.10'
LOGIN='saymon'
PASS='5tr43ewQ21'

# Outputs a log message, prefixed with current date-time.
log() {
    echo "[`date`] $1"
}

# Create MongoDB backup.
mongodump -h"$HOST" -u"$LOGIN" -p"$PASS" --db saymon --gzip --archive >
"$BACKUP"

log "MongoDB stored to $BACKUP"
```

По умолчанию резервная копия создается в директории `/backups/mongo`.

Для периодического автоматического создания новых и удаления старых резервных копий можно добавить соответствующие команды в crontab, например:

```
sudo crontab -e
0 */2 * * * /opt/saymon-scripts/mongodump.sh
10 */2 * * * ls -tr /backups/mongo | xargs realpath | head -n -6 | xargs rm
```

Импорт данных в MongoDB

Для восстановления или импорта данных в MongoDB на новой инсталляции системы необходимо создать и выполнить следующий скрипт:

```
sudo /opt/saymon-scripts/mongorestore.sh
```

Пример текста скрипта (необходимо указать HOST, LOGIN, PASS):

```
#!/bin/bash
HOST='10.130.0.10'
LOGIN='saymon'
PASS='5tr43ewQ21'

# Outputs a log message, prefixed with current date-time.
log() {
    echo "[`date`] $1"
}

# Directory for MongoDB backups.
DIR=/backups/mongo

# Ask user to specify dump file.
read -p "Please specify backup file, e.g. mongodump-2021-04-15-14-10.gz: "
BACKUP

# Check if BACKUP exists, remove DIR if needed.
if [[ "$BACKUP" = */backups/mongo/* ]]; then
    BACKUP=$(sed 's/\backups\/mongo\/' <<< "$BACKUP")
fi

if [ -f $DIR/$BACKUP ]; then
    log "Backup file $DIR/$BACKUP found!"
else
    log "Backup file $DIR/$BACKUP not found!"
    exit 1
fi

# Create MongoDB backup.
mongorestore -h"$HOST" -u"$LOGIN" -p"$PASS" --db saymon --drop --
noIndexRestore --gzip --archive="$DIR/$BACKUP"
redis-cli -h 10.130.0.10 -a '$6$9UG8HCr0nqj$bVMZfvDKTobl' flushall

log "MongoDB, database saymon, restored from $DIR/$BACKUP"
```

Экспорт данных из OpenTSDB

Для экспорта данных из OpenTSDB в архив на существующей инсталляции системы необходимо создать и выполнить следующий скрипт:

```
sudo /opt/saymon-scripts/hbasedump.sh
```


Пример текста скрипта:

```
#!/bin/bash
BACKUP=/backups/hbase/hbasedump-$(date +%F-%H-%M).tar.gz

# Outputs a log message, prefixed with current date-time.
log() {
    echo "[`date`] $1"
}

# Create HBase backup.
tar zcvf "$BACKUP" /var/lib/hbase

log "HBase stored to $BACKUP"
```

По умолчанию резервная копия создается в директории `/backups/hbase`.

Для периодического автоматического создания новых и удаления старых резервных копий можно добавить соответствующие команды в crontab, например:

```
sudo crontab -e

0 */2 * * * /opt/saymon-scripts/hbasedump.sh
10 */2 * * * ls -tr /backups/hbase | xargs realpath | head -n -6 | xargs rm
```

Импорт данных в OpenTSDB

Для восстановления или импорта данных в OpenTSDB на новой инсталляции системы необходимо создать и выполнить следующий скрипт:

```
sudo /opt/saymon-scripts/hbaserestore.sh
```

Пример текста скрипта:

```
#!/bin/bash
#
# Outputs a log message, prefixed with current date-time.
log() {
    echo "[date` ] $1"
}

# Directory for MongoDB backups.
DIR=/backups/hbase

# Ask user to specify dump file.
read -p "Please specify backup file, e.g. hbasedump-2021-04-15-14-31.tar.gz:"
BACKUP

# Check if BACKUP exists, remove DIR if needed.
if [[ "$BACKUP" = */backups/hbase/* ]]; then
    BACKUP=$(sed 's/\backups\hbase\///' <<< "$BACKUP")
fi

if [ -f $DIR/$BACKUP ]; then
    log "Backup file $DIR/$BACKUP found!"
else
    log "Backup file $DIR/$BACKUP not found!"
    exit 1
fi

# Restore from BACKUP.
docker stop opentsdb
rm -rf /var/lib/hbase
tar xvf $DIR/$BACKUP -C /
docker start opentsdb

log "HBase restored from $DIR/$BACKUP"
```

Экспорт настроек конфигурации

Для экспорта настроек конфигурации необходимо сделать копию директории с конфигурационными файлами `/etc/saymon`.

Импорт настроек конфигурации

Для импорта настроек конфигурации необходимо вставить файлы из ранее сохранённой директории с конфигурационными файлами в директорию `/etc/saymon`.

3.15 Серверные расширения

Центральный Пульт поддерживает установку расширений, дополняющих функционал системы.

Установка расширений

К списку установленных расширений имеют доступ все пользователи через меню текущего пользователя (**Имя пользователя - Расширения**), но доступ к данным ограничен их правами и доступом к объектам.

Для добавления нового расширения необходимо нажать кнопку



или

или перейти на страницу saymon.tech/extensions (Рис. 3.15.1):

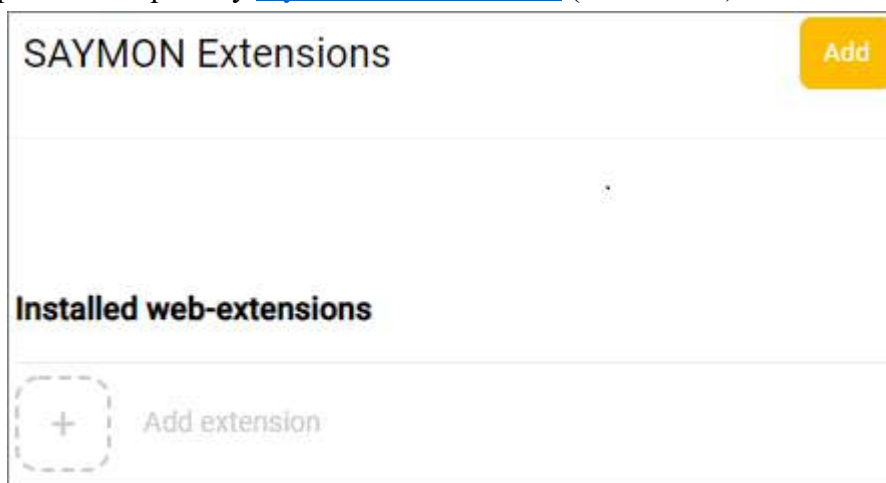


Рис. 3.15.1. Страница расширений Центрального Пульта

В открывшемся каталоге перейти на страницу интересующего расширения и выполнить шаги, описанные в инструкции по установке.

Пользовательские расширения

Пользователи могут писать собственные web-приложения, расширяющие или использующее возможности Центрального Пульта.

Чтобы включить такие приложения в состав сервера Центрального Пульта, необходимо:

1. Добавить секцию **extensions** в конфигурационный файл сервера `/etc/saymon/saymon-server.conf` и в параметре **path** указать путь к папке с расширениями, например, `"/opt/saymon-extensions"`:

```
"extensions": {  
  "path": "/opt/saymon-extensions"  
}
```

📌 Подробную информацию о файле `/etc/saymon/saymon-server.conf` см. в подразделе 3.1.3 "Конфигурация сервера" на стр. 24.

2. Расположить содержимое каждого расширения в отдельной папке внутри корневой. Например, `/opt/saymon-extensions/my-extension`. Эта папка будет точкой входа в клиентскую часть расширения, доступную по URL: `<Адрес_Сервера_Центрального_Пульты>/extensions/my-extension`.
3. В файле `/etc/nginx/sites-enabled/saymon` добавить секцию `location ^~ /extensions` и указать в параметре `alias` папку из параметра `extensions.path`:

```
# SAYMON Extensions folder.  
location ^~ /extensions {  
    alias /opt/saymon-extensions/;  
    try_files $uri $uri$args $uri$args/ @extension;  
    autoindex on;  
}
```

Чтобы расширение было доступно в общем списке расширений, отображаемых в web-интерфейсе Центрального Пульта, оно должно содержать файл `package.json` или `meta.json` (данные `meta.json` приоритетнее).

Формат и поля файла `meta.json`:

Параметр	Описание
author	Автор расширения.
date	Дата выхода установленного расширения.
description	Краткое описание расширения.
homepage	Ссылка на домашнюю страницу расширения.
icon	Прямая ссылка на иконку расширения. По умолчанию используется файл <code>icon.png</code> из директории расширения.
name	Название расширения. <i>Расширения сторонних разработчиков не могут начинаться со слова SAYMON.</i>
nameInUrl	Часть ссылки для перехода на страницу с расширением. Совпадает с названием папки, в которой лежит файл <code>index.html</code> расширения. <code><Адрес_Сервера_Центрального_Пульты>/extensions/<nameInUrl></code>
urlToMeta	Прямая ссылка на файл <code>meta.json</code> последней актуальной версии для проверки обновлений.
version	Версия установленного расширения.

Пример файла `meta.json`:

```
{
  "author": "SAYMON User",
  "date": "2020/12/31",
  "description": "Very useful custom extension",
  "homepage": "https://saymon.tech/extensions/my-extension/",
  "icon": "https://saas.saymon.info/extensions/my-extension/favicon.ico",
  "name": "My Extension",
  "nameInUrl": "my-extension",
  "urlToMeta": "https://saymon.tech/extensions_meta/my-extension/meta.json",
  "version": "1.0.1"
}
```

4 Проблемы в работе системы и способы их решения

Раздел содержит информацию об известных проблемах, которые могут возникать при работе с платформой, и способы их решения.

4.1 Недостаточно места на виртуальной машине с сервером

Условия проблемы:

- есть виртуальная машина с сервером Центрального Пульта;
- нет места на виртуальной машине с сервером Центрального Пульта.

Решение проблемы:

1. Понять содержимое и объём занимаемого места:

```
sudo du -h / | sort -h
```

2. Просмотреть список папок в *stdout*:

- если много места занимает папка `/var/log/saymon`, то можно уменьшить количество хранимых лог-файлов правкой `/etc/logrotate.d/saymon` для `saymon-server.log`: `rotate X` и `/opt/saymon-agent/conf/logback-upstart.xml` для `saymon-agent.*.log`: `<maxHistory>10</maxHistory>`;
- если много места занимают данные из MongoDB, то зайти в базу данных и оценить размеры коллекций:

```
mongo saymon
function getReadableFileSizeString(fileSizeInBytes) {
  var i = -1;
  var byteUnits = [' kB', ' MB', ' GB', ' TB', 'PB', 'EB', 'ZB', 'YB'];
  do {
    fileSizeInBytes = fileSizeInBytes / 1024;
    i++;
  } while (fileSizeInBytes > 1024);
  return Math.max(fileSizeInBytes, 0.1).toFixed(1) + byteUnits[i];
};
var collectionNames = db.getCollectionNames(), stats = [];
collectionNames.forEach(function (n) { stats.push(db.getCollection(n).stats()); });
stats = stats.sort(function(a, b) { return b['size'] - a['size']; });
for (var c in stats) { print(stats[c]['ns'] + ": " + getReadableFileSizeString(stats[c]
['size']) + " (" + getReadableFileSizeString(stats[c]['storageSize']) + ")"); }
```

В наиболее объёмных коллекциях используется `timestamp`, следующей командой можно удалить из коллекции `stateHistory` массив данных за рамками глубины хранения:

```
db.stateHistory.remove({'timestamp':{'$gt':1477994233000}})
```

После описанных выше действий место в системе не освободится, так как MongoDB аллоцирует дисковое пространство. Требуется сделать бэкап и восстановить базу:

```
mongodump
sudo rm -rf /var/lib/mongoddb/*
sudo mongorestore dump/ --dbpath /var/lib/mongoddb/
sudo chown -R mongoddb:mongoddb /var/lib/mongoddb
sudo service mongod restart
```

- если много места занимают данные Open TSDB, не вынесенные из Docker-контейнера, их можно вынести:

```
sudo docker exec -it opentsdb bash
cd /data/hbase/hbase-root
tar zcvf hbase-root.tar.gz hbase-root
scp hbase-root.tar.gz saymon@*host_ip*/opt/
exit
cd /opt/ && tar xvf hbase-root.tar.gz
sudo docker stop opentsdb
sudo docker rm opentsdb
sudo docker run -d -p 127.0.0.1:4242:4242 --restart=always --
volume /opt/hbase-root:/data/hbase/hbase-root/ --name=opentsdb
rossinno/opentsdb
```


4.2 Отсутствие подключения агента к серверу

Условия проблемы:

- агент не подключается к серверу;
- запись в логе:
12.10.2016 07:45:59.431 [pool-1-thread-1] WARN n.r.s.agent.connection.RedisBackend - Redis connection failed (will retry in 5 seconds): JedisDataException: ERR max number of clients reached

Решение проблемы:

1. Проверить на сервере проблему локально:

```
# redis-cli -a 'пароль_от_redis_в_кавычках' info clients | grep  
connected_clients | sed -e 's/connected_clients://g'  
Error: Connection reset by peer
```

2. Проверить проблему локально через redis-cli:

```
# redis-cli  
127.0.0.1:6379> auth пароль_от_redis  
(error) ERR max number of clients reached  
127.0.0.1:6379> q
```

3. Рестарт Redis-сервера:

```
# service redis-server restart  
Stopping redis-server: redis-server  
Starting redis-server: redis-server
```

4.3 Проверка работы MongoDB

Проверка наличия процесса в памяти:

```
ps -ef | grep mongod  
mongod 1147 1 0 Nov02 ? 04:23:16 /usr/bin/mongod -  
config /etc/mongod.conf
```

Остановка, запуск и рестарт процесса:

```
sudo service mongod stop  
sudo service mongod start  
sudo service mongod restart
```

4.4 Проверка работы Redis

Проверка наличия процесса в памяти:

```
ps -ef | grep redis
redis 1763 1 0 Aug10 ? 00:37:11 /usr/bin/redis-server 0.0.0.0:6379
root 1786 1 0 Aug10 ? 00:00:00 /usr/bin/stunnel4 /etc/stunnel/redis-client.conf
root 1787 1 0 Aug10 ? 00:00:00 /usr/bin/stunnel4 /etc/stunnel/redis-client.conf
...
```

Остановка, запуск и рестарт процесса:

```
sudo service redis-server stop
sudo service redis-server start
sudo service redis-server restart
```

Номер порта, на котором осуществляется процесс:

```
sudo netstat -lnp | grep redis
tcp 0 0 0.0.0.0:6379 0.0.0.0:* LISTEN 1763/redis-server 0
```

или в конфигурационном файле:

```
cat /etc/saymon/saymon-server.conf | grep cache -A 4
"cache": {
  "auth_pass": "12!@easy",
  "host": "127.0.0.1",
  "port": 6379
},
...
```

Проверка доступности (открытости) порта:

```
sudo iptables -L INPUT -n -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num pkts bytes target prot opt in out source destination
1 15M 3082M ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:6379
```

Добавление порта в список открытых и запись нового правила:

```
sudo iptables -I INPUT 1 -m state --state NEW -p tcp --dport 6379 -j ACCEPT
sudo bash -c "/sbin/iptables-save > /etc/iptables.rules"
```

4.5 500 Internal Server Error и отсутствие графиков

Условия проблемы:

- вместо графиков возникает ошибка 500.

Решение проблемы:

Необходимо перезапустить OpenTSDB:

```
less /var/log/opentsdb/opentsdb.log - (здесь можно увидеть какие-то ошибки)
sudo service opentsdb stop
sudo service hbase restart
sudo service opentsdb start
```

4.6 Ошибка работы НТТР-проверки

Условия проблемы:

- НТТР-проверка адреса `https://xxx.xxx` не работает и возникает ошибка.

Решение проблемы:

Данная проблема возникает при использовании агента в связке с Java 1.6.

Есть два варианта решения:

1. Обновить Java, установленную в операционной системе, до версии 1.7 или 1.8.
2. Скачать и установить последнюю версию агента со встроенной Java.

Приложение А (обязательное)

Права на операции

Основные права (часть 1 из 4):

Название	Описание	Запись в конфигурационном файле сервера	
Выполнение операций	Включает секцию Операции и возможность их запуска.	"execute-operations"	
Поиск и групповые операции	Включает возможность выполнения поиска и групповых операций. <i>Необходимы права на "Управление объектами, свойствами и документами"</i>	"run-bulks"	
Управление объектами, свойствами и документами	Включает <ul style="list-style-type: none"> • создание, • клонирование, • переименование, • изменение размеров, • перемещение, • удаление • объектов, • виджетов объектов, • ссылок, • подложек. Включает просмотр и редактирование всех секций объектов, кроме секции Мониторинг .	"manage-objects"	
	Создание объектов	Включает <ul style="list-style-type: none"> • создание, • клонирование объектов.	"create-objects"
	Модификация объектов	Включает <ul style="list-style-type: none"> • переименование, • изменение размеров, • перемещение • объектов, • виджетов объектов, • ссылок, • подложек. 	"modify-objects"
	Удаление объектов	Включает удаление объектов.	"delete-objects"

Основные права (часть 2 из 4):

Название	Описание	Запись в конфигурационном файле сервера
Управление связями, свойствами и документами	<p>Включает</p> <ul style="list-style-type: none"> • создание, • изменение, • удаление • связей, • виджетов связей. <p>Включает просмотр и редактирование всех секций связей, кроме секции Мониторинг.</p>	"manage-links"
Создание связей	Включает создание связей.	"create-links"
	<p>Включает</p> <ul style="list-style-type: none"> • изменение связей, • создание, изменение и удаление виджетов связей. 	"modify-links"
	Включает удаление связей.	"delete-links"
Управление потоками	<p>Включает создание, изменение и удаление потоков.</p> <p><i>Для изменения потоков требуются права на просмотр секции "Параметры".</i></p>	"manage-flows"
Создание потоков	Включает создание потоков.	"create-flows"
	<p>Включает изменение потоков.</p> <p><i>Требуются права на просмотр секции "Параметры".</i></p>	"modify-flows"
	Включает удаление потоков.	"delete-flows"

Основные права (часть 3 из 4):

Название	Описание	Запись в конфигурационном файле сервера	
Управление документами объектов и связей	Включает редактирование секции "Документы". <i>Требуются права на просмотр секции "Документы".</i>	"manage-documents"	
Создание документов	Включает прикрепление ссылок на web-страницы.	"create-documents"	
	Модификация документов	Включает редактирование документов.	"modify-documents"
	Удаление документов	Включает удаление документов.	"delete-documents"
	Загрузка документов	Включает прикрепление PDF-файлов.	"upload-documents"
Управление свойствами объектов и связей	Включает редактирование секции Свойства . <i>Требуются права на просмотр секции "Свойства".</i>	"manage-properties"	
Создание свойств	Включает создание свойств.	"create-properties"	
	Модификация свойств	Включает модификацию свойств.	"modify-properties"
	Удаление свойств	Включает удаление свойств.	"delete-properties"
Управление классами	Включает кнопку  Применить к классу в секциях <ul style="list-style-type: none"> Условия перехода состояний, Условия генерации аварий. Включает в окне конфигурации системы вкладку Управление классами .	"manage-classes"	
Управление операциями	Включает редактирование секции Операции .	"manage-operations"	
Управление настройками мониторинга	Включает просмотр и редактирование секции Мониторинг .	"manage-service-properties"	


Основные права (часть 4 из 4):

Название	Описание	Запись в конфигурационном файле сервера
Управление скриптами	Включает возможность использовать скрипт с указанным текстом при проверке Выполнение программы / скрипта . Включает в окне конфигурации системы вкладку Скрипты .	"manage-scripts"

Просмотр секций:

Секция	Запись в конфигурационном файле сервера
Данные	"view-section-stat"
Свойства	"view-section-properties"
Документы	"view-section-documents"
История состояний	"view-section-state-history"
Графики	"view-section-history-graph"
Мониторинг	"view-section-monitoring"
Параметры	"view-section-entity-settings"
Условия перехода состояний	"view-section-state-conditions"
Действия при смене состояний	"view-section-state-triggers"
Виджеты	"view-section-widgets"
История изменений	"view-section-audit-log"
Изменения конфигурации	"view-section-config-log"
Операции	"view-section-operations"
История операций	"view-section-operations-history"
Условия генерации аварий	"view-section-incident-conditions"
Правила формирования данных	"view-section-stat-rules"


Права на администрирование системы:

Название	Описание	Запись в конфигурационном файле сервера
Управление конфигурацией системы	Включает в окне конфигурации системы вкладки: <ul style="list-style-type: none"> • Журнал событий, • Шаблоны уведомлений, • Аварии, • Состояния, • Парольные политики. 	"manage-configuration"
Обновление агентов	Позволяет пользователю обновлять отдельных агентов кнопкой  и всех агентов на вкладке Агенты в окне конфигурации системы.	"upload-agent-updates"
Управление пользователями	Позволяет управлять всеми пользователями системы.	"manage-users"
Управление журналом событий	Позволяет <ul style="list-style-type: none"> • назначать ответственного, • изменять текст событий, • удалять события в журнале событий SNMP.	"manage-event-log"
Управление историческими данными	Позволяет <ul style="list-style-type: none"> • добавлять, • редактировать, • удалять комментарии на графиках.	"manage-history"
Запуск автоопределения объектов	Позволяет использовать сервисный REST-метод node/api/discovery .	"run-discovery"
Чтение журнала сессий	Включает в окне конфигурации системы вкладку Журнал сессий .	"read-session-log"

Приложение Б (обязательное)

Параметры исполняемых файлов пользовательских сенсоров и скриптов, выполняемых при создании/удалении объектов

Возможные поля файла настроек параметров (часть 1 из 3):

Поле	Описание
title	<p>Отображаемое в web-интерфейсе имя исполняемого файла.</p> <p>Опциональное поле.</p> <p>По умолчанию - идентификатор сенсора или скрипта.</p> <p><i>Если идентификатор содержит путь (исполняемый файл вложен в подпапки), имя будет отображаться с путём.</i></p> <p>Пример: <i>путь к файлу: (путь до папки с исполняемыми файлами)/cisco/task_1.sh</i> <i>отображаемое имя скрипта: cisco - task_1</i></p>
excludeForClasses	<p>Список ID классов объектов, к которым неприменим данный сенсор.</p> <p>Опциональное поле.</p> <p>По умолчанию сенсор доступен для всех классов объектов.</p> <p><i>Поле применяется только для пользовательских мониторинговых сенсоров.</i></p>
icon	<p>Иконка из набора Font Awesome, отображаемая рядом с именем проверки.</p> <p>Опциональное поле.</p> <p>По умолчанию -  - 'fa fa-cubes fa-fw'</p> <p><i>Поле применяется только для пользовательских мониторинговых сенсоров.</i></p>
args	<p>Настройки аргументов, которые задаются пользователем через web-интерфейс и передаются исполняемому файлу.</p>
args.id	<p>Имя аргумента, передаваемое исполняемому файлу.</p> <p>Опциональное поле.</p>
args.default	<p>Значение аргумента по умолчанию, подставляемое в соответствующее поле.</p> <p>Опциональное поле.</p>
args.description	<p>Описание аргумента, отображаемое в web-интерфейсе.</p> <p>Опциональное поле.</p>
args.name	<p>Название аргумента, отображаемое в web-интерфейсе.</p>

Возможные поля файла настроек параметров (часть 2 из 3):

Поле	Описание
args.required	<p>Признак обязательности заполнения значения аргумента.</p> <ul style="list-style-type: none"> • false - значение опционально, • true - значение обязательно. <p>Опциональное поле.</p> <p>По умолчанию - false.</p>
args.options	<p>Применимо только для типа select (<i>args.type.select</i>).</p> <p>Определяет набор значений, отображаемых в выпадающем списке.</p> <p>По умолчанию при создании проверки выбирается первая опция.</p> <p>Чтобы установить иную опцию значением по умолчанию, необходимо указать значение поля <i>args.options.value</i> в поле <i>args.default</i>.</p> <p>Исполняемому файлу передаются:</p> <ul style="list-style-type: none"> • имя аргумента (<i>args.id</i>); • значение аргумента (<i>args.options.value</i>). <p>Если <i>args.id</i> не задано, то исполняемому файлу передаётся только значение выбранного аргумента (<i>args.options.value</i>).</p> <p>Если значение аргумента не задано (<i>args.options.value</i>), то исполняемому файлу также не передаётся имя аргумента (<i>args.id</i>).</p> <p><i>Данную логику можно использовать для реализации пункта "Не выбрано" и разделителей в выпадающем списке.</i></p>
args.options.description	<p>Описание значения аргумента, отображаемое в выпадающем списке.</p> <p>Опциональное поле.</p> <p>По умолчанию отображается значение аргумента (<i>args.options.value</i>).</p>
args.options.value	<p>Значение аргумента.</p> <p>Опциональное поле.</p> <p>При отсутствии значения исполняемому файлу также не передаётся имя аргумента.</p> <p><i>Такие опции можно использовать для реализации пункта "Не выбрано" и разделителей в выпадающем списке.</i></p>
args.type	<p>Тип значения аргумента.</p> <p>Опциональное поле.</p> <p>По умолчанию - text.</p>

Возможные поля файла настроек параметров (часть 3 из 3):

Поле	Описание
<code>args.type.checkbox</code>	Переключатель. По умолчанию выключен. При включении исполняемому файлу передаётся значение, указанное в поле <code>args.id</code> (имя аргумента). Если это поле отсутствует, то исполняемому файлу передаётся порядковый номер аргумента (отсчёт начинается с 0).
<code>args.type.password</code>	Отображает текстовое поле для ввода значения аргумента с маскировкой введённых символов.
<code>args.type.select</code>	Отображает выпадающий список с предопределёнными значениями аргумента. Список значений задается в поле <code>args.options</code> . Для данного типа не отображается описание аргумента (поле <code>args.description</code>). Вместо этого необходимо использовать соответствующее поле для каждого значения аргумента (<code>args.options.description</code>).
<code>args.type.text</code>	Отображает текстовое поле для ввода значения аргумента.
<code>args.type.textarea</code>	Отображает текстовое поле для ввода значения аргумента. Позволяет вводить многострочный текст.

Пример содержимого файла настроек со всеми типами аргументов (часть 1 из 2):

```
{
  "title": "Example",
  "icon": "fa fa-folder fa-fw",
  "excludeForClasses": [1,2],
  "args": [
    {
      "name": "Unnamed (positional) arg"
    },
    {
      "name": "Named arg",
      "id": "--name"
    },
    {
      "name": "Behold the description on the right",
      "description": "Here I am!",
      "id": "--description"
    },
    {
      "name": "Arg with default value",
      "description": "and description",
      "id": "--defval",
      "default": "default_value"
    }
  ]
}
```

Пример содержимого файла настроек со всеми типами аргументов (часть 2 из 2):

```
"name": "Required arg",
"description": "This field is required to fill in",
"id": "--required",
"required": true
},
{
  "name": "Type - Text",
  "description": "This and all above fields have got text type",
  "id": "--text",
  "type": "text"
},
{
  "name": "Type - Text Area",
  "description": "This field is text area. \nIt is resizable in most browsers. \nAnd allows to enter
multiline texts.",
  "id": "--textarea",
  "type": "textarea"
},
{
  "name": "Type - Checkbox",
  "description": "This is the checkbox type",
  "id": "--checkbox",
  "type": "checkbox"
},
{
  "name": "Type - Password",
  "description": "This is the password field",
  "id": "--pass",
  "default": "qwerty",
  "type": "password"
},
{
  "name": "Type - Select",
  "description": "This is the select type. This description is not displayed in the web interface. Use
description for each option instead.",
  "id": "--select",
  "default": "option2",
  "type": "select",
  "options": [
    {
      "description": "== Not selected =="
    },
    {
      "value": "option1", "description": "OK"
    },
    {
      "description": "== Divider =="
    },
    {
      "value": "option2", "description": "Warning"
    },
    {
      "value": "option3", "description": "Error"
    }
  ]
}
]
```

www.cpult.ru

2023

РОССИНО