Руководство по системному администрированию компонента Indicator (Код компонента: INDA) продукта Platform V Monitor (Код продукта: OPM)

ОГЛАВЛЕНИЕ

Руководство по системному администрированию

Термины и определения

Термин/определение	Определение
АС	Автоматизированная система
БД	База данных
Авторизация/Сервис авторизации	Модуль авторизации компонента Abyss (LGDB) продукта Platform V Monitor (OPM)
Тенант (tenant)	Логическая сущность мультитенантности, имеющая возможность безопасно использовать ресурсы и сервисы внутри продукта
CPU	Central Processing Unit, центральный процессор
Druid	Часть компоненты Abyss. Колоночная база данных с открытым исходным кодом под лицензией Apache 2. 0
Abyss	Компонент Abyss (LGDB) входящий в состав продукта Platform V Monitor (OPM), предназначен для приема, пред обработки, хранения и получения загруженных данных
Indicator	Компонент Indicator (INDA) входящий в состав продукта Platform V Monitor (OPM). Обеспечивающий визуализацию в продукте Platform V Monitor (OPM).
Алерт	Программируемое оповещение о каком-либо событии.
Dashboards (Дашборд)	Набор из одной или нескольких интерактивных панелей, для визуализации значений метрик в Indicator
Панель / Panel	Представляет из себя одну визуализацию (например, в виде графика). Панель является основным строительным блоком визуализации. Каждая панель имеет редактор запросов, специфичный для источника данных, выбранного на панели.
Datasources	Настраиваемый источник данных в Indicator
Pod / Под	Экземпляр, модуль в платформе приложений-контейнеров
JOB	Джоба Jenkins
Notification channels	Канал уведомлений для отправки алерта
~~Pipeline CD~~	

Сценарии администрирования

Управление ключами и сертификатами выполняется администратором. Настройки, связанные с управлением ключами и сертификатами, осуществляются с помощью средств DevOps Pipeline CD в соответствии с Руководством по безопасности. В самом UI требуются провести дополнительные настройки Datasource см. пункт Добавление источника данных (Data Sources). Установка Indicator, входящего в состав программного продукта Platform V Monitor (OPM) осуществляется в соответствии с Руководством по установке. Откат к предыдущей версии представляет собой установку последней стабильной версии.

Проверка работоспособности

Администратору рекомендуется регулярно выполнять:

- контроль состояния работы системы Indicator;
- мониторинг производительности системы Indicator;
- контроль свободного места на жестких дисках всех серверов системы Indicator, а также в файловой системе;
- администрирование пользователей;
- администрирование источников данных;
- администрирование дашбордов.

Сделать это можно с помощью системных метрик (описаны ниже) и метрики доступности. Также контролировать работу сервиса и проверять сервис на наличие ошибок можно с помощью дашборда самомониторинга **Indicator metrics**.

Действия при возникновении нештатной ситуации

При выявлении нештатных ситуаций необходимо:

- Зайти в консоль платформы приложений-контейнеров, убедиться, что приложение INDICATOR доступно;
- Зайти в дашборда **Indicator metrics** проверить наличие ошибок на panel "Количество ошибок" или аномальных скачков по графикам.

Обязанности администратора

В рамках выполнения требований безопасной работы в Indicator, Администратор выполняет следующие функции:

- осуществляет контроль использования средств защиты информации;
- осуществляет контроль доступа к обрабатываемым данным пользователями, согласно предоставленным ему правам доступа к АС;
- несет ответственность за качество проводимых им работ.

Доступ к АС должны иметь только те сотрудники, которым он необходим в соответствии с их должностными обязанностями. Доступ должен ограничиваться минимально необходимым объемом данных. Должны разделяться среды разработки, тестирования и эксплуатации.

При этом производится разделение обязанностей между разработчиками АС, тестирующим персоналом и сотрудниками, непосредственно эксплуатирующими уже введенные в промышленную эксплуатацию системы Indicator.

Администратору доступны все функции, указанные в Руководстве для оператора. Дополнительно, Администратор может управлять источниками данных.

Для управления источниками данных:

1. Переместите курсор на шестеренку в боковом меню, которое покажет вам меню конфигурации;
2. Если боковое меню не отображается, нажмите на значок шестеренки в левом верхнем углу;
3. Нажмите кнопку **Configuration>>Data Sources** в боковом меню, и вы перейдете на страницу источники данных где вы можете добавлять и редактировать источники данных.

Как источник данных по умолчанию используется плагин **SberTech Abyss**.

Для Business activity monitoring используется плагин **SberTech Abyss** .

Для добавления источника данных (Datasources) переместите курсор на шестеренку в боковом меню, которое покажет вам меню конфигурации:

1. Нажмите на кнопку **Configuration >> Data Sources** и нажимаем **“Add data source”**;
2. Выбираем плагин SberTech Abyss SQL:
   - Включить **Exec On Front** для работы Data Sources в через frontend;
   - В типе **Work Mode** указываем *Bam Selector*;
   - Указываем endpoint подключения к Bam Selector, "Заполните поля" **AuthToken**, **HeaderNamesList**;
   - Важно! В поле name вводим название **«SberTech BAM SQL»**, именно так как называется data source в дашбордах, поэтому названия должны совпадать;
   - Для работы adhoc фильтра необходимо добавить переменную projectName, которая будет содержать в себе список проектов/подключений.
   - Нажимаем Save & Test.

Если все параметры введены корректно, то будет выведено оповещение Datasource is working.

Список функций и ограничений для Администратора:

- Может добавлять, редактировать и удалять источники данных;
- Может добавлять и редактировать пользователей и команды в своей организации;
- Может добавлять, редактировать и удалять папки, содержащие информационные панели для источников данных, связанных с их организацией;
- Можно настроить Плагины приложений и параметры организации;
- Может делать все, что разрешено ролью редактора.

Рекомендации по заданию стойких паролей

См. подробнее раздел **Рекомендации по заданию стойких паролей** в Руководстве по безопасности.

Настройка конфигурационного файл indicator.conf

Конфигурирование производиться до выполнения JOB **Pipeline_deploy** в файле **indicator.conf** расположенном **/conf/config/parameters/**. см раздел Пример файла конфигурации indicator.conf.

Здесь и далее поддерживаемой системой приложений-контейнеров является Kubernetes (использование OSE – опционально), в именах и параметрах системы могут встречаться названия систем контейнеризации.

Перед настройкой необходимо подготовить pipeline для установки.

Настройка БД

Для БД Postgresql

Внести изменения в файл **indicator.conf** в раздел #Параметры для подключения к БД.

Имя параметра	Примеры значений	Описание
#Параметры для подключения к БД (Grafana)		
GRAFANA_DB_TYPE	postgres	Тип базы данных
GRAFANA_DB_HOST	${EFS_PSTGR_DB_HOST}:${EFS_PSTGR_DB_PORT}	Глобальная переменная. IP и port подключения к БД. Если sqlite3, то например 127.0.0.1:3306
GRAFANA_DB_NAME	${EFS_PSTGR_DB_NAME}	Глобальная переменная. Имя БД
GRAFANA_DB_SSL_MODE	verify-full	Для Postgres, использовать или disable, или require ,или verify-full. При GRAFANA_DB_SSL_MODE=disable параметры: ?prepareThreshold=0&binary_parameters=yes, при GRAFANA_DB_SSL_MODE=verify-full параметр: ?binary_parameters=yes GRAFANA_DB_PARAMETERS=?binary_parameters=yes. При GRAFANA_DB_SSL_MODE=verify-full не забываем перевести параметр в true (indicator.ose.deployment.spec.template.spec.containers.indicator.change.permission.for.key=true см.внизу файла)

GRAFANA_DB_PARAMETERS	?binary_parameters=yes	Параметр используется при установленном значении GRAFANA_DB_SSL_MODE=verify-full
GRAFANA_DB_CA_CERT_PATH	${indicator.ose.deployment.spec.template.spec.containers.indicator.volumeMounts.mountPath.sslcerts}/cacert.pem	Глобальная переменная.Путь к используемому сертификату
GRAFANA_DB_CLIENT_KEY_PATH	${indicator.ose.deployment.spec.template.spec.containers.indicator.volumeMounts.mountPath.sslcerts}/cert-key.pem	Глобальная переменная.Путь к ключу клиента
GRAFANA_DB_CLIENT_CERT_PATH	${indicator.ose.deployment.spec.template.spec.containers.indicator.volumeMounts.mountPath.sslcerts}/cert.pem	Глобальная переменная. Путь к сертификату клиента
GRAFANA_DB_SERVER_CERT_NAME		Имя используемого сертификата

Здесь и далее поддерживаемой системой приложений-контейнеров является Kubernetes (использование OSE – опционально), в именах и параметрах системы могут встречаться названия систем контейнеризации.

Также необходимо выполнить настройки egress в файл indicator.istio.all.conf. в пунктах:

```
# Внешний порт на котором работает БД
indicator.ose.istio.egress.db.port=PORT1,PORT2
indicator.ose.istio.egress.db.resolution=DNS
indicator.ose.istio.egress.db.create.addresses=false
# Внутренний порт для Gateway для перемешивания
трафика (всегда должен быть уникальным)
indicator.ose.istio.egress.db.gateway.port=PORT1,PORT
2 # Внутренний порт для перемешивания трафика на
Egress, этот порт и нужно указывать для подключения к
БД (всегда должен быть уникальным)
indicator.ose.istio.egress.db.internal.port=PORT1,~~.ma~~
~~x_replicas=1~~
```

Настройка аутентификации

Для включения аутентификации необходимо внести изменения в файл **indicator.conf** в зависимости от выбранной модели аутентификации

См. подробнее раздел **Настройки аутентификации** в Руководстве по безопасности

Настройка Platform V Monitor Журналирование (LOGA)

Для каждого контейнера приложения, устанавливающегося в платформе приложений-контейнеров, ставится Sidecar-контейнер FluentBit, для сборки, обработки и транспорта логов.

Каталог с файлами логов находится на общем ресурсе модуля контейнеризация, доступ к которому имеет как контейнер приложения, так и Sidecar-контейнер FluentBit. FluentBit читает эти файлы, и отправляет логи в Kafka.

Для настройки интеграции с Logger необходимо внести изменения в файл **indicator-logger.conf**

Имя параметра	Примеры значений	Описание
#Параметры брокеров и топика куда отбрасывается лог		
fluent-bit.ose.configmaps.fluent-bit.data.brokers	host	Узлы брокеров kafka
fluent-bit.ose.configmaps.fluent-bit.data.topics	IDR.Indicator	Имя топика Kafka
fluent-bit.ose.configmaps.fluent-bit.data.security.protocol=	SSL	Тип протокола

> Здесь и далее поддерживаемой системой приложений-контейнеров является Kubernetes (использование OSE – опционально), в именах и параметрах системы могут встречаться названия систем контейнеризации.

Настройка георезервирования

Для использования георезервирования необходимо заполнить параметр БД в файле **indicator.conf**.

GRAFANA_DB_HOST=IP_БД1,IP_БД1:5001, этот параметр заполняется именно так.

Что-бы настроить выходы egress для базы данных в режиме использования георезервирования необходимо заполнить параметры:

Имя параметра	Примеры значений	Описание
## Пошаговая настройка в самом интерфейсе UI# egress-se-tcp-db		
indicator.ose.istio.egress.db.enabled	true или false	Включение настройки
indicator.ose.istio.egress.db.hosts	Имя Host,через запятую	Имя узла
indicator.ose.istio.egress.db.port	Значение порта ,через запятую	Значение порта для DB
indicator.ose.istio.egress.db.resolution	DNS	Тип resolution
# Если indicator.ose.istio.egress.db.create.addresses=true то параметр должен быть indicator.ose.istio.egress.db.resolution=DNS		

# IP адреса возьмутся из переменной GRAFANA_DB_HOST (без порта)		
indicator.ose.istio.egress.db.create.addresses	true или false	Включение настройки подстановки IP адреса из переменной

Здесь и далее поддерживаемой системой приложений-контейнеров является Kubernetes (использование OSE – опционально), в именах и параметрах системы могут встречаться названия систем контейнеризации.

Из-за внутренней логики работы Istio может возникнуть проблема использования одного порта на разные хосты в ServiceEntry

Есть два варианта решения данной проблемы: 1-й вариант заполняем параметры согласно примеру приведенному в файле 1v.txt 2-й вариант заполняем параметры согласно примеру приведенному в файле 2v.txt

Конфигурация для георезервированной схемы подключения

Если необходимо развернуть дистрибутив на разных кластерах контейнеризированого средства оркестрации, тогда для настройки необходимо заполнить параметр в файле indicator.istio.all.conf:

```
indicator.ose.istio.ingress.route.spec.host.https.appFQDN=${distrib.release.version}-indicator.${projectName}.${appsDomain}
```

Роут всех сервисов в каждом из кластеров должен указывать на один и тот же хост, по умолчанию настроенного на глобальную переменную.

Для георезервированного балансера необходимо указать URL для выполнения запросов healthcheck используемого компонента: https://host/healthz где, host - хост указанный в первом пункте.

Настройка secrets и подготовка сертификатов

Для этого необходимо создать JKS файл indicator.jks (должен содержать корневой сертификат, сертификат-сервер, ключ), затем разместить его в папку ** ansible/files/ssl ** в common репозитории.

Для правильной настройки нужно сразу проставить сертификатам признаки root, cert, key. см репозиторий ci00380023_efs_unimon_common_dev_ind/browse/ansible/files/ssl

Файл необходим для защищенного взаимодействия (SSL) со смежными компонентами или продуктами. При использовании SSL-подключения к базе данных, на сервере БД должен использоваться Сертификат с SAN (Subject Alternate Name).

Также в common репозитории добавить параметры в файл ssl.conf имя файла пароль(ссылается на параметр из passwords.conf) Произвести настройку секретов в файле _passwords.conf

См. подробнее в Руководстве по установке.

После выполнения установки JOB Pipeline_deploy, необходимо выполнить настройки в самом интерфейсе UI.

Создание организации и пользователей (через Сервис авторизации)

Добавление организации

Для создания организации в приложении Abyss необходимо выполнить следующие действия: перейти на Вкладку "Настройки" > "Организации" > "+" > Окно "Создать Организацию" > Ввести "Название Организации" и "ProjectID" > Кнопка "Сохранить" > Окно просмотра Списка организаций.

Добавление пользователя организации

Для добавления пользователя организации в приложении Abyss UI необходимо выполнить следующие действия: перейти на Вкладку "Настройки" > "Организации" > Выбрать организацию для редактирования > Окно просмотра организации > Окно "Добавить пользователя" > Найти пользователя для добавления > Проверить наличие пользователя > Добавить пользователя > Определить роль пользователя > Окно просмотра организации.

Создание организации и пользователей (без использования Сервиса авторизации)

Добавление организации

Для создания организации открываем пункт меню «Server Admin/Orgs» и в поле «Org.name» вводим название организации и нажимаем кнопку «Create».

Добавление пользователя организации

Для добавления пользователя организации откройте пункт меню «Server Admin/Users»:

- В поле «Org.name» вводим название организации и нажимаем кнопку «New user».
- Заполните нужные поля и нажимаем кнопку «Create».
- Проверьте что пользователь виден в меню «Users».
- Добавьте пользователя в нужную организацию. Для этого нажмите на него и попадаем в меню настройки пользователя.
- В поле «Add» «Organizations» начинаем вводим название организации, к которой нужно предоставить доступ, выбираем нужный уровень прав и нажимаем «Add».
- Удаляем доступ к организации по умолчанию «Main Org.».

Добавление источника данных (Datasource) в режиме Abyss

Как источник данных по умолчанию **Sbertech Abyss SQL**.

Для корректной работы потребуется плагин **Sbertech Abyss SQL**, необходимо проверить чтобы он был.

Для добавления источника данных (Datasources) переместите курсор на шестеренку в боковом меню, которое покажет вам меню конфигурации.

Нажмите на кнопку **Configuration >> Datasources** и нажимаем **“Add data source”**.

- Выбираем плагин SberTech Abyss SQL.
- В типе **Work Mode** указываем *Abyss*.
- Указываем endpoint подключения к Abyss, заполните поля **Project**, **AuthToken** и параметры базовой аутентификации логин/пароль;
- Если используется авторизация через Platform V IAM Proxy (AUTH), заполните поле **HeaderNamesList**, именем заголовка в котором Platform V IAM Proxy (AUTH) передает JWT токен.
- Важно! В поле name вводим название **«Indicator-Abyss»**, именно так как называется data source в дашбордах, поэтому названия должны совпадать;
- Нажимаем Save & Test.

Если все параметры введены корректно, то будет выведено оповещение Datasource is working. В поле URL указывается полный путь строки подключения к API Abyss, например Ваш_Url/coordinator/api/gateway/v1

Добавление источника данных (Datasource) в режиме BAM

Для добавления источника данных (Datasources) переместите курсор на шестеренку в боковом меню, которое покажет вам меню конфигурации:

- Нажмите на кнопку **Configuration >> Data Sources** и нажимаем **“Add data source”**;
- Выбираем плагин SberTech Abyss SQL.
- Включить **Exec On Front** для работы Data Sources в через frontend;
- В типе **Work Mode** указываем *Bam Selector*;
- Указываем endpoint подключения к Bam Selector, "Заполните поля" **AuthToken**, **HeaderNamesList**;
- Важно! В поле name вводим название **«SberTech BAM SQL»**, именно так как называется data source в дашбордах, поэтому названия должны совпадать;
- Для работы adhoc фильтра необходимо добавить переменную projectName, которая будет содержать в себе список проектов/подключений.
- Нажимаем Save & Test.

Если все параметры введены корректно, то будет выведено оповещение Datasource is working. Если не переключить Exec On Front, то работа дашбордов BAMN не гарантируется.

Adhoc фильтр, автоматом видит выбранный проект, фильтр получает rn и instanceId и отражает список колонок по этой таблице

Добавление источника данных (Datasource) в режиме Unimon Server

Для добавления источника данных (Datasources) переместите курсор на шестеренку в боковом меню, которое покажет вам меню конфигурации.

- Нажмите на кнопку **Configuration >> Datasources** и нажимаем **“Add data source”**.
- Выбираем плагин SberTech Abyss SQL.
- В типе **Work Mode** указываем *Unimon Server*;
- Указываем endpoint подключения к Unimon Server;

- Важно! В headernameslist нужно указать заголовок в котором передается передавать JWT Токен;
- В поле ParamName указываем префикс для обращения к API (rn, projectId);
- В поле paramValue указываем значение самого rn или project;
- Нажимаем Save & Test.

Если все параметры введены корректно, то будет выведено оповещение Datasource is working.

Добавление источника данных SOLR TENGRI PLUGIN

Просмотр аналитики журналов возможен через интерфейс, для этого потребуется настройка datasource SOLR TENGRI PLUGIN.

Нажмите на кнопку **Configuration >> Datasources** в боковом меню, и вы перейдете на страницу источники данных где вы можете добавлять и редактировать источники данных. Выбрать источник **SOLR TENGRI PLUGIN**, также для корректной работы потребуются Plugin **SberTable** и **SberGraf**.

Добавление источника данных (Datasource) в режиме Druid

Как источник данных по умолчанию **Sbertech Abyss SQL**.

Для корректной работы потребуется плагин **Sbertech Abyss SQL**, необходимо проверить чтобы он был.

Для добавления источника данных (Datasources) переместите курсор на шестеренку в боковом меню, которое покажет вам меню конфигурации.

Нажмите на кнопку **Configuration >> Data Sources** и нажимаем **“Add data source”**.

- Выбираем плагин SberTech Abyss SQL.
- В типе **Work Mode** указываем *Druid*.
- Указываем endpoint подключения к Abyss, заполните параметры базовой аутентификации логин/пароль;
- Важно! В поле name вводим название **«Indicator-Abyss»**, именно так как называется data source в дашбордах, поэтому названия должны совпадать;
- Нажимаем Save & Test.

Если все параметры введены корректно, то будет выведено оповещение Datasource is working.

Добавление источника данных Druid

Для добавления источника данных (Datasources) переместите курсор на шестеренку в боковом меню, которое покажет вам меню конфигурации. Если боковое меню не отображается, нажмите на значок в левом верхнем углу. Нажмите на кнопку **Configuration>>Datasources** в боковом меню, и вы перейдете на страницу источники данных где вы можете добавлять и редактировать источники данных.

Также для корректной работы потребуется плагин **Sbertech Druid SQL**, необходимо проверить чтобы он был если его нет приступаем к его настройке:

- Открываем меню **Configuration/Plugins** под учётной записью администратора организации или администратора;
- Ищем плагин Sbertech Druid SQL;

- Если он есть переходим дальше иначе требуется установка плагина;
- Переходим в меню **Configuration/Data Sources** и нажимаем **“Add data source”**;
- Выбираем плагин Sbertech Druid SQL;
- Указываем endpoint подключения к druid и параметры базовой аутентификации логин/пароль;
- Важно! В поле name вводим название **«Indicator-Druid»**,

Именно так как называется datasource в дашбордах, названия Datasource в источнике данных и на дашбордах должны совпадать;

- Нажимаем Save & Test.

Если все параметры введены корректно, то будет выведено оповещение Datasource is working.

Импорт дашбордов в конкретную организацию

Необходимо убедиться что мы находимся под нужной организацией. Для этого необходимо в крайнем нижнем левом углу нажать на икону пользователя и проверить какая организация выбрана. Если выбрана не та организация необходимо переключиться нажав Switch.

Для импорта дашбордов нажмите:

- на иконку плюса и выберете **Import**;
- Загрузить дашборд нажав на кнопку **Upload Json File**;
- По умолчанию Dashboard загружаются в папку General, чтобы выбрать другую папку, нажмите **Create**;
- После нажмите на **Import**;
- Далее необходимо указать правильное название топика в Abyss, которая зависит от **названия тенанта**;
- Для этого заходим в настройки только что импортированного дашборда через иконку шестеренки;
- Выбираем пункт меню **"Variables"**;
- Выбираем переменную **"$druidtable"**;
- В поле "Value" вводим корректное название таблицы и нажимаем **"Update"**.

Настройка ролевой модели (без использования Сервиса авторизации)

Возможность редактирования ролей доступна только для пользователя с ролью администратора организации и для пользователя с ролью администратора сервера Grafana. Ролевая модель включает в себя 3 уровня определения роли и доступов:

- уровень пользователя,
- уровень команды,
- уровень дашборда.

Уровни определения роли представлены в таблице ниже.

Уровень определения роли	**Где задается**
Уровень пользователя	Боковое меню Configuration/Users. Задается при непосредственном редактировании пользователя в списке пользователей.

Уровень определения роли	Где задается
Уровень команды	Боковое меню Configuration/Teams позволяет объединить пользователей с общим признаком в одну команду. Тесно связано с настройкой доступов в настройках дашборда.
Уровень дашборда	Меню дашборда Dashboard settings/Permissions

После успешной авторизации, администратор переходит в меню создания группы пользователей (Teams).

- Нажать на кнопку создания новой группы **New team**;
- Задать имя группы. Почта опционально;
- Нажать **Create**;
- В блоке Add team member найти и выбрать нужного пользователя;
- Нажать кнопку **Add member**;
- Вверху появилась зеленая плашка Member added to Team.

Уровень команды

Для создания группы пользователей перейдите в меню создания группы (**Teams**):

- Нажать на кнопку создания новой группы **New team**;
- Задать имя группы и при необходимости укажите адрес электронной почты;
- Нажать **Create**;
- В блоке **Add team member** найти и выбрать нужного пользователя;
- Нажать кнопку **Add member**;
- Вверху появилась зеленая плашка Member **added to Team**.

Уровень Dashboard (Аналитическая панель)

Для настройки уровня dashboard создания группы пользователей перейдите в меню создания группы (**Teams**):

1. Перейти на нужную аналитическую панель;
2. Перейти в настройки dashboard нажав на кнопку с пиктограммой шестеренки в правом верхнем углу (**Dashboard settings**);
3. Перейти в раздел **Permissions**;
4. Удалить для всех ролей, кроме Админа, доступ к dashboard;
5. На открывшейся странице нажать на кнопку **Add Permission**.
6. В открывшемся блоке **Add Permission** For задать следующие параметры:
    1. В первом поле выбрать **Team**;
    2. Во втором поле выбрать группу (team), созданную на предыдущих шагах (либо, любую необходимую);
    3. В третьем поле выбрать роль для группы.

Дополнительно. На экранной форме можно настроить доступ с определенными правами не только для группы, но и для конкретного пользователя.

Настройка уведомлений

Когда alert меняет состояние, отправляется уведомления. Каждое правило оповещения может иметь несколько уведомлений. Чтобы добавить уведомление в правило оповещения, вам

сначала нужно добавить и настроить канал уведомлений (это может быть электронная почта, webhook или другая интеграция). Это делается на странице Notification channels.

Типы каналов уведомлений	Описание
Email, SMS	Настраивается SMTP Сервер для отправки данных
WebHook	Webhook - это простой способ отправки информации об изменении состояния алерта по протоколу HTTP в пользовательскую конечную точку. Используя этот канал уведомлении, Вы можете интегрировать АС в любую другую систему по вашему выбору.
SM-incident	Представляет способ отправки информации об изменении состояния алерта в формате XML для отправки в систему HPSM.

Настройка Email, SMS

Для возможности отправки email, нужно произвести настройки SMTP в файл **indicator.conf** в раздел #Параметры для подключения SMTP.

Имя параметра	Примеры значений	Описание
#Параметры для подключения SMTP (отправка уведомлений)		
GRAFANA_SMTP_ENABLED	false или true	Включение функционала для отправки Email
GRAFANA_SMTP_SKIP_VERIFY	false или true	Если GRAFANA_SMTP_SKIP_VERIFY=true то оставить пустым параметр -> GRAFANA_SMTP_CERT_FILE=$/cert.pem. Если GRAFANA_SMTP_SKIP_VERIFY=true то оставить пустым параметр -> GRAFANA_SMTP_KEY_FILE=$/cert-key.pem
GRAFANA_SMTP_HOST	hostname	Сервер для подключения к SMTP
GRAFANA_SMTP_USER	username	УЗ для подключения к SMTP

GRAFANA_SMTP_FROM_ADDR	address@email.com	Адрес, используемый при отправке электронных писем
GRAFANA_SMTP_FROM_NAME	indicator	Имя, которое будет использоваться при отправке электронных писем
GRAFANA_SMTP_CERT_FILE	см. значение GRAFANA_SMTP_SKIP_VERIFY	Глобальная переменная. Путь к файлу сертификата для SMTP
GRAFANA_SMTP_KEY_FILE	см. значение GRAFANA_SMTP_SKIP_VERIFY	Глобальная переменная. Путь к файлу ключу для SMTP

Для настройки оповещения Вам потребуется перейти во вкладку **Alert** и нажать **Create Alert**. Вкладка доступна только для визуализации *Graph*.

См. подробнее в Руководстве прикладного разработчика

Настройка уведомления для автоматического заведение инцидента в HPSM

Выбираем пункт **Notification channels** в меню **Alerting**

- Необходимо заполнить XML;
- В меню Optional SM-incident settings необходимо вставить сертификаты;
- После выбрать галочки по сертификатам;
- Нажимаем Test;

  «Если все параметры введены корректно, то будет выведено оповещение *Test notification sent*

- Нажимаем Save.

Настройка WebHook

Уведомление webhook - это простой способ отправки информации об изменении состояния алерта по протоколу HTTP.

По webhook можно создавать разные группы рассылки. Настройка производиться в Alerting -> Notification channels , прописывается имя группы, и тип – webhook.

Пример тела json:

```
{   "dashboardId":1,   "evalMatches":[      {
"value":1,       "metric":"Count",       "tags":{}
}   ],
"imageUrl":"https://grafana.com/static/assets/img/blo
g/mixed_styles.png",   "message":"Notification
Message",   "orgId":1,   "panelId":2,   "ruleId":1,
```

```
"ruleName":"Panel Title alert",
"ruleUrl":"http://localhost:3000/d/hZ7BuVbWz/test-
dashboard?fullscreen\u0026edit\u0026tab=alert\u0026pa
nelId=2\u0026orgId=1",   "state":"alerting",
"tags":{     "tag name":"tag value"   },
"title":"[Alerting] Panel Title alert" }
```

state-возможные значения для состояния оповещения: ok, paused, alerting, pending, no_data.

Просмотр дашбордов

При нажатии на Home можно увидеть список папок с предустановленными дашбордами

Например, Если название папки начинается на V. то каталоги относятся к **Platform V Monitor** (OPM) Данные папки содержат каталогизации и список дашбордов данных сервисов согласно архитектуре платформы. Данные дашборды являются не редактируемыми так как находятся в provisining.

События системного журнала

События системного журнала — это объекты **JSON**, отражающие события или действия пользователя:

- Изменение информационных панелей и источников данных;
- Ошибки аутентификации пользователей.

В системном журнале должны публиковаться события следующего вида:

```
2021-03-31 09:33:01 t=2021-03-31T04:33:01Z
msg="Request Completed" logger=context userId=1
orgId=1 uname=admin method=GET
path=/api/datasources/proxy/152/api/prom/label
status=502 remote_addr=[::1] time_ms=1 size=0
referer="http://localhost:3000/explore?left=%5B%22now
-6h%22none%22%5D%7D%5D"
```

События мониторинга

Дашборд **Indicator metrics** состоит из набора панелей:

Наименование панели	Описание	Тип панели

Общая информация	Общая информация по запущенному приложению indicator, имя модуля контейнеризации, на котором работает приложение	таблица
Количество дашбордов	Информация о количестве дашбордов	таблица
Количество авторизованных пользователей	Информация о количестве пользователей	таблица
Количество активных пользователей	Информация о количестве активных пользователей	таблица
Время работы	Время работы кластера с момента старта (в разрезе "lables.app")	таблица
HTTP запросы (общее количество)	Количество http запросов отправленных приложением Indicator (HTTP request count в разрезе "lables.app")	график
HTTP запросы (общее количество в разрезе методов)	Количество http запросов отправленных приложением Indicator (HTTP request count в разрезе "lables.app" и методов),	график
HTTP запросы (общее количество в разрезе ошибочных статусов ответа)	Количество http запросов отправленных приложением Indicator с ошибками(HTTP request error count в разрезе "lables.app" и код состояния http: 4xx, 5xx),	график

Суммарная задержка по запросам	Суммарная длительность http запроса в разрезе "lables.app" и методов	график
HTTP ответы (общее количество в разрезе статусов ответов)	Количество http запросов с ошибками	график
Количество вызовов api	Количестве запросов к приложению Indicator в разрезе "lables.app"и методов,	график
Использование CPU (общее количество секунд)	Использование процессора кластером за период в сек.	график
Использование памяти контейнерами	Использование памяти контейнерами	график

Часто встречающиеся проблемы и пути их устранения

Ошибка	Описание
Bad Gateway undefined	Данное сообщение возникает при настройке Datasource, информирует о недоступности источника Datasource, необходимо проверить корректность ссылки endpoint
Failed to update datasource	Не удалось обновить Datasource, данное сообщение возникает при обновлении настройки Datasource, необходимо проверить корректность ссылки endpoint
SMTP not configuerd ...	Ошибка возникает при настройке алерта. Администратору необходимо выполнить настройку smtp в конфигурационном файле
Panel plugin not found	Сообщение появляется если на панели не установлен нужный плагин для отображения
Druid - not found	Данное сообщение информирует об отсутствии источника Datasource

Error:tsdb.HandleRequest() error could not find executor for datasource type:	Ошибка возникает если 2 экземпляра Indicator работают с одной БД, проверить настройки конфигурации БД

Выявленные ограничения

Оповещение по нескольким оповещениям производится однократно по первому срабатыванию.

Пример: В случае если запрос, например в разрезе server, и сработает alert по server1, в случае если в этот же период произойдет отклонение по server2 повторного оповещения не будет, т.к. alert уже взведен. Можно только настроить периодичное напоминание (Send Reminders на группе рассылки), в этом случае в письмо добавиться информация о server2.

Алерты не работают в случае, если в запросах используются переменные дашборда (кроме $time, $defaultFilter).

Не допускается подключение к одной базе данных Indicator, другого экземпляра Indicator (который не имеет тех же datasource первого экземпляра), так как это спровоцирует ошибки по оповещениям.

Не допускается подключение к одной базе данных Indicator, но с разными конфигурациями для дашбордов/datasource, так как это может вызвать ошибки.

Рекомендуется не запускать разные инсталляции одновременно на одну БД, в связи с возможными различиями как касаемо дашбордов, так и другого функционала, которого может не быть в предыдущей версии.