ПРОГРАММНЫЙ ПРОДУКТ
СЕНСОР АГРЕГАЦИИ И НОРМАЛИЗАЦИИ ДАННЫХ

Руководство по эксплуатации

2022

АННОТАЦИЯ

Данный документ предназначен для специалистов, выполняющих администрирование программного продукта «**Сенсор агрегации и нормализации данных**» и включает описание действий по настройке и администрированию программного продукта.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и функции Модуля

Сенсор агрегации и нормализации данных (далее – **Модуль**) – модуль системы управляющих воздействий Innostage Orchestrator, позволяющий получать данные от различных систем, обрабатывать их и передавать в необходимом формате в другие системы.

Модуль обеспечивает выполнение следующих функций:

- прием поступающих по протоколу UDP сообщений (например, события информационной безопасности, инвентаризационная информация);
- передача данных в систему управляющих воздействий Innostage Orchestrator для преобразования в нужный формат и дальнейшей передачи в целевые системы;
- журналирование операций обмена сообщениями между системами.

1.2 Структура Модуля

Модуль состоит из следующих основных компонентов:

- Программное обеспечение модуля Сенсора;
- Брокер сообщений.

ПО, обеспечивающее выполнение функциональных возможностей **Модуля**, устанавливается на сервер **Модуля** и состоит из приемников и обработчиков сообщений. Приемники реализуют получение данных по UDP портам, указанным в конфигурационном файле, и постановку их в очередь. Брокер сообщений RabbitMQ осуществляет управление очередями поступающих сообщений и вызов обработчиков ПО **Модуля**. Обработчики очередей реализуют отправку данных в систему управляющих воздействий Innostage Orchestrator для дальнейшего преобразования данных и передачи в целевые системы.

Управление и работа с **Модулем** осуществляется посредством выполнения команд на сервере **Модуля**.

Структурная схема **Модуля** представлена на рисунке ниже (Рисунок 1.1).

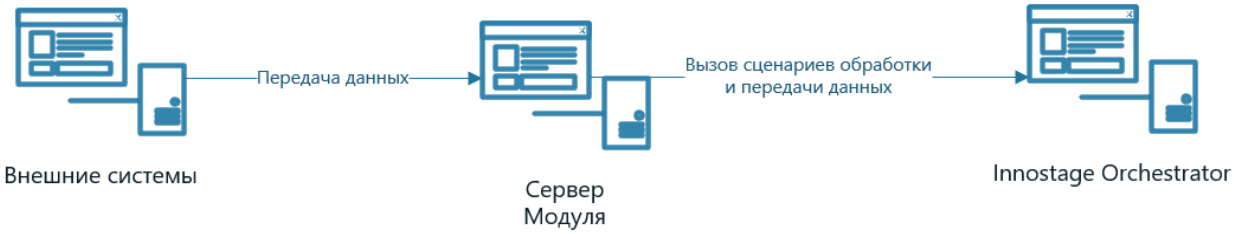

Рисунок 1.1 – Структурная схема

1.3 Требования к аппаратному и программному обеспечению

Все компоненты **Модуля** устанавливаются на один виртуальный либо физический сервер под управлением операционной системы Astra Linux 2.12, РЕД ОС 7.3, Ubuntu 20.04.

Минимальные требования к аппаратной части:

- Процессор: не менее 2 ГГц, 2 ядра.
- Оперативная память: не менее 4 Гб.
- Дисковое пространство: не менее 40 Гб свободного дискового пространства.

Требования к программной части:

- ОС (64-разрядная): Astra Linux 2.12, РЕД ОС 7.3, Ubuntu 20.04.
- Брокер сообщений: RabbitMQ 3.9.x.
- Python 3.8.

1.4 Требования к персоналу, обеспечивающему функционирование Модуля

Администратор **Модуля** должен обладать квалификацией, обеспечивающей, как минимум:

- базовые навыки администрирования ОС семейства Linux (настройка репозиториев, системные настройки и т. д.);
- базовые навыки работы с брокером сообщений RabbitMQ.

2 АДМИНИСТРИРОВАНИЕ МОДУЛЯ

2.1 Установка и обновление Модуля

2.1.1 Установка Модуля

Установка **Модуля** описана в документе «Система управляющих воздействий INNOSTAGE ORCHESTRATOR. Сенсор агрегации и нормализации данных. Руководство по развертыванию».

2.1.2 Обновление Модуля

Для обновления необходимо расположить дистрибутивы обновления ПО на сервер в директорию /opt/sensor, где расположен **Модуль**, открыть терминал и выполнить следующие команды:

```
# Активация виртуального окружения
source /opt/sensor/venv/bin/activate

# Остановка сервиса
sudo service sensor stop

# Установка дистрибутива обновления
pip install -U /opt/sensor/sensor-<version>-py3-none-any.whl

# Запуск сервиса
sudo service sensor start
```

2.2 Работа со службами Модуля

Управление запуском и остановкой служб **Модуля** осуществляется с помощью средств управления службами ОС (service, systemctl), на которой осуществлено развертывание.

Модуль включает в себя следующие службы:

- sensor – служба сенсора, обеспечивающая прием и обработку поступающих сообщений;
- rabbitmq-server – служба очереди сообщений RabbitMQ.

2.2.1 Запуск и остановка служб

Запуск и остановка служб **Модуля** осуществляется с помощью выполнения команд в терминале ОС по следующему шаблону:

- при использовании service:
  sudo service <служба> <start | stop | restart>
- при использовании systemctl:
  sudo systemctl <start | stop | restart> <служба>

2.2.2 Мониторинг текущего состояния

Мониторинг текущего состояния служб **Модуля** осуществляется с помощью выполнения команд в терминале ОС по следующему шаблону:

- при использовании service:
  sudo service <служба> status
- при использовании systemctl:
  sudo systemctl status <служба>

Текущее состояние работы можно отслеживать по статусу работы служб, в лог-файлах служб, а также в лог-файлах ПО **Модуля**.

2.3 Мониторинг и очистка лог-файлов Модуля

В процессе работы **Модуль** осуществляет журналирование событий в лог-файлы, хранящиеся на сервере:

- лог-файлы служб **Модуля**;
- лог-файлы операций обмена сообщениями **Модуля**.

Хранение лог-файлов служб **Модуля** осуществляется в следующих каталогах на сервере:

- каталог «/var/log/sensor»;
- каталог «/opt/sensor/logs».

Хранение лог-файлов операций обмена сообщениями **Модуля** осуществляется в каталоге «/opt/sensor/logs».

Рекомендуется периодическая очистка лог-файлов служб **Модуля** для освобождения дискового пространства.

2.4 Настройка Модуля

Для начала работы **Модуля** необходимо произвести его настройку в следующем порядке:

- настроить подключение к службе очереди сообщений;
- настроить прием поступающих сообщений;
- настроить подключение к системе управляющих воздействий Innostage Orchestrator.

Настройка осуществляется с помощью внесения изменений в конфигурационный файл **Модуля «**config.json», расположенный в директории «/opt/sensor».

2.4.1 Настройка подключения к службе очереди сообщений

Для настройки необходимо внести изменения в секцию «amqp» конфигурационного файла **Модуля**:

```
# Содержание секции amqp конфигурационного файла config.json
[{
        "host": "localhost",
        "port": 5672,
        "user": "guest",
        "password": "guest",
        "queues": []
}]
```

Описание секции и ее параметров для конфигурации подключения к службе очереди сообщений приведено в таблице ниже (Таблица 2.1).

Таблица 2.1 – Описание секции и ее параметров для конфигурации подключения к службе очереди сообщений

Секция	Параметр	Тип	Описание параметра
amqp	host	string	Адрес сервера службы очереди
	port	number	Порт подключения к серверу службы очереди
	user	string	Имя пользователя для подключения к службе очереди
	password	string	Пароль пользователя для подключения к службе очереди
	queues	array	Конфигурация приема поступающих сообщений

2.4.2 Настройка приема поступающих сообщений

Для настройки приема поступающих по протоколу UDP сообщений, необходимо внести изменения в секцию «amqp/queues» конфигурационного файла **Модуля**:

```
# Содержание секции amqp/queues конфигурационного файла config.json
[{
        "name": "queue_1",
        "callback": "json",
        "udpport": 49001,
        "cb_kwargs": {}
}]
```

Описание секции и ее параметров для конфигурации приема поступающих сообщений приведено в таблице ниже (Таблица 2.2).

Таблица 2.2 – Описание секции и ее параметров для конфигурации приема поступающих сообщений

Секция	Параметр	Тип	Описание параметра
amqp/queues	name	string	Имя создаваемой очереди сообщений
	callback	string	Обработчик очереди сообщений. Возможные значения: json, syslog
	udpport	number	UDP порт для приема сообщений
	cb_kwargs	object	Конфигурация передачи данных в систему управляющих воздействий Innostage Orchestrator

2.4.3 Настройка подключения к системе управляющих воздействий Innostage Orchestrator

Для настройки подключения к системе управляющих воздействий Innostage Orchestrator, необходимо внести изменения в следующие секции конфигурационного файла **Модуля**:

- orchestrator;
- general;
- amqp/queues/cb_kwargs.

Содержание секции «orchestrator» конфигурационного файла **Модуля**:

```
# Содержание секции orchestrator конфигурационного файла config.json
{
        "host": "localhost",
        "port": 443,
        "api_key": "",
        "ssl": true,
        "retry": 3,
        "delay": 10
}
```

Описание секции и ее параметров для конфигурации приема поступающих сообщений приведено в таблице ниже (Таблица 2.3).

Таблица 2.3 – Описание секции и ее параметров для конфигурации приема поступающих сообщений

Секция	Параметр	Тип	Описание параметра
orchestrator	host	string	Адрес сервера Innostage Orchestrator
	port	number	Порт подключения к серверу Innostage Orchestrator
	api_key	string	Ключ для подключения к Innostage Orchestrator
	ssl	boolean	Использование HTTPS
	retry	number	Количество попыток отправки запроса к серверу Innostage Orchestrator при отсутствии успешного ответа
	delay	number	Время ожидания между попытками отправки запроса (в секундах)

Содержание секции «general» конфигурационного файла **Модуля**:

```
# Содержание секции general конфигурационного файла config.json
{
        "tag": "Тег инсталляции Модуля (подразделение)"
}
```

Описание секции и ее параметров для конфигурации приема поступающих сообщений приведено в таблице ниже (Таблица 2.4).

Таблица 2.4 – Описание секции и ее параметров для конфигурации приема поступающих сообщений

Секция	Параметр	Тип	Описание параметра
general	tag	string	Тег инсталляции Модуля, отправляемый в Innostage Orchestrator и способный идентифицировать инсталляцию. Например, наименование подразделения.

Содержание секции «amqp/queues/cb_kwargs» конфигурационного файла **Модуля**:

```
# Содержание секции amqp/queues/cb_kwargs конфигурационного файла config.json
{
        "dag_id": "sce_test",
        "task_id": "task_test",
        "key": "param_test"
 }
```

Описание секции и ее параметров для конфигурации приема поступающих сообщений приведено в таблице ниже (Таблица 2.5).

Таблица 2.5 – Описание секции и ее параметров для конфигурации приема поступающих сообщений

Секция	Параметр	Тип	Описание параметра
amqp/queues/cb_kwargs	dag_id	string	Наименование сценария в Innostage Orchestrator
	task_id	string	Наименование задачи сценария в Innostage Orchestrator
	key	string	Ключ задачи сценария в Innostage Orchestrator, по которому необходимо передать полученное сообщение

2.5 Диагностика неисправностей

При обнаружении нарушений в процессе приема и передачи сообщений **Модулем**, необходимо осуществить диагностику неисправностей в следующем порядке:

- осуществить проверку текущего состояния служб (п. 2.2.2);

- осуществить анализ лог-файлов служб на наличие ошибок (п.2.3);
- осуществить анализ лог-файлов ПО на наличие ошибок (п.2.3);

При обнаружении ошибок, влияющих на работоспособность **Модуля**, произвести устранение неисправностей и при необходимости осуществить перезапуск служб с ошибочным статусом.

В случае, если неисправности не получается устранить самостоятельно, необходимо сформировать запрос в техническую поддержку программного продукта. К запросу приложить лог-файлы, скриншоты и описание выполняемых действий.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

Сокращение	Полное наименование
HTTPS	HyperText Transfer Protocol Secure
UDP	User Datagram Protocol
Модуль	Программное обеспечение «Сенсор агрегации и нормализации данных»
ОС	Операционная система
ПО	Программное обеспечение