Система контроля и автоматизации задач сбора данных Коллект!Ми

Collect!Me

Инструкция по установке и настройке в ОС Debian

Версия 1.3

2023

СОДЕРЖАНИЕ

Аннотация

Настоящий документ представляет собой инструкцию по установке и настройке Системы контроля и автоматизации задач сбора данных Коллект!Ми.

Сокращения

В настоящем документе использованы следующие сокращения:

Сокращение	Полное наименование
БД	База данных
ИБ	Информационная безопасность
ИС	Информационная система
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
Система, Коллект!Ми	Система контроля и автоматизации задач сбора данных Коллект!Ми (англ. Collect!Me)
СУБД	Система управления базами данных
ТЗ	Техническое задание
ТУЗ	Технологическая учетная запись
УЗ	Учетная запись
SIEM	System Information and Event Management
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование системы

Полное наименование: Система контроля и автоматизации задач сбора данных Коллект!Ми (англ. Collect!Me).

Условное обозначение и краткое наименование: Система, Коллект!Ми.

1.2 Цели и задачи Системы

Использование Системы Коллект!Ми позволяет достичь следующие цели:

- автоматизация и ведение задач по сбору данных от источников данных, обработка данных для представления в унифицированном виде;
- автоматизация действия при выполнении условий на основе обработки данных;
- снижение трудозатрат на сбор метрик и показателей от различных источников данных.

Система Коллект!Ми предназначен для решения следующих задач:

- сбор данных ИБ и ИТ от различных источников;
- хранение собранных данных с учетом временных атрибутов, а также обогащение данных;
- автоматизация сценариев и последовательностей выполнения задач, реагирования в случае выполнения некоторых условий;
- унификация задач сбора данных и приведение к единому формату;
- контроль и управление задачами сбора данных;
- интеграция с внешними системами визуализации и отчетности.

1.3 Решения по структуре Системы

Общая схема Системы Коллект!Ми представлена на рисунке (Рисунок 1).

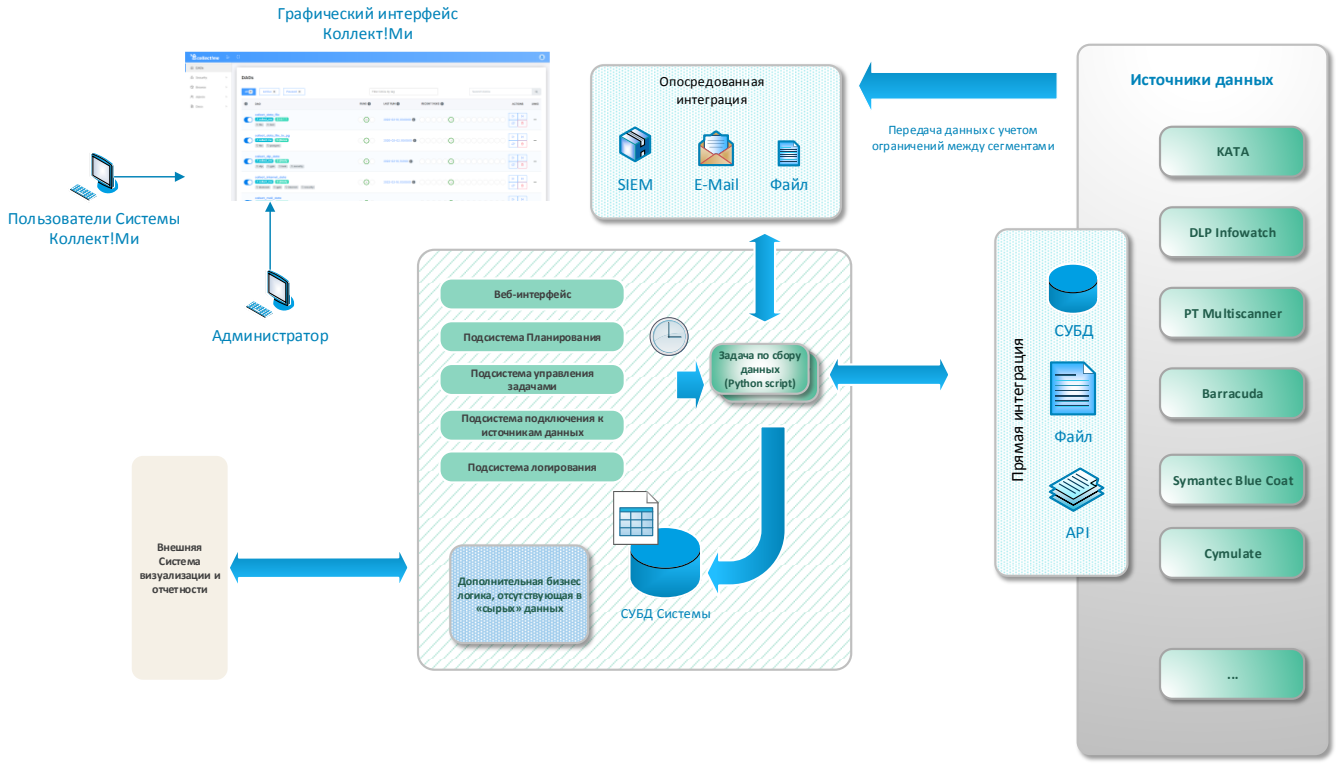

Рисунок 1

Система Коллект!Ми обеспечивает ведение задач по сбору данных от источников данных ресурсов (в качестве примера, система защиты от утечек информации, системы фильтрации данных, бухгалтерские системы, ИТ-системы и т.д.), обработку данных для представления в унифицированном виде с последующей передачей данных для хранения. По умолчанию для хранения используется СУБД Postgres.

Функции графических пользовательских интерфейсов Системы Коллект!Ми реализованы при помощи web–интерфейсов (интерфейсов взаимодействия пользователя с приложением через web–браузер). Доступ осуществляется с использованием протокола HTTP или HTTPS.

Технические решения Коллект!Ми предусматривают основной вариант развертывания, в котором все компоненты Системы находятся внутри корпоративного периметра. Передача данных за пределы корпоративного периметра не предусматривается.

2 УСТАНОВКА И НАСТРОЙКА

2.1 Общая информация

Установка выполняется в следующей последовательности:

- Установка СУБД;
- Установка Коллект!Ми.

Установка выполняется в среде ОС Debian версии не ниже 10.

Дистрибутив Коллект!Ми поставляется в виде единого tar gzip архива с именем collect-me- XX.tgz где XX – дата дистрибутива.

Состав дистрибутива:

- collect-me-installer – инсталлятор;
- collect-me-opt – архив с типовой инсталляцией (должен располагаться выше файла инсталлятора install.sh);
- collect-me-content– специализированный набор дополнительных данных.

2.2 Установка и настройка СУБД

По умолчанию предполагается использование СУБД PostgreSQL версии 12 и выше, но возможно использование в качестве хранения данных использовать любую СУБД, поддерживающую подключение по протоколам SQLAlchemy.

Далее описывается порядок установки и настройки СУБД PostgreSQL версии 13.

На сервере СУБД под УЗ root необходимо выполнить установку пакета СУБД PostgreSQL

```
apt-get update

apt install postgresql-13

apt install postgresql-client-13

pg_ctlcluster 13 main start
```

Отредактировать файл доступа /etc/postgresql/13/main/pg_hba.conf и внести разрешения сетевого доступа для трех баз данных, согласно таблице (Таблица 1):

Таблица 1

№	Имя БД	Пользователь БД	Комментарий
1	collect_me_int	collect-me_int	БД для хранения внутренней информации (расписание и т.д.) Коллект!Ми. Используется только Коллект!Ми
2	report_me	report_me	БД для хранения метрик. Используется Коллект!Ми и Репорт!Ми

Запись в файле pg_hba.conf представляется в следующем виде:

"ПУТЬ_К_БД ПОЛЬЗОВАТЕЛЬ_БД IP_ДОСТУПА ТИП ПОДКЛЮЧЕНИЯ (по умолчанию – password)"

После внесения разрешений в файл hb_pga.conf запустить сервис командой:

```
systemctl start postgresql-13
```

После запуска СУБД необходимо создать базы данных, согласно таблице (Таблица 1).

Создание БД можно выполнить любым способом, например, с помощью команд:

```
echo "Create DB user $DB_USER for DB $DB_NAME .."
sudo -u postgres psql <<EOF
CREATE DATABASE $DB_NAME;
CREATE USER $DB_USER WITH PASSWORD '$DB_PASS';
GRANT ALL PRIVILEGES ON DATABASE $DB_NAME TO $DB_USER;
\q
EOF
```

Где переменные $DB_NAME – имя БД, $DB_USER – имя пользователя БД, $DB_PASS – пароль пользователя БД.

Также для установки можно использовать вспомогательные скрипты preinstall-scripts, которые автоматизируют вспомогательные действия.

2.3 Установка и настройка Коллект!Ми

Перед установкой Коллект!Ми необходимо убедиться в наличии всех необходимых пакетов и файлов, для этого выполнить команды:

```
cd collect-me-installer
./system_check.sh
```

Скрипт system_check.sh выполняет только проверку необходимых пакетов и файлов, не выполняет установку Коллект!Ми. В случае, если каких-то пакетов или файлов не хватает, будет выведено соответствующее сообщение.

Если какой-либо пакет отсутствует, необходимо выполнить его установку командой

```
apt install PACKAGE_NAME
```

Установка Python пакета выполняется командой

```
pip install PYTHON_PACKAGE_NAME
```

На сервере Коллект!Ми под УЗ root необходимо выполнить распаковку дистрибутива командами

```
tar zxvf collect-me_XXXX.tgz
```

В каталоге collect-me-installer /config любым текстовым редактором задать конфигурационные параметры в файле install.cfg. Перечень переменных указан в таблице (Таблица 2).

Таблица 2

№	Переменная	Описание
1	DB_NAME	Имя ВНУТРЕННЕЙ БД Collect!Me, обычно collect_me_int
2	DB_USER	Пользователь для подключения к ВНУТРЕННЕЙ БД Collect!Me, обычно collect_me_int
3	DB_HOST	Узел для подключения к ВНУТРЕННЕЙ БД Collect!Me,
4	DB_PORT	Порт для подключения к ВНУТРЕННЕЙ БД Collect!Me, обычно 5432
5	DB_PASS	Пароль к ВНУТРЕННЕЙ БД Collect!Me
6	DASH_DB_NAME	Имя БД, в которой хранятся данные метрик для дашбордов, обычно report_me

7	DASH_DB_USER	Пользователь для подключения к БД, в которой хранятся метрики для дашбордов, обычно report_me
8	DASH_DB_HOST	Узел для подключения к БД
9	DASH_DB_PORT	Порт для подключения к БД, обычно 5432
10	DASH_DB_PASS	Пароль к БД, в которой хранятся метрики дашбордов
11	WEB_HOST	Адрес и порт веб-сервера для управления Collect!Me
12	WEB_PORT	Порт веб-сервера для управления Collect!Me, обычно 8080
13	SESSION_TIMEOUT_MINUTES	Таймаут действия веб-сессии (в минутах), обычно 60
14	CERT_CER_PATH	полный путь к файлу сертификата *.cer для HTTPS подключения
15	CERT_KEY_PATH	полный путь к файлу сертификата *.key для HTTPS подключения

В случае, если скрипт system_check.sh успешно отрабатывает, для запуска установки необходимо запустить инсталляционный скрипт:

```
./install.sh
```

Процесс установки интерактивный, каждое действие сопровождается соответствующим информационным сообщением.

В процессе установки создается отдельная УЗ collect-me (группа collect-me). В дальнейшем процессы Коллект!Ми выполняются от имени указанной УЗ.

В процессе установки будет дважды запрошен пароль для административной УЗ admin (для веб доступа). Запомните этот пароль.

На запрос запуска сервисов нужно согласиться. В дальнейшем сервисы стартуют автоматически при загрузке ОС.

Для просмотра статуса сервисов необходимо запустить из любой директории скрипт:

```
status_collect-me.sh
```

Система Коллект!Ми установлена в директорию /opt/collect-me/

2.4 Установка специализированного функционала

По умолчанию установка Коллект!Ми содержит только базовый функционал и не содержит в себе элементы, разработанные специально.

Для распаковки архива специализированного функционала необходимо под учетной записью root выполнить следующие команды:

```
tar zxvf collect-me-content-XXX.tgz
cd collect-me-content-XXX
```

Перейти в каталог collect-me-content- XXX/config и любым текстовым редактором при необходимости задать конфигурационные параметры в файле install.cfg. Все параметры имеют русифицированные комментарии.

Для установки специализированного функционала необходимо под учетной записью root необходимо запустить инсталляционный скрипт:

```
./install.sh
```

Процесс установки интерактивный, каждое действие сопровождается соответствующим информационным сообщением.

2.5 Настройка Коллект!Ми

Настройка подключения по протоколу LDAPS (при необходимости) выполняется согласно документу «Руководство Администратора Коллект!Ми».

Настройка параметров отправки почтовых сообщений по протоколу SMTP (при необходимости) выполняется согласно документу «Руководство Администратора Коллект!Ми».

2.6 Обновление Коллект!Ми

Обновление Коллект!Ми осуществляется аналогично процессу установки, для обновления необходимо под учетной записью root запустить скрипт:

```
cd collect-me-installer
./update.sh
```

Процесс обновления интерактивный, каждое действие сопровождается соответствующим информационным сообщением. В процессе обновления необходимые сервисы автоматически останавливаются и запускаются.

Рекомендуется сохранить архив предыдущей установки (предлагается в процессе обновления).

Обновление специализированного функционала выполняется установкой файлов «поверх», для этого необходимо запустить инсталляционный скрипт:

```
cd collect-me-content-XXX
./install.sh
```

2.7 Удаление Коллект!Ми

Удаление Коллект!Ми осуществляется аналогично процессу установки, для удаления необходимо под учетной записью root запустить скрипт:

```
cd collect-me-installer
./uninstall.sh
```

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					