ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«Begemotik»
Система поиска и установления информационных связей между данными

РУКОВОДСТВО АДМИНИСТРАТОРА

Внимание! На любом этапе установки вы можете обратиться за консультацией в службу Технической поддержки, где наши специалисты помогут на всех этапах уставновки и настройки ПО.

Также возможно предоставление доступа к **демонстрационному стенду** (demo.begemotik.group-ib.com) на территории Разработчика, где можно протестировать ПО и посмотреть на правильную конфигурацию всех компонентов. Реквизиты для доступа к демонстрационному стенду находятся в Приложении.

Аннотация

Настоящий документ содержит руководство администратора программного обеспечения «Begemotik» (система поиска и установления информационных связей между данными, далее – ПО).

Назначение ПО

Система поиска и установления информационных связей между данными «Begemotik» предназначена для поиска и анализа данных из подключенных источников.

Основными целями создания системы являются:

- Предоставление удобного и понятного Оператору интерфейса по отображению и анализу данных
- Предоставление единого интерфейса для поиска данных во всех подключенных к системе источниках данных
- Консолидация разрозненной информации из источников данных и её отображение в стандартизированном виде

Программно-аппаратные среды функционирования ПО

Требования к клиенту

ПО работает через “тонкий клиент”. Для доступа к системе необходимо использовать web-браузер на базе Chromium. (Желательно использовать браузер **Google Chrome последней версии**.)

Требования к серверу

ПО устанавливается на серверах под управлением любой Unix-совместимой ОС с использованием системы кластеризации **Docker Swarm**.

На данный момент разработчиком протестирована и гарантируется работа ПО под управлением OS семейства **Debian** версий 9 и 10 (либо Ubuntu Server 18-20 версии) в связке с **Docker-CE 20.10**

Для установки ПО требуется подключение к сети Интернет на скорости не менее 10 MBit/s. и доступ к следущим ресурсам:

- update.begemotik.group-ib.com

Требования к оборудованию

Характеристики	Минимальные	Рекомендуемые
Процессор	Intel i7 3.2GHz	Intel Xeon E5-2670 и лучше
RAM	32G	64GB
Жёсткий диск	2x240GB SSD	2x240GB NVMe

Общие принципы функционирования ПО

ПО представляет из себя клиент-серверное приложение, реализованное в виде “тонкого клиента” (SPA-приложение в веб-браузере) и сервера, состоящего из набора модулей, оформленных в виде образов Docker для удобства исталляции и использования. ПО поделенено на функциональные модули, отвечающие за интерфейс пользователя, подключение к источникам и анализ данных. Коммуникация между модулями ПО осуществляется через gRPC (по протоколу HTTP/2) и аутентификацией компонентов с использованием JWT.

Детальная информация о реализации ПО представлена в руководстве «Описание реализации».

Обязанности и функции администратора заказчика

В обязанности администратора входит:

- Произвести установку ПО
- Поддерживать функционирование ПО

Установка ПО

Подготовка к установке

В рамках подготовки к установке необходимо выполнить следующие шаги:

1. Обновить Операционную Систему и входящие в неё компоненты до последних версий.

   Пример для ОС **Debian/Ubuntu**:

   ```
   $ apt update && apt upgrade -y
   ```

2. Инициализировать Docker Swarm:

   ```
   $ docker swarm init
   ```

3. Подключить Docker Registry:

   ```
   $ docker login https://update.begemotik.group-ib.com
   ```

   Логин и пароль находятся в Приложении.

4. Создать необходимые конфигурационные файлы (docker configs):

   ```
   $ docker config create <config_name> <config_file.conf>
   ```

   Список необходимых конфигурационных файлов и их содержимое находится в Приложении. Данную процедуру необходимо повторить для каждого конфигурационного файла.

5. Создать необходимые файлы секретов (docker secrets):

   ```
   $ docker secret create <secret_name> <secret_file.txt>
   ```

   Список необходимых файлов секретов и их содержимое находится в Приложении. Данную процедуру необходимо повторить для каждого файла секретов.

6. Создать необходимые сети Docker:

   ```
   $ docker network create -d overlay -o encrypted --subnet
   10.200.0.0/16 begemotik
   $ docker network create -d overlay -o encrypted --subnet
   10.100.0.0/16 dmz
   ```

Установка компонентов

Внимание! При выполнении всех действий в данном разделе необходимо, чтобы машина, на которой происходит установка ПО имела доступ в сеть Интернет

Установка и запуск ПО происходит в несколько этапов.

1. Предварительный запуск, при котором происходит получение образов необходимых компонентов с сервера обновлений Разработчика, инициализация модулей.
2. Настройка модуля безопасности (генерация ключей компонентов, добавление ключей в настройки соответствующих компонентов)
3. Опциональная настройка модуля подключения данных (настройка подключения к необходимым источникам данных)
4. Основной запуск (на данном этапе приложение уже готово к финальной настройке и работе с пользователями)

В поставку компонентов **могут** входить следующие решения (не являющиеся частью ПО):

- Веб-сервер nginx (BSD)
- Application proxy Traefik (MIT)
- СУБД PostgreSQL (PostgreSQL – Open Source license, similar to the BSD or MIT licenses.)
- СУБД Redis (BSD)
- СУБД MongoDB (SSPL+Apache) – как источник демо-данных

Предварительный запуск

Для установки и запуска всех компонентов необходимо создать Docker Stack:

```
$ docker stack deploy --with-registry-auth --compose-file begemotik.yml begemotik
```

Настройка модуля безопасности

Внимание! На данном этапе необходимо убедиться что в конфигурационном файле модуля безопасности по пути **server:auth:token:secret** установлен надёжный секретный ключ.

Для взаимодействия с модулем Безопасности приложение должно иметь действительный AuthToken приложения, предоставляющий полномочия для выполнения определённого набора запросов к модулю Безопасности.

Для генерации токена приложения исполняемый файл Security поддерживает команду tokengen:

```
$ /bin/start tokengen
--recipient - название компонента для которого генерируется токен.
Пример: begemotik_backend
--scope - название запроса, право на выполнение которого предоставляется
в формате servicename_rpcname
    Пример:
    AuthService.AuthUser - auth_authuser
    AccountService.ModifyAccountProfile- account_modifyaccountprofile
    AccountService.GetAccount - account_getaccount
    ManagementService.RegisterCompany - management_registercompany
--expiration - срок действия токена в днях. Пример: Для действия токена
в течение года - 365
Флаг --scope (-s) может дублироваться.
```

Для генерации токенов нам понадобится доступ к модулю Безопасности:

```
$ SECURITY_CONTAINER_ID=$(docker ps | grep begemotik | grep security |
awk '{print $1};')
$ docker exec -ti $SECURITY_CONTAINER_ID bash
```

В данный момент мы находимся в конейнере security и все команды по генерации токенов выполняются именно в нём.

Список компонентов и необходимые для них разрешения для запросов описаны в Приложении.

Полученные токены необходимо добавить в конфигурационные файлы соответствующих компонентов. Обычно токены находятся в конфигурационных файлах по пути **security:token**. Также есть возможность переопределить значения конфигурационного файла через переменные окружения (**SECURITY_TOKEN**), что для токенов безопасности довольно удобно.

Переменные окружения можно как записать в stack-файл *begemotik.yml* в соответствующие блоки *environment* (рекомендуется), так и задать напрямую для сервисов средствами docker (**но в данном случае после удаления стека они пропадут**):

```
$ docker service --env-add SECURITY_TOKEN=<token> <service_name>
```

Основной запуск

После всех шагов, описанных в предыдущих пунктах, необходимо перезагрузить begemotik stack. Для этого надо выполнить следушие шаги:

```
$ docker stack rm begemotik
$ docker stack deploy --with-registry-auth --compose-file begemotik.yml
begemotik
```

Настройка ПО

После успешной установки ПО необходимо добавить первого пользователя с правами администратора. Сделать это можно только прямой записью в БД с пользователями.

```
$ DB_CONTAINER_ID=$(docker ps | grep begemotik | grep db | awk '{print
$1};')
$ docker cp add_user.sql $DB_CONTAINER_ID:/tmp
$ docker exec -ti $DB_CONTAINER_ID bash
```

После выполнения данных шагов мы попали в контейнер БД, далее пример для СУБД PostgreSQL:

```
$ su postgres
$ psql -d <begemotik_auth> -a -f /tmp/add_user.sql
$ rm /tmp/add_user.sql
```

<begemotik_auth> - необходимо заменить на название БД, которая указана в соответствующем конфигурационном файле на этапе подготовки к установке ПО.

add_user.sql - содержимое данного файла SQL указано в Приложении. Рекомендуем сменить пароль администратора на собственный перед началом установки!

Проверка корректности установки и настройки модулей ПО

Проверка корректности установки происходит в 2 этапа:

1. Все сервисы, указанные в stack-файле begemotik.yaml запушены:
2. `$ docker stack ps begemotik | grep Running`

   Если каких-то сервисов нет в списке, необходимо просмотреть записи в журнальнном файле соответствующего контейнера и исправить ошибки в конфигурации.

3. Веб-интерфейс ПО доступен и в нём отображается страница входа с предложением ввести логин и пароль для доступа к Системе.

Поддержание функционирования ПО

Поддержание функционирования ПО состоит в контроле настроек, произведенных в рамках установки ПО и функционировании Docker Swarm. Иных регламентных мероприятий со стороны администратора заказчика ПО не требует.

Приложения

Приложения предоставляются в отдельном файле формата PDF.