

Инструкция по установке программного обеспечения Spider

Оглавление

1	Область применения.....	3
2	Назначение программного обеспечения	4
3	Требования к системе	5
3.1	Требования к операционной системе	5
3.2	Аппаратные требования	5
3.3	Требования к сетевым интерфейсам.....	5
3.4	Требования к правам доступа	5
4	Подготовка к установке	6
5	Установка компонентов Spider.....	7
5.1	Компоненты системы Spider.....	7
5.2	Установка среды выполнения веб-приложения	7
5.3	Установка базы данных.....	8
5.4	Настройка базы данных.....	8
5.5	Установка аналитической базы данных	8
5.6	Настройка аналитической базы данных	9
5.7	Установка сервиса обмена сообщениями.....	9
5.8	Настройка сервиса обмена сообщениями.....	9
5.9	Установка веб-интерфейса	10
5.10	Установка брокера синхронизации	10
5.11	Настройка веб-интерфейса.....	10
5.12	Настройка брокера синхронизации	13
5.13	Создание сервисов для веб-интерфейса и брокера сообщений	17

1 Область применения

Настоящая инструкция устанавливает порядок установки и первичной настройки программного обеспечения Spider.

Документ предназначен для системных администраторов и специалистов, осуществляющих развертывание Spider в инфраструктуре заказчика.

2 Назначение программного обеспечения

Программное обеспечение Spider предоставляет пользовательский доступ к функциям продуктов Serviceripe, не имеющих собственного графического интерфейса.

Программное обеспечение предназначено для централизованного управления, контроля состояния, мониторинга событий, анализа данных и визуализации результатов работы через единый веб-интерфейс.

3 Требования к системе

3.1 Требования к операционной системе

Операционная система — Linux Server.

3.2 Аппаратные требования

Процессор — с архитектурой x86_64, не менее 4 виртуальных или физических ядер. Оперативная память — не менее 8 ГБ. Дисковое пространство — не менее 100 ГБ.

3.3 Требования к сетевым интерфейсам

Дополнительных требований к сетевым интерфейсам не предъявляется.

3.4 Требования к правам доступа

Для выполнения установки требуется пользователь с правами с административными привилегиями.

4 Подготовка к установке

Перед началом установки необходимо:

- обеспечить соответствие системы требованиям, указанным в разделе 3;
- получить учетные данные для доступа к репозиторию Serviceripe;
- обеспечить актуальную версию операционной системы;

Дополнительная подготовка к установке не требуется.

5 Установка компонентов Spider

5.1 Компоненты системы Spider

Установка компонентов выполняется из репозитория, предоставленного правообладателем программного обеспечения. Репозиторий должен быть предварительно подключён и доступен в инфраструктуре заказчика. Подключение к внешним интернет-ресурсам для установки компонентов не требуется.

Для функционирования программного обеспечения Spider используются следующие компоненты:

- SP-Spider — веб-приложение, предназначенное для управления, настройки и мониторинга программных компонентов Servicepipe;
- SP-Spider-Broker — компонент, выполняющий функции брокера синхронизации;
- Среда выполнения веб-приложения — обеспечивает запуск серверной части веб-интерфейса;
- База данных — хранит конфигурационные данные, необходимые для работы веб-интерфейса и брокера синхронизации;
- Аналитическая база данных — хранит данные о сетевой активности, событиях, метриках и агрегированных показателях, используемых для отображения статистики, построения графиков, анализа состояния системы и формирования отчётов;
- Сервис обмена сообщениями — обеспечивает передачу данных между компонентами Spider.

5.2 Установка среды выполнения веб-приложения

Установить среду выполнения веб-приложения:

```
sudo apt install nodejs=18.18.2-1nodesource1
```

5.3 Установка базы данных

Установить базу данных и библиотеку для работы с ней:

```
sudo apt install -y libpq-dev postgresql
```

5.4 Настройка базы данных

Открыть файл конфигурации для редактирования:

```
sudo nano /etc/postgresql/14/main/pg_hba.conf
```

Убедиться, что файл содержит запись:

```
host      all             all             127.0.0.1/32      scram-  
sha-256
```

Проверить наличие записи командой:

```
cat /etc/postgresql/14/main/pg_hba.conf | grep "host      all  
all             127.0.0.1/32          scram-sha-256"
```

Создать базу данных и пользователя:

```
sudo -u postgres psql
```

Выполнить команды в консоли администратора системы хранения данных:

```
CREATE DATABASE spider;
```

```
CREATE USER spider WITH ENCRYPTED PASSWORD 'password';
```

```
GRANT ALL PRIVILEGES ON DATABASE spider TO spider;
```

```
\q
```

5.5 Установка аналитической базы данных

Установить аналитическую базу данных:

```
apt-get install clickhouse-server
```

5.6 Настройка аналитической базы данных

Необходимо создать следующие таблицы в Clickhouse:

- graphite — метрики;
- graphite_index — индексы метрик;
- graphite_tagged — теги graphite.

```
clickhouse-client --multiline --multiquery <  
/usr/share/doc/clickhouse-server/graphite/dg-init.sql
```

Проверить, что все необходимые таблицы созданы:

```
clickhouse-client --query="SHOW TABLES" | wc -l
```

Открыть файл конфигурации для настройки уровня логирования:

```
sudo nano /etc/clickhouse-server/config.xml
```

Установить уровень логирования information:

```
<level>information</level>
```

Перезапустить службу:

```
sudo systemctl restart clickhouse-server
```

5.7 Установка сервиса обмена сообщениями

Установить сервис обмена сообщениями:

```
sudo apt-get install rabbitmq-server
```

5.8 Настройка сервиса обмена сообщениями

Создать пользователя:

```
sudo rabbitmqctl add_user "username" "password"
```

Назначить права доступа пользователю:

```
sudo rabbitmqctl set_permissions -p "/" "username" ".*" ".*"
".*"
```

5.9 Установка веб-интерфейса

Установить веб-интерфейс Spider:

```
sudo apt install sp-spider
```

5.10 Установка брокера синхронизации

Установить брокер синхронизации:

```
sudo apt install sp-spider-broker
```

5.11 Настройка веб-интерфейса

Сначала настраивается веб-интерфейс, затем — брокер синхронизации. В зависимости от условий установки необходимо указать параметры подключения к системе хранения данных, сервису обмена сообщениями и другим компонентам.

Открыть файл конфигурации веб-интерфейса:

```
sudo nano /opt/sp-spider/.env
```

Указать параметры в соответствии с конфигурацией стенда:

```
NODE_ENV=production
```

```
VITE_APP_PORT=3333          # Порт веб-интерфейса
```

```
HTTP_TIMEOUT=10000         # Таймаут HTTP-запросов, мс
```

IS_PRIMARY=true # Определяет, является ли интерфейс
основным, независимо от наличия резервирования

APP_SECRET=salt_salt_salt # Секретный ключ для хэширования
паролей. Не меняйте после первого запуска

Параметры подключения к базе данных

DB_HOST="localhost" # Адрес сервера базы данных

DB_PORT="5432" # Порт базы данных

DB_USER="YOUR_DB_USER" # Имя пользователя базы данных

DB_DATABASE="YOUR_DB_NAME" # Имя базы данных

DB_PASSWORD="YOUR_DB_PASSWORD" # Пароль пользователя базы
данных

Параметры сервиса обмена сообщениями для синхронизации и
брокера

RMQ_ENABLE="true" # Включает сервис обмена
сообщениями

RMQ_URL="amqp://USER:PASSWORD@localhost:5672" # URL
подключения к сервису обмена сообщениями с учётными данными

RMQ_RECONNECT_INTERVAL="5000" # Интервал переподключения к
сервису обмена сообщениями, мс

Параметры аутентификации через LDAP

LDAP_ENABLED=true # Включает интеграцию с LDAP

```
LDAP_URL="ldap://ldap.example.local:389"    # Адрес LDAP-сервера

LDAP_DN="dc=company,dc=local"    # Базовый DN каталога

LDAP_GROUP_CN="users"            # CN группы пользователей

LDAP_SERVICE_ACCOUNT_DN="uid=user1,ou=people,dc=company,dc=local"
# DN сервисной учётной записи

LDAP_SERVICE_ACCOUNT_PASSWORD="YOUR_LDAP_PASSWORD"
# Пароль сервисной учётной записи


# Параметры подключения по LDAPS

LDAP_CERT=""    # Путь к CA-сертификату при использовании LDAPS


# Параметры аутентификации через TACACS

TAC_ENABLED=true    # Включает интеграцию с TACACS

TAC_HOST="YOUR_TACACS_HOST"    # Адрес TACACS сервера

TAC_PORT="49"    # Порт TACACS

TAC_SECRET="your_secret_key"    # Секретный ключ TACACS

TAC_GROUP_NAME="group_admin,group_operator"    # Группы доступа

TAC_SERVICE_NAME="spider"    # Имя сервиса


# Параметры подключения к аналитической базе данных

CLICKHOUSE_USER=default    # Пользователь аналитической базы
данных

CLICKHOUSE_PASSWORD=password    # Пароль аналитической базы данных

CLICKHOUSE_DB=default    # База данных
```

```
CLICKHOUSE_HOST=127.0.0.1      # Адрес аналитической базы данных
CLICKHOUSE_PORT=8123           # Порт аналитической базы данных
```

При необходимости можно использовать защищённое подключение к сервису обмена сообщениями. Для этого в параметре подключения заменить протокол:

```
RMQ_URL="amqp://USER:PASSWORD@localhost:5672"
```

на:

```
RMQ_URL="amqps://USER:PASSWORD@localhost:5672"
```

5.12 Настройка брокера синхронизации

Открыть для редактирования файл `/opt/sp-spider-broker/.env`:

```
sudo nano /opt/sp-spider-broker/.env
```

Внести изменения в файл в соответствии с вашей конфигурацией:

```
APP_PORT=3335 # Порт, на котором запустится сервис
```

```
# Ключ из .env веб-интерфейса
```

```
APP_SECRET="YOUR_APP_SECRET" # Секретный ключ приложения
```

```
# Параметры от PostgreSQL из .env веб-интерфейса
```

```
DB_HOST="localhost" # Адрес сервера базы данных
```

```
DB_PORT="5432" # Порт базы данных
```

```
DB_USER="YOUR_DB_USER" # Имя пользователя базы данных
```

```
DB_DATABASE="YOUR_DB_NAME" # Имя базы данных
```

```
DB_PASSWORD="YOUR_DB_PASSWORD" # Пароль пользователя
```

Параметры сервиса обмена сообщениями из .env веб-интерфейса

RMQ_URL="amqp://USER:PASSWORD@localhost:5672" # URL
подключения к RabbitMQ

RMQ_RECONNECT_INTERVAL="5000" # Интервал переподключения к
сервису обмена сообщениями, мс

Путь к папке с политиками DosGate UH.

POLICY_PATH="/var/lib/dosgate-uh/profiles/" # Обязательно в
конце ставить "/"

Путь к конфигурации обработчика оффендеров DosGate UH

OFFENDERS_CONF_PATH="/opt/sp-spider-
broker/offenders/offenders.conf"

Путь к объектам защиты FlowCollector.

FC_MO_PATH="/opt/spfc/etc/mo/" # Обязательно в
конце ставить "/"

Путь к симлинкам на объекты защиты FlowCollector.

FC_MO_SYMLINK_PATH="/opt/spfc/etc/mo.enabled/" # Обязательно в
конце ставить "/"

Путь к объектам обучения Threshold Learner.

```
FC_LEARNER_PATH="/opt/spfc/etc/learner/"    # Обязательно в конце
ставить "/"
```

```
# Путь к симлинкам на объекты обучения Treshold Learner.
```

```
FC_LEARNER_SYMLINK_PATH="/opt/spfc/etc/learner.enabled/"
# Обязательно в конце ставить "/"
```

```
# Путь к конфигурации анализатора FlowCollector.
```

```
FC_ANALYZER_CONF_PATH="/opt/spfc/etc/analyzer.yaml"
```

```
# Путь к бинарному файлу анализатора
```

```
FC_ANALYZER_BINARY_PATH="/opt/spfc/bin/analyzer"
```

```
# Путь к конфигурации DosGate UH
```

```
DGUH_CONF="/etc/dosgate-uh.conf"
```

```
# Путь к снимкам дампов DosGate UH
```

```
DGUH_SNAPSHOTS="/var/cache/dosgate-uh-snapshots"
```

```
# Параметры GeoIP
```

```
MMDB_PATH="/etc/dosgate/GeoLite2-Country.mmdb"    # Путь к mmdb-
файлу
```

```
MMDB_DEFAULT_PATH="/usr/share/dosgate/GeoLite2-Country.mmdb"
```

```
# Путь к дефолтному mmdb файлу
```

Параметры Rlog

RLOG_RULES_PATH="/var/lib/rlog/rules/" # Путь к правилам
обработки syslog

RLOG_DUMP_PATH= "/var/lib/rlog/dumps/" # Путь к дампам Rlog

RLOG_URL= "http://127.0.0.1:3003" # URL сервиса Rlog

Параметры BGP

GOBGP_GRPC_SERVER="GOBGP_HOST:PORT" # Адрес gRPC-сервера
GoBGP

Путь к файлу со списками правил FlowSpec

FLOWSPEC_CONF_PATH="/opt/spfc/etc/"

Параметры синхронизации

UPDATE_CONFIG_INTERVAL_SECONDS=10 # Интервал обновления
конфигурации, с

SPIDER_URL="http://SPIDER_HOST:3333" # URL интерфейса
Spider

Параметры подключения к аналитической базе данных

CLICKHOUSE_USER=default # Пользователь аналитической
базы данных

CLICKHOUSE_PASSWORD=password # Пароль аналитической базы
данных

CLICKHOUSE_DB=default # База данных

```
CLICKHOUSE_HOST=127.0.0.1          # Адрес аналитической базы
данных
```

```
CLICKHOUSE_PORT=8123              # Порт аналитической базы
данных
```

5.13 Создание сервисов для веб-интерфейса и брокера сообщений

Открыть файл сервиса веб-интерфейса:

```
sudo nano /usr/lib/systemd/system/sp-spider.service
```

Добавить следующую конфигурацию:

```
[Unit]
```

```
Description=SP Spider
```

```
[Service]
```

```
ExecStart=/usr/bin/node /opt/sp-spider/server/main.js
```

```
WorkingDirectory=/opt/sp-spider
```

```
Restart=always
```

```
[Install]
```

```
WantedBy=multi-user.target
```

Открыть файл сервиса брокера синхронизации:

```
sudo nano /usr/lib/systemd/system/sp-spider-broker.service
```

Добавить следующую конфигурацию:

```
[Unit]
```

```
Description=SP Spider Broker
```

[Service]

ExecStart=/opt/sp-spider-broker/sp-spider-broker

WorkingDirectory=/opt/sp-spider-broker

Restart=always

[Install]

WantedBy=multi-user.target

Активировать и запустить сервисы:

```
sudo systemctl enable --now sp-spider sp-spider-broker
```

Проверить статус всех компонентов:

```
sudo systemctl status sp-spider
```

```
sudo systemctl status sp-spider-broker
```

```
sudo systemctl status rabbitmq-server
```

```
sudo systemctl status postgresql
```