



РУКОВОДСТВО ПО УСТАНОВКЕ

Интеллектуальный сканер защищенности веб-приложений и API
SolidPoint



АННОТАЦИЯ

Настоящий документ является руководством по установке и описывает способы установки интеллектуального сканера защищенности веб-приложений и API SolidPoint (далее по тексту — SolidPoint DAST).

ОГЛАВЛЕНИЕ

1.	УСТАНОВКА НА GNU/LINUX, В ТОМ ЧИСЛЕ С НОСИТЕЛЯ (БЕЗ ДОСТУПА К ИНТЕРНЕТУ)	4
1.1.	Подготовка к установке	4
1.2.	Добавление репозитория.....	4
1.2.1.	Добавление репозитория с носителя (без доступа к Интернету)	4
1.3.	Установка и настройка S3-хранилища.....	4
1.4.	Установка и настройка СУБД PostgreSQL.....	5
1.5.	Установка пакетов	7
1.5.1.	Узел управления	7
1.5.2.	Консольный клиент.....	7
1.5.3.	Узел сканирования.....	7
1.5.4.	Узел генерации отчетов.....	9
2.	УСТАНОВКА ЧЕРЕЗ DOCKER COMPOSE.....	10
2.1.	Создание группы и добавление пользователя	10
2.2.	Запуск	10
2.3.	Настройка	11
2.3.1.	Добавление SSL-сертификатов и HTTPS в панель управления	14
2.4.	Завершение работы	15
2.5.	Использование fuchsiactl.....	15
2.6.	Монтирование файлов для сканера.....	15
2.6.1.	Запуск сканирования.....	15
2.7.	Сервис генерации отчетов о сканировании	16
3.	УСТАНОВКА В КЛАСТЕРЕ KUBERNETES	18
3.1.	Подготовка к установке	18
3.1.1.	Развертывание базы данных для сервиса сканирования	19
3.1.2.	Развертывание базы данных для серверной части.....	19
3.1.3.	Параметры S3-соединения для сервиса сканирования.....	19
3.1.4.	Загрузка образов контейнеров в корпоративный реестр образов.....	20
3.2.	Установка в кластере Kubernetes	21
3.2.1.	Развертывание с помощью ПО Helm	21
3.2.2.	Доступность из внешней сети.....	21
3.2.3.	Переменные окружения	22
	ПРИЛОЖЕНИЕ А. ФАЙЛЫ КОНФИГУРАЦИИ ДЛЯ ОС GNU/LINUX.....	26

1. УСТАНОВКА НА GNU/LINUX, В ТОМ ЧИСЛЕ С НОСИТЕЛЯ (БЕЗ ДОСТУПА К ИНТЕРНЕТУ)

Для установки сканера SolidPoint DAST требуется дистрибутив Debian 12 «bookworm». Также возможна установка на дистрибутив Astra Linux 1.8.

Справочно файлы конфигурации приведены в приложении А **Ошибка! Источник ссылки не найден..**

Важно! Все команды запускаются пользователем с ролью «Администратор».

1.1. Подготовка к установке

В файл `$HOME/.profile` нужно добавить пути к стандартным каталогам с исполняемыми файлами в переменную `$PATH`, выполнив команду:

```
export
PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

Далее требуется установить пакет `curl`: `apt install curl`.

1.2. Добавление репозитория

При установке на Astra Linux необходимо сконфигурировать локали:

```
apt-get update
apt-get install -y locales
echo -e "en_US.UTF-8 UTF-8\nru_RU.UTF-8 UTF-8\nen_GB.UTF-8 UTF-8" | tee
/etc/locale.gen
locale-gen
update-locale LANG=en_US.UTF-8 LC_ALL=en_US.UTF-8
export LANG=en_US.UTF-8
export LC_ALL=en_US.UTF-8
```

При добавлении репозитория необходимо ввести секретный токен для получения доступа:

```
curl -fsSL repo.solidpoint.net | sh -
```

1.2.1. Добавление репозитория с носителя (без доступа к Интернету)

При добавлении репозитория с носителя (без доступа к Интернету) необходимо перейти в директорию с дистрибутивом и выполнить команду:

```
./debian/add-local-repository.sh
```

Добавлять секретный токен не требуется.

1.3. Установка и настройка S3-хранилища

Для установки S3-хранилища требуется выполнить команду:

```
apt install minio
```

Далее необходимо:

1. Добавить пользователя.

Для добавления пользователя необходимо заменить значения переменных MINIO_ROOT_USER и MINIO_ROOT_PASSWORD на пользовательские:

```
cat > /etc/default/minio << EOF
MINIO_VOLUMES=/var/lib/minio
MINIO_ROOT_USER=${MINIO_USER}
MINIO_ROOT_PASSWORD=${MINIO_PASSWORD}
EOF

mkdir /var/lib/minio
useradd minio-user
chown -R minio-user. /var/lib/minio
systemctl enable --now minio
```

2. Проверить статус S3-хранилища.

Для проверки статуса S3-хранилища следует выполнить команду: `systemctl status minio`.

1.4. Установка и настройка СУБД PostgreSQL

Для установки СУБД PostgreSQL на Debian необходимо выполнить команду:

```
apt install postgresql
su postgres -c psql
```

При установке на Astra Linux необходимо:

- Установить приоритет репозитория `repo.solidpoint.net` выше, чем у репозитория Astra Linux:

```
cat > /etc/apt/preferences.d/solidpoint.pref << EOF
Package: *
Pin: origin "repo.solidpoint.net"
Pin-Priority: 910
EOF

apt update
```

- Подключить расширенный репозиторий для установки пакета `liblvm19`. Необходимо использовать следующие команды при установке на Astra Linux версии 1.8.2 и новее:

```
cat > /etc/apt/sources.list.d/astra-extended.list <<'EOF'
deb https://dl.astralinux.ru/astra/stable/1.8_x86-64/repository-extended/
1.8_x86-64 main contrib non-free non-free-firmware
EOF
apt update
```

- Для установки на Astra linux версии 1.8.1 необходимо использовать следующую команду:

```
cat > /etc/apt/sources.list.d/astra-1.8.5-repos.list <<'EOF'
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.5/main-repository/
1.8_x86-64 main contrib non-free non-free-firmware
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.5/extended-
repository/ 1.8_x86-64 main contrib non-free non-free-firmware
EOF
apt update
```

- Установить PostgreSQL, выполнив следующую команду:

```
apt install -y postgresql-16
su postgres -c psql
```

Предупреждение. Программное обеспечение расширенного репозитория является сторонним по отношению к Astra Linux, может не дорабатываться с точки зрения выполнения требований по безопасности информации и может не проверяться при сертификации.

Ниже дано описание для дистрибутива Debian.

В следующих шагах требуется заменить значения переменных POSTGRES_PASSWORD на пользовательские:

1. Создать пользователя и базы данных для сканера:

```
> CREATE USER fuchsia WITH PASSWORD '${POSTGRES_PASSWORD}';
> CREATE DATABASE fuchsia;
> GRANT ALL PRIVILEGES ON DATABASE fuchsia TO fuchsia;
> \c fuchsia;
> GRANT ALL ON SCHEMA public TO fuchsia;
```

2. Создать пользователя и базы данных для серверной части:

```
> CREATE USER backend WITH PASSWORD '${POSTGRES_PASSWORD}';
> CREATE DATABASE solidpoint_backend;
> GRANT ALL PRIVILEGES ON DATABASE solidpoint_backend TO backend;
> \c solidpoint_backend;
> GRANT ALL ON SCHEMA public TO backend;
> quit
```

3. Установить расширение TimescaleDB:

Примечание. Версия PostgreSQL, указанная при установке пакета TimescaleDB, должна совпадать с версией установленного пакета PostgreSQL (её можно получить с помощью команды:

```
dpkg -l | grep -o 'postgresql-[0-9][0-9]*')
```

- 3.1. Установить TimescaleDB. Вместо символа «*» для команды ниже требуется указать необходимые версии:

```
apt install timescaledb-2-postgresql-* postgresql-client-*
```

3.2. Запустить настройку PostgreSQL для TimescaleDB:

```
apt install timescaledb-tools
timescaledb-tune
```

3.3. Перезапустить PostgreSQL:

```
systemctl restart postgresql
```

1.5. Установка пакетов

1.5.1. Узел управления

Установка пакетов панели управления: `apt install solidpoint-dashboard`.

В процессе установки будет предложено выполнить настройку адреса соединения базы данных. Необходимо:

1. Ввести строку подключения:

```
postgresql://backend:${POSTGRESQL_PASSWORD}@127.0.0.1:5432/solidpoint_backend
```

- Заменить значение `POSTGRESQL_PASSWORD` на пользовательское;
- Заменить IP-адрес, порт и имя пользователя, если они не имеют значения по умолчанию.

После пройденных шагов панель управления должна быть доступна извне по адресу `http://localhost:8100`.

Конфигурация веб-сервера `nginx` панели управления находится в файле `/etc/nginx/conf.d/solidpoint-frontend.conf`.

1.5.2. Консольный клиент

Для установки консольного клиента необходимо выполнить команду:

```
apt install solidpoint-cli
```

После установки данного пакета, если используется многопользовательский режим, необходимо аутентифицироваться, выполнив команду:

```
solidpoint-cli auth login -i
```

1.5.3. Узел сканирования

Примечание. Для одного узла управления имеется возможность развернуть более одного узла сканирования. Для этого следует проделать шаги данного подраздела инструкции на каждой машине, предназначенной под узел сканирования.

Для установки узла сканирования требуется выполнить команду:

```
apt install fuchsia-full
```

В процессе установки пакетов будет предложено выполнить несколько шагов по настройке:

1. Шаг строки подключения к PostgreSQL.

Необходимо:

- 1.1. Ввести строку подключения: `postgresql://fuchsia:${POSTGRESQL_PASSWORD}@127.0.0.1:5432/fuchsia;`
- 1.2. Заменить значение `POSTGRESQL_PASSWORD` на пользовательское;
- 1.3. Заменить IP-адрес, порт и имя пользователя, если они не имеют значения по умолчанию.

2. Шаг адреса S3-хранилища.

Необходимо:

- 2.1. Указать адрес S3-хранилища в формате `ip:port`, по умолчанию: `127.0.0.1:9000` (если подключение осуществляется по протоколу TLS, необходимо использовать перед адресом схему `https://`).
- 2.2. Указать заданное ранее пользовательское значение переменной `MINIO_ROOT_USER`.
- 2.3. Указать заданное ранее пользовательское значение переменной `MINIO_ROOT_PASSWORD`.

3. Шаг адреса для прослушивания сканером.

- 3.1. Необходимо ввести адрес для прослушивания соединения (например, `tcp://0.0.0.0:7075`).

4. Шаг interactsh-сервера. Необходимо выполнить следующее:

- 4.1. Указать домен персонального сконфигурированного interactsh-сервера (не требуется при наличии внутреннего заранее сконфигурированного interactsh-сервера).
- 4.2. Указать аутентификационный токен персонального interactsh-сервера, если на нем настроена аутентификация (не требуется, если настроен или используется внутренний interactsh-сервер).

5. Шаг настройки конфигурации `fuchsiactl`.

Адрес сервера должен совпадать с указанным на шаге 3 адреса для прослушивания:

```
cat > /etc/fuchsia/fuchsiactl.yml << EOF
server_address: "127.0.0.1:7075"
EOF
```

6. Шаг проверки корректности установки сканера.

Необходимо выполнить команду `systemctl status fuchsia`.

7. Шаг подключения узла сканирования к узлу управления.

Подключение к узлу сканирования можно осуществить любым из предложенных ниже способов:

- 7.1. CLI, интерактивный режим: `solidpoint-cli scanner new -i`.

Далее появится предложение к вводу значений:

```
Scanner name: > scanner_name
Scanner address: > 127.0.0.1:7075.
```

- 7.2. CLI, флаги: `solidpoint-cli scanner new -n "scanner_name" -a "127.0.0.1:7075"`.

7.3. cURL:

```
curl -sSX POST \  
https://solidpoint.local/api/scan-endpoints \  
-H 'Content-Type: application/json' \  
-d '{"name": "scanner_name", "address": "127.0.0.1:7075"}'
```

1.5.4. Узел генерации отчетов

Для установки узла генерации необходимо выполнить команду:

```
apt install solidpoint-scan-report-generator
```

2. УСТАНОВКА ЧЕРЕЗ DOCKER COMPOSE

Для развертывания сканера через Docker Compose требуется ПО Docker версии не ниже 23.0.

Варианты конфигурации:

- конфигурация с использованием файла «.env»;
- конфигурация с использованием механизма секретов.

Развертывание сканера через Docker Compose позволяет одновременно установить два узла – сканирования и управления.

2.1. Создание группы и добавление пользователя

Для создания группы `docker` необходимо выполнить команду:

```
sudo groupadd docker
```

Для добавления своего пользователя в группу `docker` необходимо выполнить команду:

```
sudo usermod -aG docker $USER
```

Для вступления изменений в силу необходимо выполнить команду:

```
newgrp docker
```

Примечание. Команды из последующих шагов следует выполнять от имени добавленного в группу пользователя.

2.2. Запуск

Для запуска необходимо:

1. При первом использовании распаковать архив с дистрибутивом. В архиве находится два варианта конфигурации Docker Compose. Первый вариант использует файл `.env` для хранения чувствительных данных (пароли для баз данных, ключи доступов к S3-совместимому хранилищу, и т. д.). Второй вариант использует встроенный в Docker механизм секретов.
2. Открыть терминал и перейти в директорию `solidpoint-compose`, полученную в результате распаковки. Все последующие примеры команд выполняются относительно этой директории.
3. Ввести секретный токен доступа, отредактировав значение переменной окружения `TOKEN` в файле `.env`, например: `TOKEN=my-secret-access-token`.
4. Настроить необходимые права доступа для локально монтированных директорий так, чтобы они были доступны для записи. Для этого необходимо выполнить следующую команду:

```
chmod a+wr fuchsiad/config/ backend/data/
```

5. Выполнить команду для запуска сервисов с конфигурацией, использующей файл `.env`:

```
docker compose up --build
```

6. Для запуска сервисов с конфигурацией, использующей механизм секретов, выполнить команду:

```
docker compose -f docker-compose-with-secrets.yml --env-file secrets.env up
--build
```

Панель управления по умолчанию доступна по адресу `http://localhost`. При использовании первого варианта конфигурации изменить адрес и порт можно в файле `docker-compose.yml`, в секции `services.dashboard.ports`. При использовании второго варианта конфигурации аналогичные изменения могут быть сделаны в файле `docker-compose-with-secrets.yml`.

2.3. Настройка

Настроить переменные окружения можно в файле `.env` при использовании первого варианта конфигурации, или в файле `secrets.env` при использовании второго варианта конфигурации. Описание переменных окружения приведено в таблице 1.

Таблица 1. Описание переменных окружения

Имя переменной	Значение по умолчанию	Описание
FUCHSIAD_POSTGRES_SERVER_URL	fuchsiad-database:5432	Адрес сервера базы данных для сервиса сканирования <code>fuchsiad</code> в формате <code>host:port</code>
FUCHSIAD_POSTGRES_DB	fuchsia	Имя базы данных PostgreSQL для сервиса сканирования <code>fuchsiad</code>
FUCHSIAD_POSTGRES_USER	fuchsia	Имя пользователя PostgreSQL для сервиса сканирования <code>fuchsiad</code>
FUCHSIAD_POSTGRES_PASSWORD	***	Пароль базы данных PostgreSQL для сервиса сканирования <code>fuchsiad</code> (используется только в первом варианте конфигурации)
FUCHSIAD_POSTGRES_PASSWORD_FILE	/tmp/secrets/fuchsiad_db_password	Путь к файлу (внутри контейнера), где будет храниться пароль базы данных PostgreSQL для сервиса сканирования <code>fuchsiad</code> (используется только во втором варианте конфигурации)
FUCHSIAD_POSTGRES_SSL_MODE	disable	Регулирует использование протокола SSL для соединения с базой данных PostgreSQL для сервиса сканирования <code>fuchsiad</code>
FUCHSIAD_SOCKET_PORT	7075	Адрес TCP-порта сервиса сканирования <code>fuchsiad</code>
FUCHSIAD_SOCKET_ADDR	fuchsiad	Адрес, по которому другие контейнеры могут взаимодействовать с <code>fuchsiad</code>
FUCHSIAD_CONFIG_DIR	/etc/fuchsia	Директория, содержащая конфигурационные файлы сервиса сканирования <code>fuchsiad</code>

Имя переменной	Значение по умолчанию	Описание
FUCHSIAD_OMIT_JOB_LOGS	false	Если имеет значение true, то записи журнала задач сервиса сканирования не передаются на стандартные потоки вывода или ошибок (только сохраняются в S3-совместимое хранилище)
FUCHSIAD_LOGS_FILE	Не задано	Если значение задано, то записи журнала сервиса сканирования дублируются в указанный файл
FUCHSIAD_CREDENTIALS_FILE	Не задано	Если значение задано, то файл используется как дополнение к конфигурации сервиса сканирования fuchsiad. Необходимо для хранения чувствительной информации отдельно от основной конфигурационной директории, заданной переменной окружения FUCHSIAD_CONFIG_DIR (например, в директории только для чтения)
BACKEND_POSTGRES_SERVER_URL	backend-database:5432	Адрес сервера базы данных для бэкенда в формате host:port
BACKEND_POSTGRES_DB	backend	Имя базы данных PostgreSQL для серверной части
BACKEND_POSTGRES_USER	backend	Имя пользователя PostgreSQL для серверной части
BACKEND_POSTGRES_PASSWORD	***	Пароль базы данных PostgreSQL для серверной части (используется только в первом варианте конфигурации)
BACKEND_POSTGRES_PASSWORD_FILE	/tmp/secrets/backend_db_password	Путь к файлу (внутри контейнера), где будет храниться пароль базы данных PostgreSQL для серверной части (используется только во втором варианте конфигурации)
BACKEND_POSTGRES_SSL_MODE	disable	Регулирует использование протокола SSL для соединения с базой данных PostgreSQL для серверной части
BACKEND_STATE_DIRECTORY	/var/lib/fuchsia/backend	Директория, в которой хранится состояние серверной части
BACKEND_LISTEN_PORT	8085	Адрес TCP-порта серверной части
BACKEND_ADDR	backend	Адрес, по которому другие контейнеры могут взаимодействовать с серверной частью
BACKEND_LOGS_FILE	Не задано	Если значение задано, то записи журнала серверной части дублируются в указанный файл

Имя переменной	Значение по умолчанию	Описание
BACKEND_DATABASE_URI_FILE	Не задано	Если значение задано, то строка подключения к PostgreSQL считывается из файла, путь к которому указан в данной переменной, а не из переменной окружения
BACKEND_SMTP_USERNAME	Не задано	Имя пользователя SMTP-клиента
BACKEND_SMTP_PASSWORD	Не задано	Пароль пользователя SMTP-клиента
BACKEND_SMTP_ADDRESS	Не задано	Адрес SMTP-клиента в формате host:port или ip:port. Выбор номера порта влияет на использование TLS: Порт 25 — без использования TLS (не рекомендуется). Порт 465 — использование TLS. Порт 587 — использование STARTTLS (рекомендуется)
S3_SERVER_URL	http://minio:9000	Адрес сервера S3-совместимого хранилища в формате schema://host:port
S3_ROOT_USER	fuchsia	Ключ доступа пользователя root к S3-совместимому хранилищу (используется только в первом варианте конфигурации)
S3_ROOT_USER_FILE	/tmp/secrets/s3_root_user	Путь к файлу (внутри контейнера), где будет храниться ключ доступа пользователя root к S3-совместимому хранилищу (используется только во втором варианте конфигурации)
S3_ROOT_PASSWORD	***	Пароль пользователя root к S3-совместимому хранилищу (используется только в первом варианте конфигурации)
S3_ROOT_PASSWORD_FILE	/tmp/secrets/s3_root_password	Путь к файлу (внутри контейнера), где будет храниться пароль пользователя root к S3-совместимому хранилищу (используется только во втором варианте конфигурации)
S3_NO_CHECK_CERT	true	Регулирует игнорирование самозаверенных серверных сертификатов при использовании протоколов SSL/TLS
INTERACTSH_DOMAIN	Не задано	Домен сконфигурированного interactsh-сервера. Оставьте пустым для использования внутреннего заранее сконфигурированного interactsh-сервера
INTERACTSH_TOKEN	Не задано	Аутентификационный токен interactsh-сервера. Если настроена аутентификация персонального заранее сконфигурированного interactsh-

Имя переменной	Значение по умолчанию	Описание
		сервера, укажите его аутентификационный токен; Если аутентификация не настроена или используется внутренний interactsh-сервер, оставьте пустым
CHANNEL	stable	Указание канала репозитория deb-пакетов
TOKEN	Не задано	Токен для доступа к репозиторию deb-пакетов
TZ	Europe/Moscow	Задаёт временную зону

Примечание. Дальнейшие команды указаны для первого варианта дистрибутива. Для их переиспользования со вторым вариантом к команде `docker compose` необходимо добавить флаги:

```
-f docker-compose-with-secrets.yml --env-file secrets.env
```

2.3.1. Добавление SSL-сертификатов и HTTPS в панель управления

Для добавления SL-сертификатов и HTTPS в панель управления необходимо выполнить следующее:

1. В файле конфигурации `docker-compose.yml` для блока настроек панели управления добавить блок `volumes` и в блоке `ports` указать маппинг для порта 443:

```
dashboard:
  image: repo.solidpoint.net/dashboard:25.17.1
  env_file:
    - .env
  depends_on:
    - backend
  ports:
    - 0.0.0.0:80:8100
    - 0.0.0.0:443:8443
  volumes:
    - ./dashboard/conf.d:/tmp/conf.d:rw
    - ./dashboard/certs:/etc/nginx/certs:ro
  logging:
    driver: journald
  networks:
    - dashboard
    - external
```

2. В директории с файлом конфигурации `docker-compose.yml` создать директории `dashboard/conf.d` и `dashboard/certs`.
3. В директории `dashboard/certs` добавить сертификаты вида `<cert_name>.cert` и `<cert_name>.key`.
4. В директории `dashboard/conf.d` создать файл `https.conf` со следующей конфигурацией:

```
server {
    listen 8443 ssl;
    server_name _;
    ssl_certificate /etc/nginx/certs/<cert_name>.cert;
    ssl_certificate_key /etc/nginx/certs/<cert_name>.key;
    include /usr/share/solidpoint/frontend/nginx.conf;
}
```

2.4. Завершение работы

Для завершения работы и очистки томов (флаг `-v`) необходимо выполнить команду:

```
docker compose down -v
```

Для удаления неименованных томов необходимо выполнить команду:

```
./remove-unnamed-volumes.sh
```

2.5. Использование fuchsiactl

Предупреждение. Консольный клиент `fuchsiactl` предназначается для прямого доступа к сервису сканирования `fuchsiad`.

Консольным клиентом `fuchsiactl` можно пользоваться, добавив следующий ярлык (алиас) для запуска его внутри контейнера:

```
alias fuchsiactl="docker compose exec fuchsiad fuchsiactl"
```

После этого можно использовать консольный клиент, например, выполнив команду:

```
fuchsiactl help
```

2.6. Монтирование файлов для сканера

Директория `fuchsiad/files/` в корне дистрибутива примонтирована внутри контейнера `fuchsiad` в директорию `/files`.

2.6.1. Запуск сканирования

1. Использование OpenAPI-спецификации.

Находясь в корневой директории дистрибутива, нужно переместить файлы OpenAPI-спецификации в директорию `fuchsiad/files/`, например:

```
cp /path/to/spec.json fuchsiad/files/
```

Далее следует использовать `fuchsiactl` для запуска сканирования, указывая необходимые файлы относительно директории `/files`, например:

```
fuchsiactl scan --url http://example.com --file "openapi-hars-generator:OpenAPISpec@/files/spec.json"
```

2. Использование клиентского TLS-сертификата.

Для использования клиентского TLS-сертификата нужно выполнить команду:

```
fuchsiactl scan --url https://example.com --
file=@proxy:CERT.crt@/files/somecert.crt --
file=@proxy:CERT.key@/files/somecert.key
```

2.7. Сервис генерации отчетов о сканировании

Сервис генерации отчётов о сканировании предназначен для генерации PDF-отчётов.

Важно! Данный сервис рекомендуется запускать в изолированной среде (на отдельной машине), поэтому для службы создания отчетов о проверке используются профили Docker Compose.

Переменные окружения сервиса генерации отчетов приведены в таблице 2.

Таблица 2. Переменные окружения сервиса генерации отчетов

Имя переменной	Значение по умолчанию	Описание
SCAN_REPORT_GENERATOR_ADDR	scan-report-generator	Имя сервиса генерации отчётов, отображаемое во внутренней сети Docker Compose. В процессе развёртывания необходимо изменить на используемый адрес
SCAN_REPORT_GENERATOR_PORT	9090	Порт машины, на которой развёрнут сервис генерации отчётов. В процессе развёртывания необходимо изменить, если используется порт не по умолчанию
SCAN_REPORT_GENERATOR_STATE_DIRECTORY	/var/lib/solidpoint/scan-report-generator	Указывает директорию, в которой хранятся файлы, связанные с отчётами
SCAN_REPORT_GENERATOR_LOGS_FILE	Не задано	Если значение задано, то записи журнала сервиса генерации отчётов о сканировании дублируются в указанный файл

Существует два способа развёртывания с помощью Docker Compose:

1. Использование конфигурации Docker Compose для сервиса scan-report-generator для развёртывания на отдельной машине (рекомендуется).
- Загрузите из хранилища архивов конфигурацию вида solidpoint-compose-v{RELEASE}.tgz, где RELEASE – необходимая версия. Команда для выполнения: docker compose up.

- На отдельной машине загрузите из хранилища архивов конфигурацию вида `solidpoint-compose-generator-v{RELEASE}.tgz`, где `RELEASE` – необходимая версия. Команда для выполнения: `docker compose up`.
2. Запуск всех сервисов на одной машине (не рекомендуется).
- Загрузите из хранилища архивов конфигурацию вида `solidpoint-compose-v{RELEASE}.tgz`, где `RELEASE` – необходимая версия. Команда для выполнения: `docker compose --profile reporter up`.

3. УСТАНОВКА В КЛАСТЕРЕ KUBERNETES

Совместимые с Kubernetes версии ПО приведены в таблице 3.

Таблица 3. Совместимые с Kubernetes версии ПО

Рекомендуемое ПО	Версия рекомендуемого ПО	Альтернативное ПО	Версия альтернативного ПО
Helm	3	—	—
PostgreSQL	16+	Postgres DB (Platform V Pangolin SE)	6.x.x (используются стандартные API)
MinIO	Latest (используются стандартные API)	Ceph	Latest (используются стандартные API)

3.1. Подготовка к установке

В директории дистрибутива присутствуют основные файлы, приведенные в таблице 4.

Таблица 4. Основные файлы директории дистрибутива

Имя файла	Описание
values.yaml	Файл, содержащий значения переменных, требуемых для развертывания. Требуется ручное редактирование параметров перед развертыванием
images/solidpoint-backend.tar	Образ контейнера с серверной частью
images/solidpoint-dashboard.tar	Образ контейнера с веб-интерфейсом
images/solidpoint-fuchsiad.tar	Образ контейнера с сервисом сканирования
chart.yaml	Файл метаданных Helm-чарта
templates/	Каталог, в котором содержатся манифесты

Примечание 1. Архивы образов опциональны и не всегда поставляются в дистрибутиве.

Примечание 2. Если производится обновление предыдущей инсталляции, достаточно переиспользовать ранее созданные параметры в `values.yaml` для баз данных и для S3-хранилища. Структуры данных и схемы будут автоматически обновлены при запуске новой версии.

Примечание 3. Структура файла `values.yaml` может отличаться в разных версиях дистрибутива.

Развертывание баз данных PostgreSQL и S3-хранилища, как правило, производится заранее. Не рекомендуется развертывать базы данных в Kubernetes.

3.1.1. Развертывание базы данных для сервиса сканирования

Необходимо развернуть базу данных на основе PostgreSQL для сервиса сканирования со списком параметров (см. таблицу 5), затем занести значения в параметры файла `values.yaml`.

Таблица 5. Параметры для файла `values.yaml` для сервиса сканирования

Параметр <code>values.yaml</code>	Описание
<code>FUCHSIAD_POSTGRES_SERVER_URL</code>	URL-адрес базы данных сервиса сканирования
<code>FUCHSIAD_POSTGRES_DB</code>	Имя базы данных сервиса сканирования
<code>FUCHSIAD_POSTGRES_USER</code>	Имя пользователя для базы данных сервиса сканирования
<code>FUCHSIAD_POSTGRES_PASSWORD</code>	Пароль пользователя
<code>FUCHSIAD_POSTGRES_SSL_MODE</code>	Регулирует использование протокола SSL для соединения с базой данных

3.1.2. Развертывание базы данных для серверной части

Необходимо развернуть базу данных на основе PostgreSQL для серверной части со списком параметров (см. таблицу 6), затем занести значения в параметры файла `values.yaml`.

Таблица 6. Параметры для файла `values.yaml` для серверной части

Параметр <code>values.yaml</code>	Описание
<code>BACKEND_POSTGRES_SERVER_URL</code>	URL-адрес базы данных серверной части
<code>BACKEND_POSTGRES_DB</code>	Имя базы данных серверной части
<code>BACKEND_POSTGRES_USER</code>	Имя пользователя для базы данных серверной части
<code>BACKEND_POSTGRES_PASSWORD</code>	Пароль пользователя
<code>BACKEND_POSTGRES_SSL_MODE</code>	Регулирует использование протокола SSL для соединения с базой данных

3.1.3. Параметры S3-соединения для сервиса сканирования

Предварительное создание бакетов в S3-хранилище не требуется, они автоматически создаются сканером. Значения параметров нужно присвоить соответствующим параметрам файла `values.yaml` (см. таблицу 7).

Таблица 7. Параметры S3-соединения файла `values.yaml` для сервиса сканирования

Параметр <code>values.yaml</code>	Описание
<code>S3_SERVER_URL</code>	URL-адрес API S3-интерфейса
<code>S3_ROOT_USER</code>	Пользователь S3 с правами на создание bucket
<code>S3_ROOT_PASSWORD</code>	Пароль пользователя

3.1.4. Загрузка образов контейнеров в корпоративный реестр образов

Для загрузки образов контейнеров в корпоративный реестр образов следует:

1. Создать пространство имён: `kubectl create namespace solidpoint`.
2. Загрузить три образа из архива в среду выполнения контейнеров (имена образов находятся в таблице 9):
`docker load < [имя_образа]`.
3. Загрузить образы в корпоративный реестр: `docker push [имя_образа]`.
4. Если корпоративный реестр доступен только с помощью аутентификации, создать секрет в пространстве имён, в котором планируется установка приложения, например:

```
apiVersion: v1
kind: Secret
metadata:
  name: registry
  namespace: solidpoint
data:
  .dockerconfigjson: [config]
type: kubernetes.io/dockerconfigjson
```

Имя данного секрета необходимо внести в файл `values.yaml` (см. таблицу 8).

Таблица 8. Секрет для файла `values.yaml`

Параметр <code>values.yaml</code>	Параметры из коробки. Необходимо сменить на актуальные	Описание
<code>imagePullSecrets</code>	Параметры	Секрет для доступа к корпоративному Docker Registry

5. Если загрузка образов планируется из корпоративного реестра поставщика, создать секрет с данными для аутентификации (имя пользователя и пароль при необходимости будут поставлены вместе с дистрибутивом):

```
kubectl create secret docker-registry registry --docker-
server=repo.solidpoint.net --docker-username=USERNAME --docker-
password=PASSWORD -n solidpoint
```

6. Для всех трех образов отредактируйте содержимое файла `values.yaml`, как указано в таблице 9.

Таблица 9. Параметры для файла `values.yaml` для корпоративного реестра образов

Параметр <code>values.yaml</code>	Параметры производителя. Необходимо сменить на актуальные для внутреннего реестра	Описание
<code>dashboard.repository</code>	<code>nexus.solidlab.ru/solidlab-dast/solidpoint-dashboard</code>	Имя образа панели управления
<code>dashboard.tag</code>	<code>26.1.0</code>	Тег образа панели управления

Параметр values.yaml	Параметры производителя. Необходимо сменить на актуальные для внутреннего реестра	Описание
backend.repository	repo.solidlab.ru/solidlab-dast/solidpoint-backend	Имя образа серверной части
backend.tag	26.1.0	Тег образа серверной части
fuchsiad.repository	repo.solidlab.ru/solidlab-dast/solidpoint-fuchsiad	Имя образа сканера
fuchsiad.tag	26.1.0	Тег образа сканера

Важно! В случае предварительной загрузки и получения образов через корпоративный реестр необходимо сменить дефолтные данные поставщика на имя и тег образа, которые содержатся в вашем корпоративном реестре.

После загрузки в корпоративный реестр при необходимости можно заменить значения параметров values.yaml на пользовательские.

3.2. Установка в кластере Kubernetes

3.2.1. Развертывание с помощью ПО Helm

На данном этапе уже должен быть отредактирован файл values.yaml с актуальными параметрами. Для развертывания на сервере необходимо выполнить команду:

```
helm install solidpoint . -f values.yaml -n solidpoint
```

3.2.2. Доступность из внешней сети

Необходимо настроить Ingress для сервиса solidpoint-dast-dashboard, чтобы обеспечить доступность веб-интерфейса. Для этого в файле values.yaml следует изменить значения указанных в таблице 10 полей на пользовательские в зависимости от конфигурации кластера и требований.

Таблица 10. Значения полей

Параметр	По умолчанию	Примеры	Описание
dashboard.ingress.enabled	false	true, false	Включает или отключает создание ресурса Ingress. При значении false доступ возможен только через kubectl port-forward
dashboard.ingress.hostname	Не задано	https://solidpoint.example.com	Адрес, по которому будет доступна панель управления. Необходимо указать, если dashboard.ingress.enabled: true

Параметр	По умолчанию	Примеры	Описание
<code>dashboard.ingress.ingressClassName</code>	Не задано	nginx, traefik	Указывает, какой Ingress-контроллер должен обслуживать этот ресурс. Если не указан, используется класс по умолчанию кластера

3.2.3. Переменные окружения

Список всех доступных переменных окружения представлен в таблице 11.

Таблица 11. Доступные переменные окружения

Имя переменной	Значение по умолчанию	Описание
<code>FUCHSIAD_POSTGRES_SERVER_URL</code>	Не задано	Адрес сервера базы данных для сервиса сканирования <code>fuchsiad</code> в формате <code>host:port</code>
<code>FUCHSIAD_POSTGRES_DB</code>	Не задано	Имя базы данных PostgreSQL для сервиса сканирования <code>fuchsiad</code>
<code>FUCHSIAD_POSTGRES_USER</code>	Не задано	Имя пользователя PostgreSQL для сервиса сканирования <code>fuchsiad</code>
<code>FUCHSIAD_POSTGRES_PASSWORD</code>	Не задано	Пароль базы данных PostgreSQL для сервиса сканирования <code>fuchsiad</code> (используется только в первом варианте конфигурации)
<code>FUCHSIAD_POSTGRES_PASSWORD_FILE</code>	<code>/tmp/secrets/fuchsiad_db_password</code>	Путь к файлу (внутри контейнера), где будет храниться пароль базы данных PostgreSQL для сервиса сканирования <code>fuchsiad</code> (используется только во втором варианте конфигурации)
<code>FUCHSIAD_POSTGRES_SSL_MODE</code>	<code>require</code>	Регулирует использование протокола SSL для соединения с базой данных PostgreSQL для сервиса сканирования <code>fuchsiad</code>
<code>FUCHSIAD_SOCKET_PORT</code>	<code>7075</code>	Адрес TCP-порта сервиса сканирования <code>fuchsiad</code>
<code>FUCHSIAD_SOCKET_ADDR</code>	Вычисляется на основе заданного пространства имен	Адрес, по которому другие контейнеры могут взаимодействовать с <code>fuchsiad</code>
<code>FUCHSIAD_OMIT_JOB_LOGS</code>	<code>false</code>	Если имеет значение <code>true</code> , то записи журнала задач сервиса сканирования не передаются на стандартные потоки вывода или ошибок (только сохраняются в S3-совместимое хранилище)

Имя переменной	Значение по умолчанию	Описание
FUCHSIAD_LOGS_FILE	/var/log/fuchsia/fuchsiad.log	Если значение задано, то записи журнала сервиса сканирования дублируются в указанный файл
FUCHSIAD_CREDENTIALS_FILE	/tmp/secrets/fuchsiad	Если значение задано, то файл используется как дополнение к конфигурации сервиса сканирования fuchsiad. Необходимо для хранения чувствительной информации отдельно от основной конфигурационной директории, заданной переменной окружения FUCHSIAD_CONFIG_DIR (например, в директории только для чтения)
BACKEND_POSTGRES_SERVER_URL	Не задано	Адрес сервера базы данных для бэкенда в формате host:port
BACKEND_POSTGRES_DB	Не задано	Имя базы данных PostgreSQL для серверной части
BACKEND_POSTGRES_USER	Не задано	Имя пользователя PostgreSQL для серверной части
BACKEND_POSTGRES_PASSWORD	Не задано	Пароль базы данных PostgreSQL для серверной части (используется только в первом варианте конфигурации)
BACKEND_POSTGRES_PASSWORD_FILE	/tmp/secrets/backend_db_password	Путь к файлу (внутри контейнера), где будет храниться пароль базы данных PostgreSQL для серверной части (используется только во втором варианте конфигурации)
BACKEND_POSTGRES_SSL_MODE	require	Регулирует использование протокола SSL для соединения с базой данных PostgreSQL для серверной части
BACKEND_STATE_DIRECTORY	/tmp/solidpoint-backend	Директория, в которой хранится состояние серверной части
BACKEND_LISTEN_PORT	8085	Адрес TCP-порта серверной части
BACKEND_ADDR	Вычисляется на основе заданного пространства имен	Адрес, по которому другие контейнеры могут взаимодействовать с серверной частью
BACKEND_LOGS_FILE	/var/log/solidpoint/solidpoint-backend.log	Если значение задано, то записи журнала серверной части дублируются в указанный файл
BACKEND_DATABASE_URI_FILE	/tmp/secrets/backend	Если значение задано, то строка подключения к PostgreSQL считывается из файла, путь к которому указан в данной переменной, а не из переменной окружения
BACKEND_SMTP_USERNAME	Не задано	Имя пользователя SMTP-клиента

Имя переменной	Значение по умолчанию	Описание
BACKEND_SMTP_PASSWORD	Не задано	Пароль пользователя SMTP-клиента
BACKEND_SMTP_ADDRESS	Не задано	Адрес SMTP-клиента в формате host:port или ip:port. Выбор номера порта влияет на использование TLS: Порт 25 — без использования TLS (не рекомендуется). Порт 465 — использование TLS. Порт 587 — использование STARTTLS (рекомендуется)
S3_SERVER_URL	Не задано	Адрес сервера S3-совместимого хранилища в формате schema://host:port
S3_ROOT_USER	Не задано	Ключ доступа пользователя root к S3-совместимому хранилищу (используется только в первом варианте конфигурации)
S3_ROOT_USER_FILE	/tmp/secrets/s3_root_user	Путь к файлу (внутри контейнера), где будет храниться ключ доступа пользователя root к S3-совместимому хранилищу (используется только во втором варианте конфигурации)
S3_ROOT_PASSWORD	Не задано	Пароль пользователя root к S3-совместимому хранилищу (используется только в первом варианте конфигурации)
S3_ROOT_PASSWORD_FILE	/tmp/secrets/s3_root_password	Путь к файлу (внутри контейнера), где будет храниться пароль пользователя root к S3-совместимому хранилищу (используется только во втором варианте конфигурации)
S3_NO_CHECK_CERT	true	Регулирует игнорирование самозаверенных серверных сертификатов при использовании протоколов SSL/TLS
SCAN_REPORT_GENERATOR_ADDR	Вычисляется на основе заданного пространства имен	Имя сервиса генерации отчётов, отображаемое во внутренней сети Docker Compose. В процессе развёртывания необходимо изменить на используемый адрес
SCAN_REPORT_GENERATOR_PORT	9090	Порт машины, на которой развёрнут сервис генерации отчётов. В процессе развёртывания необходимо изменить, если используется порт не по умолчанию
SCAN_REPORT_GENERATOR_STATE_DIRECTORY	/tmp/solidpoint-scan-report-generator	Указывает директорию, в которой хранятся файлы, связанные с отчётами
SCAN_REPORT_GENERATOR_LOGS_FILE	Не задано	Если значение задано, то записи журнала сервиса генерации отчётов о сканировании дублируются в указанный файл

Имя переменной	Значение по умолчанию	Описание
INTERACTSH_DOMAIN	Не задано	Домен сконфигурированного interactsh-сервера. Оставьте пустым для использования внутреннего заранее сконфигурированного interactsh-сервера
INTERACTSH_TOKEN	Не задано	Аутентификационный токен interactsh-сервера. Если настроена аутентификация персонального заранее сконфигурированного interactsh-сервера, укажите его аутентификационный токен; Если аутентификация не настроена или используется внутренний interactsh-сервер, оставьте пустым
CHANNEL	stable	Указание канала репозитория deb-пакетов
TOKEN	Не задано	Токен для доступа к репозиторию deb-пакетов
TZ	Europe/Moscow	Задаёт временную зону

ПРИЛОЖЕНИЕ А. ФАЙЛЫ КОНФИГУРАЦИИ ДЛЯ ОС GNU/LINUX

Файлы, расположенные в каталоге `/etc/default/` приведены в таблице 12.

Таблица 12. Файлы, расположенные в каталоге `/etc/default/`

Имя файла	Описание
<code>solidpoint-backend</code>	Файл конфигурации серверной части
<code>solidpoint-scan-report-generator</code>	Файл конфигурации генератора отчётов
<code>minio</code>	Файл конфигурации S3-хранилища

Файлы, расположенные в каталоге `/etc/fuchsia/` приведены в таблице 13.

Таблица 13. Файлы, расположенные в каталоге `/etc/fuchsia/`

Имя файла	Описание
<code>config.yml</code>	Файл конфигурации сканера <code>fuchsiad</code>
<code>powby2_config.yml</code>	Файл конфигурации модуля пассивного сигнатурного анализа <code>Powby2</code>
<code>fuchsiactl.yml</code>	Файл конфигурации консольного клиента <code>fuchsiactl</code>
<code>waf-har-extractor_config.yml</code>	Файл конфигурации модуля интеграции с SolidWall WAF
<code>waf-har-extractor_filters.yml</code>	Файл конфигурации фильтров модуля интеграции с SolidWall WAF. Фильтры — это карта списков фильтров для различных типов персональных данных