ПРОГРАММНЫЙ ПРОДУКТ

СИСТЕМА ИНВЕНТАРИЗАЦИИ СЕТЕВЫХ УСТРОЙСТВ

СКАНЕР

Руководство по эксплуатации

2023

АННОТАЦИЯ

Данный документ предназначен для специалистов, выполняющих администрирование программного продукта «Система инвентаризации сетевых устройств **Сканер**» (далее – **Система**) и включает описание действий по администрированию и работе с программным продуктом.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и функции Системы

Основным назначением **Системы** является инвентаризация ИТ-инфраструктуры предприятия.

Система обеспечивает выполнение следующих функций:

- обнаружение устройств в сети;
- сбор инвентаризационных данных с устройств;
- определение типов сканируемых устройств;
- хранение истории сканирования;
- логирование операций.

1.2 Структура Системы

Система состоит из следующих основных компонентов:

- ПО Системы;
- БД Системы PostgreSQL;
- исполнитель задач Celery;
- брокер сообщений Redis.

ПО, обеспечивающее выполнение функциональных возможностей **Системы**, устанавливается на сервер **Системы**. Брокер сообщений осуществляет управление очередями поступающих запросов на сканирование и передачу данных исполнителю задач. Задачи сканирования выполняются параллельно. Данные, получаемые в ходе сканирования, записываются в БД **Системы**.

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

Рисунок 1.1 – Структурная схема

1.3 Требования к аппаратному и программному обеспечению

Все компоненты **Системы,** устанавливаются на один виртуальный либо физический сервер под управлением ОС, поддерживающей систему управления контейнерами Docker.

Минимальные требования к аппаратной части:

- Процессор: не менее 2 ГГц, 4 ядра.
- Оперативная память: не менее 6 Гб.
- Дисковое пространство: не менее 150 Гб свободного дискового пространства.

Требования к программной части:

- Docker 20.10.22.
- Docker Compose 1.29.2.
- ОС, поддерживающие систему управления контейнерами Docker (Astra Linux, РЕД ОС, Ubuntu, Debian и т. д.).
- Система управления БД PostgreSQL версии 12, 13, 14.

1.4 Требования к персоналу, обеспечивающему функционирование Системы

Персонал, обеспечивающий функционирование **Системы,** должен обладать следующими навыками:

- базовые навыки администрирования ОС семейства Linux (настройка репозиториев, системные настройки и т. д.);
- базовые навыки работы с Docker, Docker Compose;
- базовые навыки работы с системой управления БД PostgreSQL.

2 АДМИНИСТРИРОВАНИЕ СИСТЕМЫ

2.1 Установка и обновление Системы

2.1.1 Установка Системы

Установка **Системы** описана в документе «Сканер Руководство по развертыванию».

2.1.2 Обновление Системы

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

```
# Предоставление прав доступа на запись
sudo chmod o+rw /opt/

# Перейти в папку /opt
cd /opt

# Запуск Системы
docker-compose up -d --build
```

2.2 Работа с контейнерами Системы

Для запуска **Системы** – открыть терминал и выполнить команды:

```
# Перейти в папку /opt
cd /opt

# Запуск Системы
docker-compose up -d --build
```

Управление запуском/остановкой/перезапуском **Системы** осуществляется с помощью команд:

```
# Управление Системой
docker-compose stop – остановка
docker-compose start – запуск
docker-compose down – удаление
docker-compose up -d – повторное создание (при отсутствии) и запуск контейнеров в фоновом режиме
docker-compose ps – проверка статуса запущенных контейнеров
```

2.3 Мониторинг и очистка лог-файлов Системы

В процессе работы **Системы** осуществляет логирование операций в части фиксации информации о запуске сканирования и его результатов в лог-файлы.

Хранение лог-файлов осуществляется в каталоге «/opt/logs» на сервере.

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

2.4 Первичная настройка Системы

Для начала работы **Системы** необходимо произвести ее первичную настройку. Первичная настройка **Системы** описана в п.2.2.2 документа «Сканер Руководство по развертыванию».

2.5 Диагностика неисправностей

При обнаружении ошибок в запуске сканирования сети, необходимо осуществить диагностику неисправностей в следующем порядке:

- осуществить проверку текущего состояния контейнеров Системы (п.2.2)
- осуществить анализ лог-файлов Системы на наличие ошибок (п.2.3).

При обнаружении ошибок, влияющих на работоспособность **Системы**, произвести устранение неисправностей и при необходимости осуществить перезапуск **Системы**.

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.

3 РАБОТА С СИСТЕМОЙ

В **Системе** реализовано два типа сканирования:

− обнаружение устройств, в рамках данного типа выполняется сбор информации по устройствам посредством технологии Nmap.

− инвентаризация, в рамках данного типа выполняется сбор информации по устройствам посредством технологии WinRM/WMI/SSH.

Работа с **Системой** осуществляется с помощью обращения к программным интерфейсам взаимодействия с Системой (REST API). Документация программных интерфейсов представлена в веб-консоли «Swagger UI» и доступна по адресу: http://<host>:<port>/swagger.

3.1 Запуск сканирования типа обнаружение устройств

Для запуска сканирования необходимо выполнить запрос:

```
curl -X 'POST' \
  'http://<host>:<port> /api/v1/app_discovery/' \
  -H 'authorization: Basic <base64(user:password)>' \
  -d '{
  "hosts": "1.1.1.1",
  "ports": "8080"
}'
```

Для просмотра информации по задачам необходимо выполнить запрос:

```
curl -X 'GET' \
  'http:// <host>:<port> /api/v1/tasks/' \
  -H 'authorization: Basic <base64(user:password)>' \
```

Для просмотра результатов задачи необходимо выполнить запрос:

```
curl -X 'GET' \
  'http:// <host>:<port> /api/v1/tasks/<task_id>' \
  -H 'authorization: Basic <base64(user:password)>' \
```

Запросы для получения подробной информации по сканированию приведены в веб-консоли «Swagger UI».

3.2 Запуск сканирования типа инвентаризация

Для запуска сканирования типа инвентаризация используется учетная запись для подключения к устройству:

− для устройств с ОС Windows необходимо создать пользователя с правами локального администратора;

- для устройств с ОС Linux необходимо создать пользователя, который обладает root-правами на выполнение следующих команд: hostname, arch, dmidecode, cat /etc/os-release, lsb_release -a, ifconfig -a, ip a, cat /etc/resolv.conf, ip route, lscpu, cat /proc/meminfo, df -TPk, rpm -qa, dpkg-query, last, cat /etc/passwd, cat /etc/group, service status-all, systemctl.

Для создания учетной записи в **Системе** необходимо выполнить запрос:

```
curl -X 'POST' \
  'http://<host>:<port> /api/v1/app_profiles/' \
  -H 'authorization: Basic <base64(user:password)>' \
  -d '{
  "name": " profile_windows",
  "description": "профиль для сканирования устройств на Windows",
  "provider": "windows",
  "domain": "example",
  "login": "test",
  "password": "Password"
}'
```

Для запуска сканирования необходимо выполнить запрос:

```
curl -X 'POST' \
  'http://<host>:<port> /api/v1/app_inventory/' \
  -H 'authorization: Basic <base64(user:password)>' \
  -d '{
  "object": "1.1.1.1",
  "windows_user_id": 1,
  "linux_user_id": 0,
  "cisco_asa_user_id": 0
}'
```

Для просмотра информации по задачам необходимо выполнить запрос:

```
curl -X 'GET' \
  'http:// <host>:<port> /api/v1/tasks/' \
  -H 'authorization: Basic <base64(user:password)>' \
```

Для просмотра результатов задачи необходимо выполнить запрос:

```
curl -X 'GET' \
  'http:// <host>:<port> /api/v1/tasks/<task_id>' \
  -H 'authorization: Basic <base64(user:password)>' \
```

Запросы по работе с учетными записями и другие запросы с подробной информации по сканированию приведены в веб-консоли «Swagger UI».

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

Сокращение	Полное наименование
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
Система	Система инвентаризации сетевых устройств Сканер