Программное обеспечение, выполняющее функции информационного справочника о территориальном распределении IP-адресов «Jet Geo IP»

Инструкция по скачиванию и установке дистрибутива

Содержание

Термины и сокращения

В документе используются термины и определения, приведенные в таблице 1.

Таблица 1 – Термины и определения

Термин	Описание
API	Программный интерфейс программы, представляющий собой набора программных функций, с помощью которых программа взаимодействует со смежными программами
ASN-данные	Информация об автономных системах: номер автономной системы; владелец IP-адресов автономной системы
ASN-файл	Файл, полученный в результате скачивания специальными программами ASN-данных из открытых интернет-источников
Docker	Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации, контейнеризатор приложений
GeoIP-данные	Информация о географическом местоположении IP-адресов сети Интернет, содержащих информацию: о стране и городе расположения IP-адреса; владельцах IP-адресов и др.
GeoIP-файл	Файл, полученный в результате скачивания специальными программами GeoIP-данных из открытых интернет-источников
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP. В версии протокола IPv4 IP-адрес имеет длину 4 байта, а в версии протокола IPv6 IP – 16 байт
Tor/Proxy-данные	Список IP-адресов, которые принадлежат: прокси-серверам или прокси-серверам, позволяющим устанавливать анонимное сетевое соединение с помощью специального программного обеспечения, называемого Tor (от англ. The Onion Router)
Tor/Proxy-файл	Файл, полученный в результате скачивания специальными программами Tor/Proxy-данных из открытых интернет-источников
БД	База данных
ГПИ	Графический пользовательский интерфейс
Доменное имя	Символьное имя. Служит для идентификации областей, которые являются единицами административной автономии в сети Интернет и входят в состав вышестоящей по иерархии области. Каждая такая область называется доменом. Общее пространство имен сети Интернет функционирует благодаря DNS-системе доменных имен. Доменные имена дают возможность адресации интернет-узлов и расположенным на них сетевым ресурсам (веб-сайтам, серверам электронной почты, другим службам) быть представленными в удобной для человека форме
Контролируемый ресурс	Информационный ресурс сети Интернет, находящийся под особым контролем. Программа использует информацию об IP-адресах, доменных именах и принадлежности организациям информационных ресурсов
ПО	Программное обеспечение

Термин	Описание
Скачиватель ASN	Программа, выполняющая скачивание ASN-данных из открытого интернет-источника, преобразование и загрузку полученных данных в ASN-файлы. Скачиватели GeoIP не входят в состав программы и разрабатываются отдельно
Скачиватель GeoIP	Программа, выполняющая скачивание GeoIP-данных из открытого интернет-источника, преобразование и загрузку полученных данных в GeoIP-файлы. Скачиватели GeoIP не входят в состав программы и разрабатываются отдельно
Скачиватель Tor/Proxy	Программное, выполняющая скачивание списка TOR/Proxy открытого Интернет-источника, преобразование и загрузку полученных данных в TOR/Proxy-файлы. Скачиватели Tor/Proxy не входят в состав программы и разрабатываются отдельно
Хост	Компьютер или сервер, подключённый к сегменту вычислительной сети

1 Общие сведения о программном обеспечении

Полное наименование: Программное обеспечение «Jet GeoIP».
Краткое наименование: GeoIp.

1.1 Назначение ПО

GeoIP предназначено для обеспечения следующих возможностей:

- формирование справочника о территориальном распределении IP-адресов сети Интернет и об их владельцах на основе данных интернет-источников (далее – GeoIP-данные);
- обогащение данных справочника признаками принадлежности IP-адресов к Tor и Proxy сетевым узлам на основе данных интернет-источников (далее – Tor/Proxy-данные);
- обогащение данных справочника признаками принадлежности IP-адресов и доменных имен контролируемым ресурсам (далее – контролируемые ресурсы);
- получение выписки по IP-адресу;
- ведение истории изменения:
- географического местоположения IP-адресов,
- владельцев IP-адресов;
- принадлежности IP-адресов и доменных имен к контролируемым ресурсам;
- принадлежности IP-адресов к Tor и Proxy узлам;
- предоставление данных справочника;
- формирование отчетности по хранящимся в GeoIP объектам и их характеристикам, отображение данных в графическом пользовательском интерфейсе;
- получение регистрационных сведений и abuse-контактов IP-адреса;
- получение сведений о доменных именах IP-адреса;
- получение репутационного показателя IP-адреса;
- получение и внесения комментариев к IP-адресу;
- массовый анализ IP-адресов;
- поиск организации по доменному имени.

1.2 Требования к аппаратному и программному обеспечению

Для работы необходимы:

1) Сервер БД: geoip_db:

- 20xCore 2,4GHZ 32GB RAM 2TB
- Ubuntu LTS;
- docker;
- docker-compose.

2) Сервер скачивателей: geoip_dl:

- 4xCore 2,4GHZ 16GB RAM 500GB
- Ubuntu LTS;
- docker;

- docker-compose.

3) Сервер приложения: geoip_app:

- 8xCore 2,4GHZ 32GB RAM 500GB
- Ubuntu LTS;
- docker;
- docker-compose.

2 Установка и настройка GeoIP

2.1 Загрузка дистрибутива

Для развертывания GeoIp необходимо воспользоваться бинарным файлом.

2.2 Настройка сервера БД

Настроить сервер БД с помощью документации на официальном сайте Postgres: https://www.postgresql.org/download/

2.3 Настройка сервера БД

1) Установить Docker по инструкции с официального сайта https://docs.docker.com/engine/install/.
2) Распаковать комплект поставки в папку /opt/geoip.
3) Перейти в каталог /opt/geoip.
4) Создать каталоги (если отсутствуют):
   - ./exchange/to_process/
   - ./exchange/success/
   - ./exchange/failed/
   - ./log/
   - ./reports/
5) Загрузить docker образы через команду docker load < app.tar.gz.
6) Исправить необходимые настройки в config.env файле.
7) Запустить систему через команду docker-compose up –d.

2.4 Настройка сервера скачивателя

1) Установить docker по инструкции с официального сайта https://docs.docker.com/engine/install/.
2) Распаковать комплект поставки в папку /opt/geoip.
3) Перейти в каталог /opt/geoip.
4) Создать каталоги(если отсутствуют):
5) ./exchange/processed/
6) Загрузить docker образы через команду docker load < downloader.tar.gz.
7) Запустить систему через команду docker-compose up -d.

2.5 Организация связи между серверами скачивателя и приложения

Для корректной работы программы rsync требуется наличие публичного ssh-ключа пользователя root на сервере скачивателя. Необходимо установить ключ на сервер скачивателя запустив команду ssh-copy-id <ipaddress сервера скачивателя>

Команда должна быть запущена с сервера приложения пользователем root.

2.6 Обновление программного обеспечения

Для обновления предполагается поставка исключительно докер образов.

Процедура обновления следующая:

1) Загрузить на сервер архив с новыми образами.
2) Загрузить докер образы через команду docker load < <тип набора образов>.tar.gz.
3) Перейти в папку /opt/geoip.
4) Запустить docker-compose up –d.

3 Проверка работоспособности и диагностика неисправностей

3.1 Сервер БД

Сервис postgres должен быть запущен и отвечать на стандартном порту. Лог сервера БД не должен содержать ошибки уровня error и выше.

3.2 Сервер приложения

Результат команды docker-compose ps должен показывать, что все контейнеры находятся в статусе UP. Логи контейнеров (docker-compose logs -f) не должны содержать ошибки уровня error и выше. Сервер приложения должен отвечать на 80м порту и показывать ГПИ приложения.

3.3 Сервер скачивателя

Результат команды docker-compose ps должен показывать, что все контейнеры находятся в статусе UP. Логи контейнеров (docker-compose logs -f) не должны содержать ошибки уровня error и выше.