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

Руководство администратора (системного программиста)

Содержание

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 Установка и настройка GeoIp

2.1.1 Настройка сервера БД

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

2.1.2 Настройка сервера БД

4) Установить Docker по инструкции с официального сайта https://docs.docker.com/engine/install/;
5) распаковать комлект поставки в папку /opt/geoip;
6) перейти в каталог /opt/geoip;
7) создать каталоги (если отсутствуют):
   - ./exchange/to_process/
   - ./exchange/success/
   - ./exchange/failed/
   - ./log/
   - ./reports/
8) загрузить docker образы через команду docker load < app.tar.gz;
9) исправить необходимые настройки в config.env файле;
10) запустить систему через команду docker-compose up –d.

2.1.3 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):
   - ./exchange/processed/
5) загрузить docker образы через команду docker load < downloader.tar.gz
6) запустить систему через команду docker-compose up -d

2.1.4 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.

2.1.5 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.

4 Резервное копирование

Единственное место где хранятся изменяемые данные – база данных Postgres, данному сервису рекомендуется уделить особое внимание.

Рекомендуется делать резервные копии базы данных в бинарном формате не менее раза в неделю и хранить не менее 3х копий БД.

Сервер приложений и сервер скачивателя рекомендуется архивировать с помощью системы виртуализации путем сохранения полного образа системы.

Данная операция оправдана в случаях:

- установки системы первый раз;
- установки обновлений;
- изменения конфигурационных файлов системы.

Периодическое создание резервных копий не считается обязательным.

5 Мониторинг работоспособности системы

Для бесперебойной работы системы необходимо проверять:

- наличие свободного места в ос на всех серверах;
- работу службы postgresql на сервере БД;
- работу всех контейнеров, указанных в docker-compose.yml файлах.

6 Список сокращений

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
Скачиватель ASN	Программа, выполняющая скачивание ASN-данных из открытого интернет-источника, преобразование и загрузку полученных данных в ASN-файлы.

Термин	Описание
	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