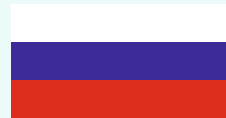
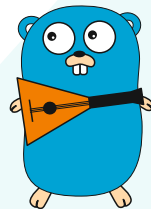



PowerC



Сделано в России
Не зависит от
сторонних библиотек

PowerSLAL

Статистика AnyConnect пользователей

Для оборудования 

Версия 3, со встроенным сервером Syslog

Cisco ASA

Настройки на Cisco ASA, пример (192.168.0.5 IP адрес сервера, где запущен контейнер)

```
logging list SSLUSERS2 level informational
logging list SSLUSERS2 message 605005
logging list SSLUSERS2 message 611103
logging list SSLUSERS2 message 113039
logging list SSLUSERS2 message 113019
logging list SSLUSERS2 message 722051
logging trap SSLUSERS2
logging host inside

event manager applet StartSession
event syslog id 722051 occurs 1
action 0 cli command "call-home send alert-group snapshot profile VPNSH"
output none
event manager applet EndSession
event syslog id 113019 occurs 1
action 0 cli command "call-home send alert-group snapshot profile VPNSH"
output none

service call-home

call-home
alert-group-config snapshot
add-command "show vpn-sessiondb anyconnect"
profile VPNSH
destination address http http://192.168.0.5:7002/vpnsession msg-format xml
```

Запуск сервисов

Установка (на докер сервер): **git clone https://github.com/OlegPowerC/anyconnectusersandsyslog.git**

Зайти в папку и запустить файл initdb.sh

cd anyconnectusersandsyslog

chmod 777 initdb.sh

./initdb.sh

Дождаться готовности PSQL сервера Не должно быть сообщений об ошибках и вывод должен быть примерно следующий:

```
server started
/usr/local/bin/docker-entrypoint.sh: sourcing /docker-entrypoint-initdb.d/1_createdb.sh
CREATE ROLE
CREATE DATABASE GRANT
/usr/local/bin/docker-entrypoint.sh: sourcing /docker-entrypoint-initdb.d/2_createtabledb.sh
CREATE TABLE
CREATE TABLE
```

PostgreSQL init process complete;
ready for start up

LOG: database system is ready to accept connections

После этого остановить запущенный контейнер - ctrl+c

Затем можно запускать все контейнеры командой: **docker-compose up -d**

По умолчанию интерфейс AnyConnect статистики доступен по пдресу:

HTTP://<ваш docker сервер>:8182

а syslog по адресу

HTTP://<ваш docker сервер>:8181

Порты:

SQL порт TCP снаружи 5442 (можно выключить)

Порт TCP 7002 слушает Call-Home сообщения от Cisco ASA

Для геолокации по IP адресу используется сервис

<https://ipstack.com/> Необходимо получить API ключ и указать его в файле **docker-compose.yml** (параметер **GEOLOCATIONAPIKEY:**)

Больше информации

Россия, Санкт-Петербург
Таллинская 6-В
Телефон: +7 (812) 7034338
<http://www.powerc.ru>
<http://www.ciscolive.ru>

info@powerc.ru

