Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 2, 842 16, Bratislava 4

Inštalačná príručka

Dokumentácia k tímovému projektu

Tímový projekt

Tím č. 21

Vedúci: Ing. Ivan Srba, PhD.

Členovia tímu:
Matej Groma
Matej Horváth
Peter Jurkáček
Jozef Kamenský
Adam Kňaze
Kristína Macková
Lenka Pejchalová
Jakub Sedlář

tim21.2018.fiit@gmail.com

Akademický rok: 2018/2019

Posledná zmena: 14. decembra 2018

Obsah

1 Úvod

Tento dokument obsahuje postupy využívané v tíme Traffic Watch v rámci predmetu Tímový projekt týkajúce sa konfigurovania a inštalácie podporných prostriedkov a samotnej aplikácie. V nasledujúcich kapitolách sa detailne venuje jednotlivým postupom, od pomocných určených prevažne na interné použitie v rámci tímu po postupy, ktoré je potrebné aplikovať na kompletné sprevádzkovanie systému.

2 Nasadenie serverovej časti systému (BE+FE)

Najskôr naklonujeme repozitár deployment, ktorý zastrešuje záležitosti týkajúce sa nasadzovania. Presunieme sa do priečinku backend_and_frontend, v ktorom sa nachádzajú skripty pre nasadenie backendu a frontendu aplikácie na server.

V súbore hosts pod [servers] nakonfigurujeme FQDN servera, na ktorý chceme aplikáciu nasadiť. Parametrom ansible_user špecifikujeme meno používateľa, prostredníctvom ktorého sa na server pripájame (root alebo používateľ so sudo oprávneniami). Pod [servers:vars] môžeme upraviť niektoré konfiguračné parametre servera (napr. porty, na ktorých BE/FE bežia). Pod [all:vars] upravujeme nastavenia, ktoré sa aplikujú lokálne (ako cesta k repozitáru, alebo vetva ktorú nasadiť). Následne skopírujeme súbor host_vars/example.com do host_vars/FQDN a definujeme používateľské mená a heslá ktoré chceme použiť pre MQTT (kvôli citlivosti obsahu takéto súbory nie sú verziované).

Nasadenie spustíme cez ./play.sh (stiahne podporné roly a vykoná samotný playbook). Po vykonaní aplikácia beží na serveri bez potreby ďalšieho manuálneho zásahu. Predvolene aplikácia beží s využitím https na portoch 8123 (backend) a 8124 (frontend).

Menej závažným problémom bolo, že Java využíva vlastný systém na infraštruktúru verejného kľúča – v prípade jeho využitia by bolo potrebné zakaždým prekonvertovať používaný certifikát do java keystore, navyše výmena certifikátu počas behu aplikácie nie je podporovaná (potrebné kvôli renewals). Z tohto dôvodu je backend zabezpečený pomocou reverzného proxy využitím web servera nginx.