Követelményspecifikáció

Teljesen elosztott rendszer elkészítése nagy méretű felvonórendszer központi monitorozására és irányítására

Szoftverarchitektúrák tárgy házi feladat

Feladatkiírás

A feladat egy teljesen elosztott rendszer elkészítése, mely lehetővé teszi egy nagy méretű felvonórendszer központi monitorozását és irányítását.

- Egy központi adminisztrációs felületről lehessen követni a felvonók állapotát, terheltségét, várható sorbanállási időt, szélerősséget stb.
- A felvonóknak jelezniük kell az általuk észlelt hibákat, vészhelyzeteket a központi komponens felé.
- A központból lehessen utasításokat küldeni a felvonók operátorai felé (lift indítás, leállítás stb.) A központ folyamatosan monitorozza a felvonókat működtető komponenseket és hiba esetén jelezze ezt az operátorok felé.
- Vészhelyzet esetén lehessen megbízhatóan leállítani egy felvonót a központi felületről.
- Egy külön komponens jelenítse meg a nagyközönség számára a felvonók egyszerűsített állapotát térképen.
- A rendszer komponensei elosztott módon kerüljenek megvalósításra.
- A rendszer kritikus részei redundánsan legyenek megvalósítva.
- A komponensek kommunikációja legyen megbízható módon megvalósítva.
- A liftek terheltségének változása egy egyszerű sorbanállásos modellel legyen közelítve.

Részletes feladatleírás

A projekt során a célunk egy olyan alkalmazás fejlesztése, amely képes egy síparadicsomban (vagy akár bármely más helyen, ahol használnak felvonókat) működő felvonók monitorozására, és irányítására. Az alkalmazás elosztott módon lesz implementálva, azaz az egyes komponensek külön alkalmazásként is működnek, így lehetőség nyílik az alkalmazás több gépen való futtatására és skálázására. A rendszer központi komponensének állapotát egy bizonyos intervallumonként lementjük, és bármilyen okból az meghibásodna, akkor azt a Kubernetes klaszter azonnal újraindítja, és a legutolsó mentéstől indul újra a működés. Az alkalmazás központi komponense mellett minden felvonóhoz tartoznak majd Worker komponensek, amelyek az egyes felvonók monitorozását, és irányítását is végzik. Az egyes síliftek jelenlegi állapotát minden állapotváltozásnál lementjük, legyen az a központ által kért állapotváltozás vagy a Worker operátor által kiadott parancs, ezzel biztosítva azt, hogy ne történjen inkonzisztencia a központi elem leállása esetén.

A felvonók jelzik az általuk észlelt hibákat, vészhelyzeteket a központi komponens felé. A központ is folyamatosan monitorozza a felvonókat működtető komponenseket és hiba esetén jelzi ezt az operátorok felé. (Például kiugró vagy hibás értékek)

A síliftek a következő adatokat küldik magukról:

- Jelenlegi állapot (FULL STEAM, HALF STEAM vagy STOP)
- Terheltség [db ember]
- Várható sorbanállási idő
- Szélerősség (kezdőpont és végpont)
- Hőmérséklet (kezdőpont és végpont)

A központból javaslatokat/figyelmeztetéseket lehet küldeni a felvonók felé (FULL STEAM, HALF STEAM vagy STOP). Ekkor a felvonónál lévő operátor dönt, hogy jogos-e a központ által adott parancs, és ha nem ért egyet felülírhatja. (2 szintű döntéshozatal/Failsafe) Vészhelyzet esetén a központ közvetlenül is küldhet egy emergency stop parancsot a felvonónak, amit a sílift operátora nem tud felülbírálni. Az emergency stop parancs kiadásához egy külön gomb áll rendelkezésére a központnak, aminek megnyomása után, meg is kell erősíteni a megállítási szándékot.

A Master és Worker komponensekbe egyaránt csak autentikáció után lehet belépni. Lehetőség lesz a központi komponens hétköznapi felhasználó szintű elérésére is, amelynek során a felhasználó egy olyan nézetet lát, amin keresztül tájékozódhat a liftek elhelyezkedéséről, és terheltségéről. Itt látja majd a síterep térképét, az egyes felvonókat jól láthatóan kiemelve rajta, és a várható sorbanállási időt minden egyes felvonónál, mindezt egy felhasználóbarát felületen. Ebben a nézetben természetesen nincs lehetőség parancsok kiadására a liftek felé.

A komponensek UID segítségével azonosítják egymást, amit a földrajzi koordinátáikból (kezdőpont és végpont) generálunk, és a Master csak beregisztrált komponensektől fogad el

üzeneteket. A komponensek közötti kommunikációt AMQP protokoll segítségével valósítjuk meg, ami garantálja a FIFO sorrendiséget az egyes liftenként küldött üzeneteken belül, illetve minden üzenetet titkosítva küldünk át. A liftek terheltségének változása egy M/M/c Queue (Erlang-C) modellel lesz közelítve. Mivel a jelenlegi megoldással a RabbitMQ queue könnyen válhat "single point of failure"-é, különös prioritást kap majd a redundanciában. A megbízhatóság és hibatűrés érdekében kulcsfontosságú a RabbitMQ megfelelő klaszterkonfigurációja, a magas rendelkezésre állás biztosítása, és az üzenetek perzisztenciája.

Technikai paraméterek

Az alkalmazás fő komponense három rétegű architektúrát követ a következő képpen. Az felvonók működtetéséhez szükséges adatokat egy Postgres adatbázisban tároljuk. Az adatbázishoz szükséges adatelérési réteg Django keretrendszerben kerül megvalósításra. Az egyszerű és felhasználóbarát kezelés érdekében az alkalmazáshoz készül egy felhasználói interfész is Angular technológiával. A felhasználó autentikációra Keycloak-ot használunk. Az egyes felvonókat külön-külön működtető komponensek ettől eltérő módon kerülnek megvalósításra. Ezen kisebb felvonó komponensek mind Pythonban kerülnek megírásra. Maga a síparadicsom modellje egy lokális Kubernetes klaszterben fog elkészülni. Ezen belül a különböző komponensek Docker konténerek formájában fognak elhelyezkedni, amihez Minikube-ot használunk. A komponensek közti megfelelő kommunikációért a RabbitMQ nyílt forráskódú szoftver felel. Tekintettel arra, hogy a Kubernetes control pane egysége csak Linuxon tud futni, így az alkalmazás működését csak ezen a platformon tudjuk garantálni.

Szótár

Felvonó/sílift: A sípályán található berendezés, amely a síelőket a hegy aljától a tetejéig szállítja. A rendszerben ez egy önálló egység, amely adatokat küld és utasításokat fogad. Egy kiinduló és egy érkezési pont földrajzi koordinátáival lehet inicializálni.

Felvonó állapota: A felvonó aktuális működési módja, amely lehet:

- FULL STEAM: Teljes sebességű üzemelés
- HALF STEAM: Csökkentett sebességű üzemelés
- STOP: Leállított állapot

Felvonó terheltsége: Az aktuálisan a felvonót használó síelők száma vagy aránya. Ez az adat folyamatosan frissül és továbbításra kerül a központi rendszer felé.

Sorbanállási idő: A becsült várakozási idő a felvonó használatához. Ezt a rendszer számolja ki az M/M/c Queue (Erlang-C) modell segítségével, figyelembe véve a jelenlegi terhelést és egyéb tényezőket.

Vészhelyzet: Olyan kritikus helyzet, amelyet a felvonó vagy a központi operátor észlel. Ilyen lehet például műszaki hiba vagy biztonsági kockázat.

Központi komponens: A rendszer fő irányító egysége, amely összegyűjti az adatokat minden felvonótól, feldolgozza azokat, és utasításokat küldhet vissza. Állapotát rendszeresen lementjük.

Worker operátor (Worker Operator): A felvonónál tartózkodó kezelő, aki közvetlenül felügyeli a felvonó működését. Jogosultsága van felülbírálni a központból érkező utasításokat, kivéve, ha az egy “Emergency Stop” típusú parancs.

Master operátor (Master Operator): A központi komponenst kezelő operátor, aki teljes hozzáféréssel rendelkezik a rendszerhez és utasításokat adhat ki a felvonók felé.

Hétköznapi felhasználó (Public User): Olyan felhasználó, aki csak korlátozott hozzáféréssel rendelkezik a rendszerhez. Láthatja a liftek elhelyezkedését és terheltségét, de nem adhat ki parancsokat, és egyes monitorozott adatokat is elrejtünk előle.

Kubernetes klaszter: Konténer-orkesztrációs rendszer, amely a központi komponens és más rendszerelemek futtatását, skálázását és újraindítását végzi.

AMQP protokoll: Advanced Message Queuing Protocol, amelyet a rendszer a komponensek közötti biztonságos és megbízható kommunikációra használ. Garantálja a FIFO sorrendet és az üzenetek titkosítását.

M/M/c Queue modell: Sorbanállási elmélet modell, amelyet a rendszer a felvonók terheltségének és várakozási idejének becslésére használ.

Szélerősség és hőmérséklet: A felvonókon elhelyezett műszerek által mért és jelentett környezeti adatok, amelyeket a kezdő- és végpontnál egyaránt rögzítenek és továbbítanak a központi rendszer felé.

Use-case diagram