SVEUČILIŠTE U SPLITU

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

DIPLOMSKI RAD

IZRADA SKALABILNE CHAT APLIKACIJE KOJA SE IZVRŠAVA NA KUBERNETES SUSTAVU

Ivo Kovačević

Split, rujan 2020.

SVEUČILIŠTE U SPLITU

FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE

Diplomski studij: **FESB**

Smjer/Usmjerenje: **Računarstvo**

Oznaka programa: 250

Akademska godina: 2019./2020.

Ime i prezime: **IVO KOVAČEVIĆ**

Broj indeksa: 744-2018

**ZADATAK DIPLOMSKOG RADA**

Naslov: **IZRADA SKALABILNE CHAT APLIKACIJE KOJA SE IZVRŠAVA NA KUBERNETES SUSTAVU**

Zadatak: Izučiti principe dizajna i izrade skalabilnih web aplikacija. Izučiti način korištenja Kubernetes sustava kao i prednosti koje donosi u rada sa skalabilnim aplikacijama. Izradom chat aplikacije demonstrirati način i prednosti korištenja Kubernetes sustava.

Prijava rada: 05.10.2020. (početak semestra u kojem se prijavljuje rad)

Rok za predaju rada: 05.02.2020. (deset dana prije završetka semestra u kojem je rad prijavljen)

Rad predan:

Predsjednik   
Odbora za diplomski rad: Mentor:

prof. dr. sc. Ime Prezime izv. prof. dr. sc. Marin Bugarić

**IZJAVA**

Ovom izjavom potvrđujem da sam završni rad s naslovom (Izrada skalabilne chat aplikacije koja se izvršava na Kubernetes sustavu) pod mentorstvom (prof. dr. sc. Marin Bugarić) pisao samostalno, primijenivši znanja i vještine stečene tijekom studiranja na Fakultetu elektrotehnike, strojarstva i brodogradnje, kao i metodologiju znanstveno-istraživačkog rada, te uz korištenje literature koja je navedena u radu. Spoznaje, stavove, zaključke, teorije i zakonitosti drugih autora koje sam izravno ili parafrazirajući naveo/la u završnom radu citirao/la sam i povezao/la s korištenim bibliografskim jedinicama.

Student

Ivo Kovačević

**SADRŽAJ**

[1 UVOD 1](#_Toc42186118)

[2 MOTIVACIJA ZA UVOĐENJE KUBERNETES SUSTAVA 2](#_Toc42186119)

[2.1 Prelazak na mikro-servis arhitekturu 2](#_Toc42186120)

[2.2 Uvod u container tehnologiju 4](#_Toc42186121)

[2.3 Potreba za Kubernetes sustavom 6](#_Toc42186122)

[3 UVOD U KUBERNETES SUSTAV 7](#_Toc42186123)

[3.1 Pojednostavljeni prikaz rada Kubernetes sustava 7](#_Toc42186124)

[3.2 Arhitektura Kubernetes sustava 7](#_Toc42186125)

[3.3 Izvršavanje aplikacije na Kubernetes klasteru 9](#_Toc42186126)

[3.4 Prednosti korištenja Kubernetes sustava 10](#_Toc42186127)

[4 PRVA APLIKACIJA NA KUBERNETES SUSTAVU 12](#_Toc42186128)

[5 TEMELJNI POJMOVI KUBERNETES SUSTAVA 19](#_Toc42186129)

[5.1 Pods 19](#_Toc42186130)

[5.1.1 Oznake Pod-ova 21](#_Toc42186131)

[5.1.2 Objava Pod opisa kroz yaml datoteku 22](#_Toc42186132)

[5.2 Deployments 23](#_Toc42186133)

[5.2.1 Kontrole ispravnosti Pod-a 24](#_Toc42186134)

[5.2.2 Objava Deployment opisa i demonstracija automatske zamjene neispravnih Pod-ova 25](#_Toc42186135)

[5.3 Services 27](#_Toc42186136)

[5.3.1 Vrste servisa 30](#_Toc42186137)

[5.4 Volumes 33](#_Toc42186138)

[5.5 ConfigMaps i Secrets 33](#_Toc42186139)

[6 AUTOMATSKO SKALIRANJE 34](#_Toc42186140)

[7 CHAT APLIKACIJA 35](#_Toc42186141)

[8 ZAKLJUČAK 36](#_Toc42186142)

[LITERATURA 37](#_Toc42186143)

[POPIS OZNAKA I KRATICA 38](#_Toc42186144)

[SAŽETAK 39](#_Toc42186145)

# UVOD

Novi trend razvijanja aplikacija su svakako mikro-servisi. Mikro-servis arhitektura se uveliko razlikuje od tradicionalnog razvoja aplikacija gdje je cijela aplikacija „zapakirana“ kao jedna velika cjelina. Takve aplikacije nazivaju se monolitne aplikacije.

Monolitan razvoj je i dalje vrlo raširen iako ima mnogo nedostataka. Samim tim što je aplikacija jedna velika cjelina gdje su svi „servisi“ strogo povezani, jako je teško nadograđivati i mijenjati aplikaciju pa su nove verzije aplikacija vrlo rijetke. Nakon što se takve aplikacije naprave, programeri aplikaciju proslijede Ops timu. Ops tim potom aplikaciju ručno migrira na „zdravi“ (engl. healthy) server. Ukoliko dođe do prekida rada servera, aplikaciju je potrebno opet ručno migrirati na drugi „zdravi“ server.

Mikro-servis arhitektura je skup više nezavisnih, samostalnih, odvojenih servisa. Svaki servis se razvija zasebno, najčešće od strane manjeg tima unutar organizacije te se potom migrira (engl. deploy) i održava neovisno o ostalim servisima. Ovakva arhitektura donosi mnoge prednosti u odnosu na tradicionalni razvoj. Glavna prednost je svakako mogućnost učestalijeg mijenjanja pojedinih komponenti ovisno o poslovnim zahtjevima.

Kod velikih aplikacija mikro-servis arhitektura može rezultirati velikim brojem zasebnih servisa. Kod kompanija kao što su Amazon i Netflix taj broj prelazi nekoliko tisuća. Upravljati s nekoliko tisuća zasebnih mikro-servisa bi svakako bilo nemoguće da ne postoje alati koji nam olakšavaju i omogućavaju taj posao. Jedan od tih alata je i Kubernetes sustav koji će biti objašnjen u okviru ovog diplomskog rada. Rad će biti fokusiran na Kubernetes sustavu u oblaku (engl. cloud) radije nego na Kubernetes sustavu koji se nalazi na vlastitom klasteru s ograničenim hardverom.

# MOTIVACIJA ZA UVOĐENJE KUBERNETES SUSTAVA

## Prelazak na mikro-servis arhitekturu

Monolitne aplikacije sastoje se od više strogo povezanih aplikacija ili servisa koji se razvijaju, migriraju i održavaju kao cjelina. Takva aplikacija je u biti jedan proces koji se vrti unutar servera. Za svaku i najmanju promjenu neke od komponenti, cijela aplikacija se treba iznova migrirat na server (engl. redeploy).   
Ovakva arhitektura predstavlja ograničenje u skaliranju aplikacije pri promjeni opterećenja. Postoje dva tipa skaliranja: vertikalno i horizontalno skaliranje. Vertikalno skaliranje podrazumijeva nadogradnju servera dodavanjem procesorske snage, memorije, povećanje frekvencije procesora itd. Horizontalno skaliranje odnosi se na dodavanje više servera koji su najčešće slabijih performansi nego kod vertikalnog skaliranja, ali je ključ u njihovom broju. Ti serveri posjeduju istu instancu aplikacije te se opterećenje raspoređuje između servera. Ukoliko je neki server u velikom opterećenju novi zahtjevi će se prebaciti na drugi, manje opterećen server.   
Monolitne aplikacije vrlo se lako vertikalno skaliraju. Zamislimo scenarij da posjedujemo Internet trgovinu koja prodaje kreme za sunčanje. Lako je zaključiti da će u periodu od jeseni do proljeća posjećenost naše Internet trgovine biti vrlo mala. Za takvo opterećenje će vrlo vjerojatno biti dovoljni prosječni serveri. Pri dolasku sunčanijih ljetnih mjeseci, za očekivati je da će posjećenost naše stranice naglo porasti. Moguć je scenariji da naš prosječni server neće biti u mogućnosti podnijeti nagli porast opterećenja. Jedno od rješenja bi bilo vertikalno skalirati našu aplikaciju dodavanjem procesorske snage i memorije. Ukoliko se radi o manjoj Internet trgovini ovo će vrlo vjerojatno riješiti problem. U ovoj priči radi se o velikoj Internet trgovini koja drži monopol prodaje krema za sunčanje u cijelom svijetu. Može se pomisliti: „Pa zašto ne bismo dodali još, još i još procesorske snage i memorije?“. Naime, vertikalno skaliranje ima svoja ograničenja. Glavno ograničenje svakako bi bila cijena. Snažni i moćni hardver je vrlo skup. Drugo ograničenje je proizvodnja i dostupnost hardvera na tržištu. Iako danas na tržište vrlo brzo izlaze nove i bolje verzije hardvera opet ćemo doći do točke gdje više nećemo moći dobiti bolji server nego što ga imamo. Kao ograničenje svakako treba izdvojiti i rizik prestanka rada servera. Ukoliko imamo samo jedan server, prestankom rada tog servera usluga koju pružamo će biti nedostupna. Može se naslutiti da smo dosegli vrhunac vertikalnog skaliranja i da moramo pronaći neko drugo rješenje. To bi bilo horizontalno skaliranje. Međutim, monolitne aplikacije je najčešće vrlo teško horizontalno skalirati jer su komponente strogo povezane. Ukoliko samo jedan dio monolitne aplikacije nije skalabilan, cijela aplikacije će biti neskalabilna. Uvjet za horizontalno skaliranje je neovisnost komponenti. Da bi ispunili taj preduvjet monolitnu aplikaciju moramo „razbiti“ na više neovisnih servisa gdje svaki servis predstavlja jedan nezavisni proces (Slika 2.1). Procesi mogu međusobno komunicirati. Komunikacija među procesima može se ostvariti velikim brojem protokola koji nisu strogo vezani za određeni programski jezik nego su implementirani gotovo u svakom programskom jeziku. To su HTTP, TCP, AMQP itd.

A screenshot of a cell phone

Description automatically generated

Slika 2.1 Prelazak s tradicionalnog razvoja na mikro-servis arhitekturu

Budući da je svaki mikro-servis neovisni proces, moguće ih je migrirati, razvijati i održavati neovisno o drugim mikro-servisima. Promjena na jednom mikro-servisu ne uzrokuje „redeploy“ ostalih mikro-servisa. Posljedično tome, kao rezultat dobijemo mogućnost skaliranja svakog mikro-servisa zasebno, neovisno o drugim mikro-servisima (Slika 2.2). Na taj način možemo skalirati samo one mikro-servise koji zahtijevaju više resursa, a ne cijelu aplikaciju.

A close up of a logo

Description automatically generated

Slika 2.2 Svaki mikro-servis može biti skaliran zasebno

## Uvod u container tehnologiju

Kod migracije aplikacija na server, može se dogoditi da različite aplikacije koriste različite verzije biblioteka. Kako je već rečeno, kod mikro-servis arhitekture, najčešće se razvoj aplikacije radi unutar manjih timova od kojih svaki tim razvija jedan zasebni servis. To također može rezultirati korištenjem različitih verzija biblioteka između timova što će rezultirati brojnim problemima kod migracije na isti server.   
Kako bi se riješio spomenuti problem, pribjegava se korištenju virtualizacijskih tehnologija kao što su virtualne mašine i „container“ tehnologije. Virtualizacijom se postiže neovisne, izolirane okoline pogodne za izvršavanje aplikacija. Kod aplikacija koje se sastoje od manjeg broja komponenti, moguće je svaku komponentu izolirati unutar vlastite virtualne mašine (VM). Svaka VM ima svoj operacijski sustav (OS). Kada se broj ovakvih komponenti počne povećavati, dodjeljivanjem VM svakoj komponenti predstavlja veliki gubitak hardverskih resursa iz razloga što VM imaju veliki „overhead“ budući da se unutar svake VM izvršava vlastiti OS. Osim hardverskih resursa, upravljanje (engl. manage) VM odvija se zasebno što predstavlja i veliki trošak ljudskih resursa.  
Umjesto korištenje virtualnih mašina za osiguravanje izolirane cjeline za svaki mikro-servis koristi se Linux „container“ tehnologija. Container tehnologija ima znatno manji „overhead“ od virtualnih mašina jer se izvršavaju na operacijskom sustavu domaćina (engl. host) umjesto da svaki container ima vlastiti OS unutar kojeg se izvršava proces. Proces unutar containera je također izoliran kao i kod VM. Korištenje container tehnologije naspram VM rezultira većim brojem aplikacija koje je moguće smjestiti na jedan server.

Na slici (Slika 2.3) vidimo spomenute razlike dvaju tehnologija. Uočavamo da svaka VM ima svoj vlastiti OS koji je na slici označen kao „Guest OS“ dok se aplikacije kod container tehnologije izvršavaju na OS hosta označenog kao „Host OS“. To je ujedno i glavna prednost VM u odnosu na container tehnologiju jer se postiže potpuna izoliranost što rezultira i većom sigurnošću.

A screenshot of a cell phone

Description automatically generated

Slika 2.3 Usporedba VM i container tehnologije [1]

Najpopularnija container tehnologija je svakako Docker. Docker omogućava „pakiranje“ aplikacija, zavisnih biblioteka, pa čak i cijelog OS datotečnog sustava unutar jednog, jednostavnog paketa koji se lako prenosi na druge mašine. Kada se takav paket prenese na drugu mašinu, on vidi identični datotečni sustav kao i kada je zapakiran. To omogućava rad aplikacije čak i na kompletno različitom operacijskom sustavu od onoga na kojem je aplikacija razvijana. Na primjer, ukoliko razvijamo našu aplikaciju na Ubuntu Linux distribuciji, a server na kojem ćemo migrirati aplikaciju posjeduje Debian distribuciju, Docker tehnologija omogućava da zapakirani Docker container i dalje vjeruje kako se izvršava u Ubuntu. Jedini uvjet je da sve mašine između kojih se razmjenjuju Docker containeri imaju instaliran Docker.

## Potreba za Kubernetes sustavom

Iako je monolitni razvoj puno brži, dugoročno gledano, svakako se isplati uložiti vrijeme u mikro-servis arhitekturu. Velika većina startup-ova u početku razvoja krene sa monolitnim pristupom te vrlo brzo naiđe na ograničenja. Mnoge velike kompanije su shvatile niz prednosti mikro-servis arhitekture te se odlučile prebaciti na istu. Arhitektura kompanija kao što su Amazon i Netflix se sastoji od nekoliko tisuća mikro-servisa koji međusobno komuniciraju (Slika 2.1). Gotovo nemoguće je upravljati s nekoliko tisuća mikro-servisa koji komuniciraju i zajedno obavljaju neki složeniji posao. Uzročno tome, došlo je do potrebe za sustavom koji će olakšati razvoj aplikacije temeljene na mikro-servis arhitekturi.

A close up of a logo

Description automatically generated

Slika 2.4 Mikro-servis arhitektura Amazon-a i Netflix-a [2]

Google kompanija je prva uvidjela ovaj problem te se odlučila na razvoj vlastitog, besplatnog i svima dostupnog rješenja koji su nazvali Kubernetes. Kubernetes je programsko rješenje koje omogućava jednostavno raspoređivanje i upravljanje container aplikacijama [3]. Zbog toga što su containeri izolirane cjeline, ne mogu utjecati na rad drugih aplikacija na istom serveru. To je vrlo važno svojstvo iz razloga što Cloud kompanije nastoje što bolje iskoristiti resurse, stavljajući različite aplikacije na isti server. Upravo na tom svojstvu se temelji i Kubernetes sustav. Migracija aplikacije na server kod Kubernetes sustava je vrlo jednostavna. Postupak je uvijek isti i ne razlikuje se o broju čvorova u klasteru. Dakle, isto je da li klaster ima jedan čvor ili 100 čvorova, što je uveliko doprinijelo prihvaćanju Kubernetes softvera i masivnom korištenju istog.

# UVOD U KUBERNETES SUSTAV

## Pojednostavljeni prikaz rada Kubernetes sustava

Najveći nivo apstrakcije Kubernetes sustava izgleda kao na slici (Slika 3.1). Sustav se sastoji od glavnog čvora (Kubernetes master) i radnih čvorova. Broj radnih čvorova nije ni na koji način ograničen. Može se kretati od samo jednog čvora pa do preko tisuću radnih čvorova, ovisno o potrebi. Developer pri migraciji aplikacije na server specificira koliko instanci pojedine komponente aplikacije želi, sve ostalo je zadaća Kubernetes sustava. Kubernetes potom, na osnovu specificiranih zahtjeva, komponente aplikacije migrira na klaster radnih čvorova. Nebitno je na koji će radni čvor Kubernetes smjestiti komponentu aplikacije. Bitno je samo da su ispunjeni uvjeti koje je developer specificirao. Kubernetes sustav će samostalno zaključiti koji je radni čvor najpogodniji za izvršavanje pojedine komponente. Također, developer može naznačiti ukoliko je potrebno da se neke komponente nalaze na istom čvoru te će sukladno tome Kubernetes navedene komponente rasporediti na isti radni čvor. Ukoliko nije posebno naglašeno, Kubernetes će imati potpunu slobodu rasporeda komponenti na dostupne radne čvorove. Komponente će i dalje moći međusobno komunicirati iako se nalaze nasumično raspoređene na klasteru radnih čvorova.

A picture containing drawing

Description automatically generated

Slika 3.1 Proces „deploy-a“ na Kubernetes cluster

## Arhitektura Kubernetes sustava

Arhitektura kubernetes sustava se sastoji od puno čvorova (engl. nodes). Dva su glavna tipa čvorova:

1. Master čvor – sadrži Kubernetes upravljačku ploču koja upravlja cijelim sustavom.
2. Radni čvorovi – čvorovi na kojima se izvršava aplikacija koju „deploy-amo“.

A screenshot of a cell phone

Description automatically generated

Slika 3.2 Arhitektura Kubernetes sustava - glavni čvor i radni čvorovi [4]

Master čvor sastoji se od sljedećih komponenti:

* API server – korisnici (developeri, sistem administratori i drugi…) upravljaju Kubernetes klasterom komunicirajući s API serverom. U prethodnom poglavlju (Slika 3.1) prikazano je da korisnik opis zahtjeva aplikacije šalje master čvoru. Komunikacija između korisnika i master čvora se odvija upravo preko API servera.
* Kontroler (engl. Controller manager) – kontrolira cjelokupni klaster. Zadužen je za replikaciju komponenti, praćenje radnih čvorova, poduzima radnje u slučaju prestanka rada pojedinih čvorova i slično.
* Raspoređivač (engl. Scheduler) – Zadužen je za raspoređivanje komponenti aplikacije na radne čvorove kako bi resursi bili što bolje iskorišteni i kako bi bili zadovoljeni svi specificirani zahtjevi.
* etcd – pouzdana baza podataka koja sprema konfiguraciju i stanje klastera.

Radni čvor sastoji se od sljedećih komponenti:

* Kubelet – komunicira s API serverom i upravlja komponentama radnog čvora na kojem se nalazi.
* Kube-Proxy – zadužen je za optimalni raspored opterećenja između radnih čvorova.
* Docker – zadužen za dohvaćanje „container image-a“ i pokretanje container-a.

## Izvršavanje aplikacije na Kubernetes klasteru

Nakon što smo objasnili arhitekturu Kubernetes sustava, možemo detaljnije objasniti proces migriranja i izvršavanja aplikacije na Kubernetes klasteru nego što li je to objašnjeno u poglavlju 3.1.   
Prvi korak migriranja aplikacije na Kubernetes kluster (u nastavku „deploy“) je „pakiranje“ aplikacije u jednu ili više „container“ slika (engl. container images). Te se slike potom objave na registru slika (engl. image registry). Zatim developer objavi opis aplikacije na Kubernetes API server (Slika 3.1). U opisu aplikacije specificirano je koliko treba biti replika pojedine komponente, koje komponente se moraju nalaziti na istom radnom čvoru (ukoliko ima takvih komponenti), od koje container slike će nastati pojedina komponenta itd.   
API server obradi zahtjev te posao preuzima Raspoređivač (engl. Scheduler). Raspoređivač raspoređuje containere na slobodne radne čvorove uzimajući u obzir opterećenje radnog čvora, zahtijevane resurse pojedinog containera i sl. Nakon što Raspoređivač rasporedi gdje će ići koji container, Kubelet radnog čvora na kojem je container smješten naredi Dockeru da preuzme container sliku s registra slika te pokrene container na osnovu preuzete slike. Na slici (Slika 3.2) ostao je neobjašnjen termin „Pod“. Pod sadrži jedan ili više pokrenutih slika – containera. Pod će detaljno biti objašnjen u nadolazećim poglavljima.

Nakon što je aplikacija uspješno pokrenuta, Kubernetes sustav će i dalje kontinuirano nadgledati rad naše aplikacije vodeći računa da je broj svakog containera jednak broju kojeg je developer specificirao u opisu aplikacije. Ukoliko neki od containera prestane s radom Kubernetes će automatski restartirati problematični container. Slično tome, ukoliko neki od radnih čvorova prestane s radom, Kubernetes će odabrati drugi radni čvor pogodan za premještanje svih containera koji se nalaze na problematičnom radnom čvoru.

Svaka aplikacija ima periode kada posjećenost raste ili pada. Na već spomenutom primjeru Internet stranice krema za sunčanje, porast prometa će biti u ljetnim mjesecima, dok će u zimskom periodu promet biti vrlo mali. Koristeći Kubernetes sustav, ne moramo se brinuti da će dolaskom ljetnih mjeseci, naša aplikacija prestati s radom zbog velike posjećenosti. Isto tako, u zimskim mjesecima će Kubernetes sustav zaključiti kako imamo previše resursa nego što nam u tom trenutku treba te će automatski skalirati aplikaciju da ne trebamo plaćati dodatne, nepotrebne resurse. Na taj način ćemo uštedjeti novac, a isto tako osigurati da aplikacija radi i u periodima nagle velike posjećenosti. Kada potreba za pojedinim servisom pređe dozvoljenu specificiranu vrijednost, Kubernetes će automatski za nas napraviti još jednu kopiju kritičnog servisa.

## Prednosti korištenja Kubernetes sustava

Osim već spomenutog automatskog skaliranja u prethodnom poglavlju, Kubernetes sustav donosi i niz drugih prednosti. Automatskim skaliranjem postiže se ušteda novca reduciranjem nepotrebnih resursa i konzistentni rad naše aplikacije čak i u periodima povećane posjećenosti. Kubernetes sustav vrši konstantno nadgledanje cjelokupnog klastera. Ukoliko neki od čvorova ili containera prestane s radom, automatski će se poduzeti potrebna radnja. Dok nije bilo Kubernetes sustava, sistem administratori su morali konstantno nadgledati opterećenje pojedinih komponenti aplikacije i sukladno tome vršiti radnje koje bi rezultirale novim brojem instanci pojedine komponente, premještanjem svih komponenti na drugi radni čvor itd. Ovo možda i ne zvuči toliko strašno dok vam u 2 sata ujutro ne zazvoni mobitel da aplikacija nije dostupna u srcu sezone i da ste izgubili nekoliko tisuća ili milijuna potencijalne zarade. Kubernetes sustav omogućava sistem administratorima da mirno spavaju noću tako što automatski zamjenjuje pokvarene instance novim instancama. Ujutro, kada se naspavaju, u okviru radnog vremena mogu proučiti zbog čega je nastao problem i raditi na otklanjanju problema.

Koristeći Kubernetes sustav posao migriranja aplikacije na server više ne treba raditi Ops tim. Iz razloga što su aplikacije zapakirane u containere (engl. containerized), posjeduju sve potrebne biblioteke i okolinu za njihovo izvršavanje. Nije potrebno instalirati ništa dodatno na servere. Sukladno tome, programeri mogu samostalno aplikaciju migrirati na klaster. Svi radni čvorovi predstavljeni su kao jedna cjelina te nije potrebno imati nikoju informaciju u karakteristika servera za izvršavanje aplikacije. Radni čvorovi Kubernetes klastera ne moraju biti svi isti. Određen broj čvorova npr. može imati SSD diskove, dok drugi posjeduju HDD diskove. Ukoliko je potrebno, može se npr. specificirati zahtjev da se određena komponenta izvršava samo na čvorovima koji posjeduju SSD disk. Kubernetes sustav će samostalno rasporediti tu komponentu na čvor koji posjeduje SSD disk bez da mu mi točno navedemo koji je to čvor. S ovim smo postigli da ne trebamo voditi brigu na koji će se čvor pojedina komponenta smjestiti sve dok su zadovoljeni zahtjevi koje smo naveli u opisu aplikacije. Bez Kubernetes sustava, sistem administrator bi samostalno morao odabrati radni čvor koji posjeduje SSD disk od svih mogućih čvorova sa SSD diskom i na njega smjestiti komponentu.

Ljudi, za razliku od računala, su vrlo loši u pronalaženju optimalnih kombinacija pogotovo kad je broj takvih kombinacija velik. Zbog toga možemo biti sigurni da će Kubernetes sustav bolje i optimalnije rasporediti komponente aplikacije na klaster nego što bi to napravili ljudi. Kod odabira svakog radnog čvora uzimaju se u obzir razni parametri kao što su opterećenost radnog čvora, ispravnost rada, zahtijevani resursi i sl.

# PRVA APLIKACIJA NA KUBERNETES SUSTAVU

Prije nego što se objasne temeljni pojmovi Kubernetes sustava, svakako bi bilo dobro prvo na jednostavnom primjeru vidjeti kako izgleda proces izvršavanja aplikacije na Kubernetes-u. Mnogi autori literatura o Kubernetes sustavu slično pristupaju objašnjavanju istog navodeći sličnost s vožnjom auta. Prvo naučite voziti auto, a tek potom krenete učiti što se nalazi ispod haube i kako promijeniti ulje.

U ovom poglavlju cilj će biti napraviti „deploy“ jednostavne NodeJs aplikacije na Kubernetes klaster. Kompletan kod aplikacije može se naći na Github linku: <https://github.com/ikovac/kubernetes-hello-world>.  
Aplikacija se sastoji od svega par linija koda:

const express = require('express');

const app = express();

app.use('/', (req, res) => {

    res.send('Hello world!');

});

app.listen(3000, () => {

    console.log('App is listening on port 3000');

});

Sve što aplikacija radi je kreira server koji sluša sav dolazni promet na portu 3000 i odgovara sa „Hello world!“.

U poglavlju 3 već smo opisali kako izgleda ovaj proces, stoga će biti mnogo sličnosti ali s dodanim praktičnim primjerima. Kako je već rečeno prije nego što započnemo sa samim migriranjem na server, moramo aplikaciju zapakirati u Docker container. Da bi to napravili moramo kreirati Docker sliku.  
Unutar projekta kreirajmo datoteku naziva Dockerfile sa sljedećim naredbama:

FROM node:12.17.0

WORKDIR /usr/src/app

COPY package\*.json ./

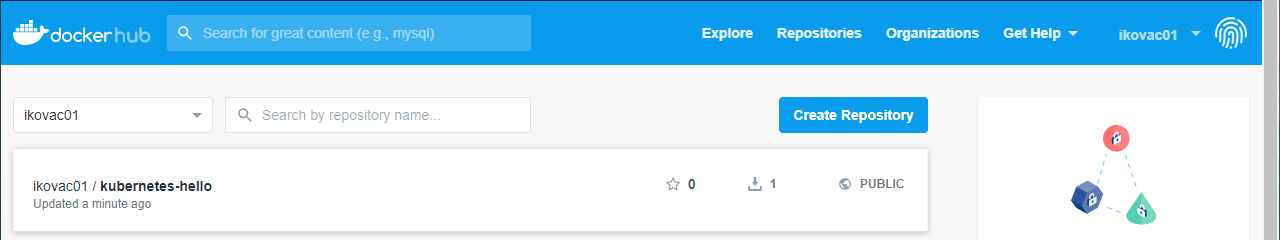
RUN npm install

COPY ./ ./

EXPOSE 3000

CMD ["node", "index.js"]

S ovim kažemo Dockeru da kreira sliku na temelju Nodejs slike. Time ćemo imati mogućnost izvršavanja NodeJs aplikacija bez da samostalno instaliramo NodeJs. Potom odaberemo radni direktoriji i kopiramo package.json datoteku unutar containera te instaliramo sve biblioteke.  
Naredbom „EXPOSE 3000“ naznačimo koji PORT koristimo unutar Docker containera. Naredba ništa ne radi nego služi samo kao smjernica. Na posljetku pokrenemo NodeJs aplikaciju sa naredbom „node index.js“ kao što bi to napravili i da izvršavamo aplikaciju izvan Docker-a. Da bi kreirali Docker sliku na temelju datoteke Dockerfile moramo izvršiti sljedeću naredbu:  
docker build -t image-name .  
Za image-name odabrao sam ikovac01/kubernetes-hello, gdje ikovac01 označava ime mog korisničkog računa na Docker Hub-u, a kubernetes-hello je ime same slike. Sliku je potrebno potom objaviti na registar slika – Docker Hub. To se postiže komandom: docker push ikovac01/kubernetes-hello. Ukoliko vam objava slike nije uspjela, morate se prijaviti na Docker Hub račun sa naredbom docker login. Pri uspješnoj objavi, Docker slika se treba pojaviti na Docker Hub-u (Slika 4.1).



Slika 4.1 Objava slike na Docker Hub

Prethodnim korakom našu aplikaciju smo zapakirali unutar Docker slike i to objavili na registar slika. Kubernetes će dohvatiti našu sliku i na temelju nje kreirati Docker container unutar kojeg će se izvršavati naša aplikacija.

Sljedeći korak je kreiranje Kubernetes klastera. Da bi mogli kreirati klaster prvo moramo imati račun na GKE. Iako se usluga plaća, dostupan je probni period od jedne godine koji je potpuno besplatan i bit će korišten u svrhu ovog diplomskog rada.

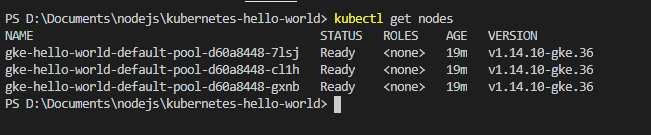
Kreiranje klastera je vrlo jednostavno. Stisnemo dugme „Create cluster“ i odaberemo ime našeg klastera (Slika 4.2).

A screenshot of a cell phone

Description automatically generated

Slika 4.2 Izrada klastera

Izrada klastera će potrajati neko vrijeme dok se ne kreiraju svi radni čvorovi koji posjeduju vlastite IP adrese. Klaster će se sastojati od 3 radna čvora, ukoliko niste promijenili standardne postavke pri kreiranju klastera. Nakon što se klaster kreira, možemo se iz komandne linije računala spojiti na novo-kreirani klaster. To se radi pritiskom na dugme „Connect“ i kopiranjem danog linka u komadnu liniju. Da bi se uvjerili kako klaster stvarno sadrži 3 radna čvora možemo izvršiti naredbu „kubectl get nodes“ (Slika 4.3). Kao rezultat dobijemo listu 3 radna čvora s nazivom, statusom i ostalim specifikacijama.



Slika 4.3 Lista radnih čvorova klastera

Sada konačno možemo objaviti našu aplikaciju na Kubernetes klaster. U prethodnim poglavljima rečeno je da developer mora objaviti opis aplikacije Kubernetes glavnom čvoru. Opis aplikacije se piše u yaml datotekama. Za objaviti aplikaciju kreirat ćemo datoteku Deployment.yaml sa sljedećim kodom:

apiVersion: apps/v1

kind: Deployment

metadata:

  name: kubernetes-hello

spec:

  replicas: 1

  selector:

    matchLabels:

      app: kubernetes-hello

  template:

    metadata:

      labels:

        app: kubernetes-hello

    spec:

      containers:

      - image: ikovac01/kubernetes-hello

        name: kubernetes-hello

U opisu se nalazi specificirano na osnovu koje Docker slike želimo kreirati aplikaciju i koliko replika te aplikacije želimo. Iako sama datoteka može izgledati zbunjujuće to je doista sve što smo naveli. Kao vrstu opisa koju šaljemo glavnom čvoru stavili smo „Deployment“. Rečeno je da Kubernetes u slučaju prestanka rada neke komponente kreira novu komponentu. To upravo radi Deployment resurs. Ukoliko trenutni broj replika ne odgovara specificiranom broju (u ovom slučaju samo jedna replika) onda Deployment poduzme radnje kako bi se postigao specificirani broj replika. Iz razloga što se naša aplikacija može sastojati od velikog broja servisa sa selektorom smo odabrali koju komponentu želimo staviti u nadzor ovog Deployment-a. Odabrali smo selektor „kubernetes-hello“ jer je to oznaka (engl. label) koju smo dodijelili toj komponenti. Deployment tip resursa će biti objašnjen detaljnije u narednim poglavljima.

Objava na glavni čvor se vrši naredbom „kubectl apply -f ./Deployment.yaml“. Primjetit ćemo da se pojavila crvena oznaka jer jedna replika ove aplikacije još nije spremna (Slika 4.4). Imamo 0/1 pokrenutih Pod-ova. Pod će također detaljnije biti objašnjen kasnije. Za sada to zamislimo kao kutiju u kojoj se izvršava jedan ili više containera.

A screenshot of a computer

Description automatically generated

Slika 4.4 Replika je u procesu stvaranja

Nakon što Kubernetes dohvati objavljenu Docker sliku i kreira Doker container iz iste trebali bi dobiti zelenu oznaku koja govori kako je sve prošlo uspješno (Slika 4.5).

A screenshot of a social media post

Description automatically generated

Slika 4.5 Replika je kreirana

Ovo možemo provjeriti i ako dohvatimo sve Pod-ove na kreiranom klasteru naredbom „kubectl get po“ (Slika 4.6) što je skraćeno od „kubectl1 get pods“.

A close up of a screen

Description automatically generated

Slika 4.6 Lista svih Pod-ova

Završetkom ovog koraka aplikacija je spreman i izvršava se na Kubernetes klasteru.

Kako pristupiti aplikaciji i uvjeriti se da stvarno radi?  
Pri kreiranju Pod-a, svaki dobije vlastitu IP adresu. Ta IP adresa je interna adresa i nije joj moguće pristupiti iz vanjskog svijeta. Da bi pristupili aplikaciji moramo nekako izložiti pristup aplikaciji i izvan klastera. To se radi pomoću novog Kubernetes resursa nazvanog „Service“ koji će također biti detaljnije objašnjen kasnije.

Da bi kreirali Service, kreirajmo novu datoteku service.yaml sa sljedećim kodom:

apiVersion: v1

kind: Service

metadata:

  name: kubernetes-hello-service

spec:

  type: LoadBalancer

  ports:

  - port: 3000

    targetPort: 3000

  selector:

    app: kubernetes-hello

Service možemo nazvati kako hoćemo. U primjeru je nazvan kubernetes-hello-service. Sljedeće što moramo napraviti je specificirati tip servisa. LoadBalancer je tip servisa koji će biti dostupan izvan klastera jer će imati vanjsku IP adresu na koju ćemo moći pristupiti aplikaciji. Uz IP adresu moramo specificirati i na kojem portu želimo da aplikacija bude dostupna. Odabran je port 3000. Ovo može biti bilo koji drugi slobodni i dostupni port samo je bitno da kao „targetPort“ bude navedeno 3000 jer je to port na kojem aplikacija sluša dolazeće zahtjeve. Naposljetku, sa selektorom kažemo Kubernetes-u koju točno komponentu aplikacije želimo izložiti da bude javno dostupna. Naša aplikacija ima samo jednu komponentu kojoj smo dodijelili oznaku „kubernetes-hello“.

Nakon što objavimo servis na glavni čvor već poznatom naredbom „kubectl apply -f ./service.yaml“ u listi servisa moći ćemo vidjeti novo-kreirani servis (Slika 4.7).

A screenshot of a social media post

Description automatically generated

Slika 4.7 Servis je kreiran, ali još nije spreman

Aplikacija još neće biti dostupna jer proces dodjele javne IP adrese traje neko vrijeme. Nakon što se dodijeli javna IP adresa možemo pristupiti servisu (Slika 4.8).

A screenshot of a social media post

Description automatically generated

Slika 4.8 Javna IP adresa je dodijeljena servisu

Ovim korakom aplikacija je u potpunosti spremna i možemo joj pristupiti. Ukoliko odemo na dobivenu vanjsku IP adresu na port 3000 vidjet ćemo „Hello world!“ kao rezultat (Slika 4.9).

A screenshot of a social media post

Description automatically generated

Slika 4.9 Aplikacija je dostupna izvan klastera

Bilo tko u svijetu može pristupiti aplikaciji na dobivenoj IP adresi. Aplikacija je napokon objavljena i radi.

Iako se proces možda u početku pari kompliciran, u biti je vrlo jednostavan. Ukoliko napravimo sažetak, sve što smo napravili je zapakirali aplikaciju u Docker sliku i tu sliku objavili na registar slika. Potom smo glavnom čvoru poslali opis aplikacije sa navedenim imenom Docker slike i koliko replika želimo i na kraju smo kreirali servis da naša aplikacija bude dostupna i izvan klastera. Aplikacija je sada u rukama Kubernetes sustava koji će biti zadužen da uvijek imamo željeni broj replika i u slučaju prestanka rada kreirati nove replike. Moguće je i naknadno mijenjati broj replika. Samo uredite datoteku tako što promijenite broj iz 1 u novi željeni broj replika i spremite promjene. Kubernetes sustav će potom vidjeti da željeni broj replika nije jednak postojećem stanju te će kreirani nove replike.

# TEMELJNI POJMOVI KUBERNETES SUSTAVA

U prethodnom poglavlju spomenute su neke osnovne Kubernetes komponente koje još nisu detaljno objašnjene. U ovom poglavlju detaljnije ćemo objasniti najvažnije Kubernetes komponente koje je nužno poznavati ukoliko želimo da se naša aplikacija uspješno izvršava na Kubernetes sustavu. Započet ćemo sa komponentom koja se naziva Pod.

## Pods

Container je Docker slika koja se izvršava. Predstavlja proces tj. program u izvođenju. Zamisao containera je da izoliraju jedan zaseban proces. Iako se unutar containera može nalaziti više procesa, to nije preporučljivo. Svaki container bi trebao sadržavati najviše jedan proces (osim ukoliko proces ne pokreće vlastite pod-procese). Ukoliko se unutar containera nagomila više procesa, odgovornost programera je da osigura ponovno pokretanje procesa u slučaju grešaka.

Iz razloga što ne bismo smjeli grupirati više procesa unutar jednog containera, mora postojati neka komponenta koja će osigurati viši nivo konstrukcije. Upravo ta komponenta se naziva Pod. Pod-ovi omogućavaju povezivanje različitih containera u jedinstvenu cjelinu. Pod je najmanja migracijska jedinica (engl. deploy unit) Kubernetes sustava. Umjesto da se containeri samostalno migriraju, migracija se uvijek radi na Pod-u koji sadrži containere. Preporučljivo je da svaki Pod ima samo jedan container, iako postoje iznimke kada je potrebno da Pod sadržava više containera. Naknadno će biti objašnjeno kada je to slučaj. Ukoliko Pod sadrži više containera pravilo je da se svi containeri uvijek izvršavaju na istom radnom čvoru (Slika 2.1).

A screenshot of a cell phone

Description automatically generated

Slika 5.1 Svi containeri Pod-a moraju se izvršavati na istom radnom čvoru

Pod omogućava da se srodni procesi pokreću zajedno pružajući istu okolinu kao i da se pokreću skupa unutar istog containera, uz prednost što su procesi izolirani jer se svaki izvršava unutar vlastitog containera.

Svaki Pod posjeduje vlastitu IP adresu koju dijele svi containeri unutar Pod-a. Containeri unutar Pod-a mogu komunicirati preko localhost-a . Također, svi containeri dijele i isti port prostor. Posljedično tome, moramo paziti da containeri unutar Pod-a ne dijele isti port broj. Ovo se samo odnosi na containere koji se nalaze u istom Pod-u. Containeri u različitim Pod-ovima mogu bez problema dijeliti isti port broj.

Komunikacija između Pod-ova je također moguća. Čak i u slučajevima kada se Pod-ovi ne nalaze na istom radnom čvoru oni i dalje mogu komunicirati. Razlog tome je upravo što svaki Pod posjeduje vlastitu IP adresu koja je dohvatljiva bilo gdje u klasteru.

Pod-ove zamislimo kao zasebne mašine gdje se u svakoj mašini nalazi zasebna komponenta aplikacije. Pod-ovi su vrlo učinkoviti s obzirom na hardverske resurse. Zbog toga se ne moramo misliti da li nešto odvojiti u različite Pod-ove ili smjestiti sve u jedan Pod. Na primjer, ukoliko imamo aplikaciju koja se sastoji od front-end i back-end komponente, uvijek bi trebali te dvije komponente smjestiti u različite Pod-ove. Iako nas ništa ne sprječava da sve smjestimo u isti Pod, to svakako nije poželjno i preporučljivo. Razlog više je i skaliranje. Razne komponente aplikacije će vrlo vjerojatno imati različite potrebe za skaliranjem. Zamislimo situaciju da od ukupnog prometa samo 10% zahtjeva ide na back-end. Vrlo vjerojatno ćemo imati potrebu za većim brojem front-end Pod-ova nego back-end Pod-ova. Da se ove dvije komponente nalaze unutar istog Pod-a, ne bismo ih mogli skalirati odvojeno nego kao cjelinu. Slično je i da imamo web server i bazu podataka. Ove dvije komponente aplikacije također ima smisla odvojiti u različite Pod-ove.

Zbog svega navedenog, vidimo da ima smisla odvajati različite komponente aplikacije u različite Pod-ove, nekada ima smisla staviti različite komponente u isti Pod. Komponente bi trebalo staviti u isti Pod samo i samo ako su usko povezane. Na primjer, ukoliko imamo primarni container i sekundarni container koji zajedno rade istu zadaću. Zamislimo da imamo web server koji poslužuje sadržaj iz određenog direktorija i sekundarni proces koji sa interneta dohvaća resurse i sprema ih u folder iz kojeg web server poslužuje sadržaj.

Na ovom primjeru dva containera dijele isti datotečni sustav. Sekundarni container sprema u datoteku iz koje primarni container čita. Samo u ovakvim i sličnim situacijama trebalo bi različite containere staviti u isti Pod.

### Oznake Pod-ova

Kod mikroservis arhitektura uobičajeno je da imamo veliki broj različitih servisa. To rezultira velikim brojem Pod-ova. Kako bi s Pod-ovima bilo lakše raditi koristimo oznake (engl. labels) s kojima Pod-ove grupiramo u različite kategorije (Slika 5.2). Oznaka se sastoji od para ključ-vrijednost (engl. key-value) koja se pridodaje ne samo Pod-ovima nego i ostalim resursima Kubernetes sustava. Na primjer, radnom čvoru možemo dodijeliti oznaku disk=SSD ukoliko radni čvor posjeduje SSD disk. Ova tehnika predstavlja vrlo moćan alat Kubernetes sustava jer znatno olakšava upravljanje resursima. Kod migracije na klaster, ukoliko želimo da se neki Pod izvršava na radnom čvoru sa SSD diskom, samo ćemo dodati tu oznaku u selektor.

A screenshot of a cell phone

Description automatically generated

Slika 5.2 Organizacija Pod-ova pomoću oznaka [3]

Dodavanjem oznaka kao na slici (Slika 5.2) postižemo organizaciju Pod-ova u dvije dimenzije. App se odnosi na vrstu komponente aplikacije. Na primjer, korisničko sučelje će za ključ app imati vrijednost ui, kupovna košarica će imati svoju oznaku sc itd. Svaka komponenta može imati i više različitih verzija. U procesu izrade softvera svaka komponenta prolazi kroz više ciklusa. Kada programer isprogramira komponentu, komponenta najprije mora proći testiranje prije nego što se stavi u produkciju. Oznakama možemo označiti i je li komponenta pripada produkcijskoj, testnoj ili nekoj drugoj verziji. Ukoliko želimo korisnicima prikazati samo produkcijsku verziju aplikacije, prilikom kreiranja Pod-a kao selektor ćemo staviti samo produkcijsku oznaku verzije. Oznake se mogu dodavati i mijenjati kod već postojećih Pod-ova. U nadolazećim poglavljima vidjet ćemo zašto je ovo važno.

### Objava Pod opisa kroz yaml datoteku

Kao što smo već vidjeli, s Kubernetes glavnim čvorom komuniciramo šaljući zahtjeve u obliku yaml datoteka. Yaml datoteke sadrže opis resursa kojeg želimo kreirati na Kubernetes klaster. Ukoliko želimo kreirati Pod resurs, trebamo poslati yaml datoteku glavnom čvoru koja kao tip resursa sadrži „Pod“.

Jednostavan primjer pod.yaml datoteke koja kreira Pod je sljedeći:

apiVersion: v1

kind: Pod

metadata:

  name: kubernetes-hello

spec:

  nodeSelector:

    gpu: "true"

  containers:

  - image: ikovac01/kubernetes-hello

    name: kubernetes-hello

Ova datoteka će kreirati resurs tipa Pod unutar kojeg će se pokretati container koji nastaje iz Docker slike ikovac01/kubernetes-hello. Slika je javno dostupna na Docker registru slika. Oznakom gpu: „true“ smo specificirali da želimo odabrati radni čvor koji posjeduje grafičku karticu. Ovim primjerom vidimo koliko je jednostavno pomoću oznaka (engl. labels) selektirati željene resurse.

Datoteku šaljemo glavnom čvoru već viđenom naredbom: „kubectl apply -f pod.yaml“. Ukoliko je sve prošlo u redu, Pod će biti kreiran na klasteru. Naredbom „kubectl get pods“ se mogu ispisati svi Pod-ovi na klasteru i vidjeti je li novo-kreirani Pod na listi.

## Deployments

U prethodnom poglavlju je pokazano kako se može kreirati Pod resurs na Kubernetes klasteru. U praksi se vjerojatno ovaj proces nikada neće samostalno raditi. Kada Pod resurs kreiramo na spomenuti način, Kubernetes odabere radni čvor kojem će dodijeliti novo-stvoreni Pod. Ukoliko Pod prestane s radom ili se iz nekog razloga izbriše iz klastera neće biti stvoren novi Pod. Na primjer, ukoliko radni čvor na kojem se nalazi Pod prestane s radom, Pod koji je na ovaj način stvoren i nalazi se na ovom radnom čvoru je izgubljen i neće biti ponovno kreiran od strane Kubernetes-a.

Ukoliko želimo da Kubernetes sustav vodi računa o automatskom ponovnom pokretanju neispravnih Pod-ova moramo kreirati resurs Deployment koji će potom kreirati potreban broj Pod-ova. Deployment smo već kreirali u poglavlju 4.

Zadaća Deployment resursa je prvo da kreira potreban broj Pod-ova u skladu sa specifikacijom, a potom da prati status tih Pod-ova. Ukoliko container unutar Pod-a prestane s radom, Pod će ponovno pokrenuti neispravni container. Slično tome, ukoliko Pod prestane s radom (npr. zbog memory leak-a) zadaća Deployment resursa je da uvidi problematičnost Pod-a i kreira novi Pod kojim će zamijeniti problematični Pod. Ovim načinom iskorišteni su svi potencijali Kubernetes sustava i u pravilu ne bih trebalo nikad samostalno kreirati Pod-ove nego taj posao prepustiti Deployment resursu.

Slika 5.3 opisuje razliku između Pod-a koji je stvoren ručno i onoga koji je stvoren od strane Deployment-a. Primjećujemo da prilikom prestanka rada radnog čvora 1, Deployment uoči da trenutno ne postoji dovoljan broj Pod-a B koji je pod nadležnosti tog Deployment-a te stvori novi Pod B na nekom od ispravnih radnih čvorova. Pod A koji se nalazio na radnom čvoru 1 će biti izgubljen i neće biti stvoren novi isti takav Pod. Razlog tome je što je Pod A ručno stvoren i nije u nadležnosti niti jednog Deployment resursa.

A screenshot of a cell phone

Description automatically generated

Slika 5.3 Prilikom prestanka rada radnog čvora, Deployment resurs kreira novi Pod

### Kontrole ispravnosti Pod-a

Dvije su glavne tehnike kojima se provjerava ispravnost Pod-ova. Nazivaju se „probe života i spremnosti (engl. liveness i readiness probes).

Liveness probe zadužena je za praćenje ispravnosti Pod-a tokom njegovog rada. Provjera ispravnosti Pod-a se odvija periodički u postavljenim vremenskim intervalima. Za svaki container unutar Pod-a može biti postavljena zasebna liveness proba. Više je načina na koji se liveness proba može izvršiti a najpoznatiji je onaj putem HTTP GET zahtjeva. Ova proba uključuje slanje HTTP GET zahtjeva na URL koji se sastoji od IP adrese containera, porta containera i putanje koje specificiramo u yaml opisu. Ukoliko kao odgovor dobijemo statusni kod 2xx ili 3xx, proba se smatra uspješnom. U protivnom, proba se smatra neuspješnom i kreće postupak stvaranja novog Pod-a koji će zamijeniti neispravni Pod. Naravno da se novi Pod ne stvara odmah nakon prve neuspjele probe, nego se treba dogoditi određen broj neuspjelih probi i tek onda kreće spomenuti postupak.

Primjer liveness probe prikazan je sljedećim yaml opisom:

apiVersion: v1

kind: Pod

metadata:

 name: kubernetes-hello

spec:

 containers:

 - image: ikovac01/kubernetes-hello

   name: kubernetes-hello

   livenessProbe:

     httpGet:

       path: /

       port: 3000

Ovim opisom kreiramo novi Pod koji nastaje iz slike ikovac01/kubernetes-hello. Jedino što se razlikuje od prijašnje kreacije Pod-a je dodana liveness proba pod „livenessProbe“ sekcijom. Liveness proba će poslati GET zahtjev na putanju „path: /“ i na port 3000. Dakle GET zahtjev će se u konačnici poslati na url: „http://[CONTAINER\_IP]:3000/“. Nakon što kreiramo Pod, ukoliko dođe do bilo kakve pogreške servera i odgovor na liveness probu ne bude uspješan Kubernetes će automatski pokrenuti stvaranje novog Pod-a kojim će zamijeniti postojeći problematični Pod.

Osim spomenutih specifikacija, za liveness probu se mogu konfigurirati i period slanja zahtjeva, vrijeme odgode (vrijeme koje prođe od stvaranja Pod-a do prve liveness probe), vrijeme u kojem container mora dati odgovor na probu, koliko najviše puta proba smije biti neuspješna prije kreiranje novog Pod-a itd.

Za razliku liveness probi koje su zadužene za provjeru ispravnosti Pod-a tokom rada Pod-a, postoje i readiness probe. Readiness probe su zadužene za provjeru je li Pod ispravno započeo sa svojim radom.

Readiness probe sprječavaju slanje zahtjeva Pod-u koji još nije spreman za rad. Na primjer, ukoliko imamo jedan Pod web server komponente i želimo dodati još jedan Pod, novo-stvorenom Pod-u neće biti prosljeđivani zahtjevi sve dok uspješno ne odgovori na readiness probu. U slučaju da ne postoji readiness proba, promet bi bio ravnomjerno raspoređen između dva Pod-a te bi novo-stvoreni Pod odgovorio sa server pogreškom ili bi isteklo vrijeme u kojem je potrebno dobiti odgovor servera. Tek nakon što bi novo-stvoreni Pod započeo s radom, sve bi uspješno radilo.

Liveness i Readiness probe je uvijek dobro staviti u yaml opis jer predstavljaju vrlo koristan i moćan alat Kubernetes sustava.

### Objava Deployment opisa i demonstracija automatske zamjene neispravnih Pod-ova

Deployment resurs ćemo objaviti na isti način kao i u poglavlju 4. Objavit ćemo deployment.yml datoteku s naredbom „kubectl apply -f ./deployment.yml“.

Sadržaj deployment.yml datoteke je sljedeći:

apiVersion: apps/v1

kind: Deployment

metadata:

  name: kubernetes-hello

spec:

  replicas: 3

  selector:

    matchLabels:

      app: kubernetes-hello

  template:

    metadata:

      labels:

        app: kubernetes-hello

    spec:

      containers:

      - image: ikovac01/kubernetes-hello

        name: kubernetes-hello

Sadržaj je u potpunosti isti kao i u poglavlju 4 osim što je broj replika povećaj na 3.

Ukoliko ispišemo sve Pod-ove na klasteru naredbom: „kubectl get po“ dobit ćemo ispis kao na slici ispod (Slika 5.4).

A close up of a screen

Description automatically generated

Slika 5.4 Ispis Pod-ova na klasteru

Demonstracije radi, ručno ćemo izbrisati jedan Pod kako bi se uvjerili da Deployment resurs automatski kreira novi Pod kako bi specificirani broj Pod-ova (u ovom primjeru je 3) bio jednak stvarnom broju Pod-ova.  
Pod ćemo izbrisati komandom „kubectl delete pod [POD\_NAME]“ kao što je prikazano na slici ispod (Slika 5.5).

A close up of a screen

Description automatically generated

Slika 5.5 Ispis Pod-ova nakon brisanja jednog Pod-a

Za očekivati je bilo da ćemo nakon brisanja Pod-a imati samo 2 Pod-a. To se nije dogodilo zbog već spomenutog Deployment resursa koji je odmah kreirao novi Pod. Proces kreiranja novog poda se odvio toliko brzo da nismo uspjeli niti ispisat stanje na klasteru kada smo imali samo 2 Pod-a.

## Services

Kao što smo već vidjeli u poglavlju 4 Service resurs nam omogućava pristup skupu Pod-ova za koje je taj Service zadužen. U ovom dijelu ćemo detaljnije objasniti zbog čega uopće postoji potreba za Service resursima.

U mikro-servis arhitekturi postoje servisi koji moraju međusobno komunicirati kako bi zajedno izvršili neki zadatak. Ukoliko ne govorimo o Kubernetes sustavu, da bi ostvarili komunikaciji između dvaju servisa, sistem administrator bi vjerojatno trebao migrirati taj servis na neki server i javno dobivenu IP adresu podijeliti s ostalim servisima koji žele komunicirati s tim servisom. Međutim u Kubernetes sustavu ovo ne bi bilo funkcionalno. Sljedeći su razlozi zašto je to tako:

* U svakom trenutku novi Pod-ovi se mogu stvarati i uklanjati zbog promjene broja instanci Pod-a, zbog prestanka rada određenog Pod-a, zbog premještanja Pod-a na neki drugi radni čvor i slično.
* IP adresa se dodjeljuje Pod-u nakon što je smješten na odgovarajući radni čvor i prije nego što je sami Pod kreiran. Posljedično tome, klijent ne može unaprijed znati IP adresu koju će novo-stvoreni Pod imati te nema nikoju informaciju o tome kako pristupiti Pod-u.
* Horizontalnim skaliranjem se povećava broj Pod-ova od kojih svaki ima svoju vlastitu i jedinstvenu IP adresu. Klijent se ne bi trebao zamarati koliko je tih Pod-ova i koje su im IP adrese. Umjesto da klijenti prate listu svih Pod-ova koji pružaju isti servis i traže njihove IP adrese lakše bi bilo da tom servisu mogu pristupiti preko jedinstvene IP adrese.

Service resurs upravo rješava sve ove probleme. Kreiranjem Service resursa omogućuje se pristup određenom Pod-u ili određenoj grupi Pod-ova koja predstavlja neku komponentu aplikacije. Service resurs prilikom kreiranja dobije jedinstvenu IP adresu koja se više ne mijenja te je Service-u moguće pristupiti neovisno o tome jesu li u međuvremenu stvoreni ili uklonjeni neki Pod-ovi. Dakle Service-i pružaju jedinstvenu IP adresu i port koji se nikada ne mijenjaju dok Service postoji. Klijent može poslati zahtjev na IP adresu i port Service-a koji će se potom proslijediti na neki od Pod-ova koji spadaju pod taj Service. Može biti više raznih Service-a na klasteru. Obično za svaku komponentu aplikacije (svaki mikro-servis) postoji jedan Service resurs preko kojeg se pristupa toj komponenti.

Na ovaj način prilikom pristupa komponenti, nije potrebno poznavati lokaciju pojedinog Pod-a koji se mogu slobodno premještati na radne čvorove klastera.

Service može biti i interni i eksterni dohvatljiv. To znači da ukoliko je Service interni, može biti dohvatljiv samo unutar klastera dok eksterni Service može biti dohvatljiv i izvan klastera.   
Na primjeru dva tipa servisa ćemo pokazati ulogu Service resursa. Neka imamo prvu komponentu koja predstavlja web server i drugu komponentu koja predstavlja bazu podataka. Web server prilikom klijentskog zahtjeva radi upit na bazu podataka i klijentu vraća odgovor. Vanjski klijent mora imati mogućnost spajanja samo na web server. Također klijent se ne bi trebao zamarati detaljima da li postoji samo jedan ili više instanci tog web servera. Klijentu je bitno samo da poznaje jedinstvenu IP adresu i port na koji može poslati svoj zahtjev da dobije željeni odgovor.

Komponenta baze podataka mora također biti dohvatljiva ali ne i izvan klastera. Web server će morati komunicirati sa komponentom baze podataka da bi klijentu dao željeni odgovor. Web server mora poznavati jedinstvenu IP adresu Service-a baze podataka. Slika ispod (Slika 5.6) pokazuje ovaj primjer. Ukoliko dođe do potrebe horizontalnog skaliranja web servera i dodaju se novi web server Pod-ovi, IP adresa web server Service-a će ostati nepromijenjena te će klijent i dalje pristupati web serveru na isti način kao što je i prije pristupao.

A close up of a piece of paper

Description automatically generated

Slika 5.6 Vanjski i unutrašnji klijenti Pod-ovima pristupaju preko Service resursa

Unutar Kubernetes klastera nije potrebno raditi s IP adresama Service-a. Kubernetes posjeduje lokalni DNS server koji nam omogućava da pojedinim servisima pristupamo na nama lakši i jednostavni način. Ljudi su vrlo loši u pamćenju brojeva kao što je IP adresa i mnogo bolje pamte riječi. Kubernetes nam omogućava da unutar klastera servisima pristupamo preko njihovog imena. Tako ćemo u gornjem primjeru servisu baze podataka moći pristupiti i preko imena servisa umjesto IP adrese 10.10.10.11. Ovo ćemo detaljnije vidjeti u narednim poglavljima na primjeru Chat aplikacije koja će biti obrađena u sklopu ovog diplomskog rada.

Ukoliko naročito nije specificirano, Service će nasumično proslijediti zahtjev nekom od Pod-ova. Može se specificirati da Service prosljeđuje zahtjev uvijek istom Pod-u na koji je proslijedio prvi zahtjev tog klijenta. To se radi na temelju IP adrese klijenta. Ako je odabran ovaj način, nakon što se nasumično odabere Pod kod prvog zahtjeva, svi budući zahtjevi ovog klijenta će se također slati na isti Pod. Service resursi ne rade na HTTP razini te će biti moguće prosljeđivati zahtjeve samo na temelju IP adrese a ne recimo i informacije u kolačićima (engl. cookies). Da bi ovo postigli morat ćemo koristiti neke druge tipove Service-a kao Ingress servis koji će biti objašnjen naknadno.

### Vrste servisa

Više je vrsta Service resursa:

1. ClusterIP - ovakav tip servisa je dostupan samo unutar klastera. Ovo je zadani tip servisa te će servis biti ovog tipa ukoliko nikoji drugi tip servisa nije specificiran.
2. NodePort - na svakom radnom čvoru izlaže broj porta servisa. Servisu će se moći pristupiti na <NodeIp>:<NodePort> te će servis biti eksterni, dakle moći će mu se pristupiti i izvan klastera.
3. LoadBalancer - ovakav tip servisa je također dostupan i izvan klastera. LoadBalancer dobije jedinstvenu IP adresu preko koje klijent pristupa servisu. Zahtjev se potom prosljeđuje radnim čvorovima na specificiranom portu. Ovaj tip servisa je u stvari NodePort tip servisa ali je na neki način odvojen od same klaster arhitekture.
4. Ingress – mehanizam koji omogućava izlaganje više servisa preko jedinstvene IP adrese. Radi na HTTP razini koja omogućava još više konfiguracijskih opcija nego standardni tip Service resursa.

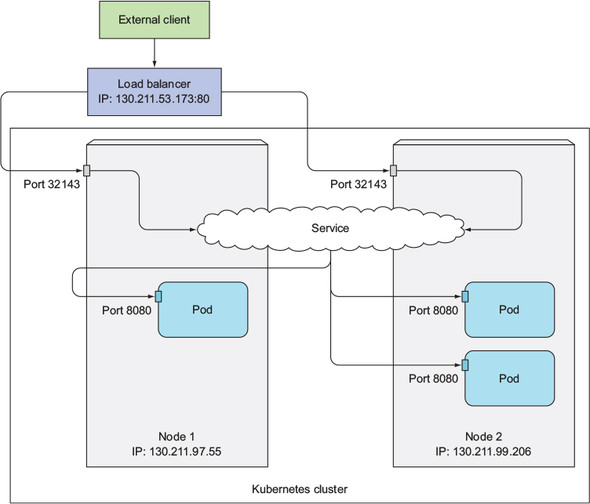
**NodePort** je najlakše razumijeti iz slike (Slika 5.7). Klijent se spaja na prikazani servis preko IP adrese nekog od radnih čvorova te porta radnog čvora koji je namijenjen tom servisu. U ovom slučaju klijent može specificirati IP adresu radnog čvora 1 ili radnog čvora 2. Iako je za zaključiti da će se zahtjev proslijediti nekom od Pod-ova na radnom čvoru kojeg klijent specificira, to nije tako. Nakon što klijent navede IP adresu i port na radnom čvoru, zahtjevi će se ravnomjerno raspoređivat između Pod-ova. Nije važno koju IP adresu radnog čvora klijent odabere, sve dok je odabrani čvor ispravan. Ukoliko se dogodi da radni čvor kojeg je klijent odabrao prestane s radom, neće biti moguće slati zahtjeve na isti radni čvor.

A close up of a logo

Description automatically generated

Slika 5.7 Eksterni klijent se povezuje s NodePort servisom preko IP adrese radnog čvora 1 ili preko IP adrese radnog čvora 2 [3]

**LoadBalancer** tip servisa je odvojen od klaster arhitekture (Slika 5.8). Klijent pristupa servisu tako što navede IP adresu LoadBalancer-a koji potom zahtjev prosljeđuje na neki od dostupnih radnih čvorova. LoadBalancer tehnika kao podlogu koristi NodePort tehniku, ali i rješava problem NodePort tehnike kada neki od radnih čvorova prestane s radom. Tada smo rekli da klijent neće moći pristupiti servisu ukoliko koristi IP adresu radnog čvora koji je prestao s radom. LoadBalancer to rješava tako da postoji viši sloj koji je odvojen od NodePort tehnike. Taj viši sloj prosljeđuje zahtjev na onaj čvor koji je u tom trenutku ispravan ili ukoliko su svi ispravni onda ravnomjerno raspoređuje zahtjeve između radnih čvorova.



Slika 5.8 Eksterni klijent pristupa LoadBalancer servisu [3]

Još je jedan tip servisa, a to je **Ingress** servis. Ingress servis radi na HTTP razini te znatno proširuje mogućnosti Service resursa. Ingress resurs može raditi preusmjeravanje prometa ne samo na osnovu IP adrese već i na osnovu imena domene i na osnovu putanje (engl. path) (Slika 5.9).

A screenshot of a cell phone

Description automatically generated

Slika 5.9 Više servisa može biti izloženo kroz jedan jedini Ingress

Korištenjem LoadBalancer tipa, moramo za svaki servis osigurati vlastitu javnu IP adresu. Ingress zahtjeva samo jednu IP adresu. To je moguće iz razloga što Ingress radi na već spomenutoj HTTP razini pa je moguće raditi usmjeravanje i na osnovu host polja te na osnovu putanje. S ovim je moguće postići da imamo na primjer jednu domenu: „http://example.com“ te ukoliko je putanja '/' zahtjev preusmjeriti na servis koji izvršava klijentsku aplikaciju, a ako je putanja 'api' (http://example.com/api) zahtjev preusmjeriti na API web server.

Osim usmjeravanja prometa na osnovu putanje, Ingress posjeduje još i mnogo drugih mogućnosti. Jedna od njih je svakako postavljanje TSL prometa. Umjesto da programeri unutar same aplikacije postavljaju TSL certifikate, to se jednostavno postiže u postavkama Ingress-a. Promet između klijenta i Ingress kontrolera je TSL enkriptiran, dok nije enkriptiran promet između Ingress-a i servisa koji se svakako nalazi unutar klastera. Koristeći TSL na razini Ingress-a smo osigurali da programeri ne trebaju mijenjati aplikaciju postavljajući TSL certifikate. To nije dobro iz više razloga a jedan od njih je da mijenjanje TSL certifikate (npr. zbog isteka istog) uzrokuje rekompajliranje cijele aplikacije.

## Volumes

Procesi unutar Pod-a dijele iste resurse kao što su CPU, RAM, mrežna sučelja i druge. Međutim, procesi ne dijele isti disk prostor. Već smo rekli da svaki container u Pod-u posjeduje vlastiti izolirani datotečni sustav iz razloga što datotečni sustav nastaje na osnovu Docker slike. Prilikom kreiranja novih containera iz iste Docker slike, svi će imati isti početni datotečni sustav. Container unutar Pod-a se može ponovno pokrenuti uslijed prestanka rada ili ukoliko liveness probe otkrije neispravnost u radu containera. Prilikom ponovnog pokretanja containera cijeli datotečni sustav u tom trenutku će se izgubiti. Novi container će vidjeti samo one datoteke koje nastaju iz same Docker slike, a ne i one koje je sam proces unutar containera izgenerirao (ukoliko postoje).

Kubernetes sustav omogućava rješavanjem ovog problema koristeći Volumes resurs. Volumes resurs se ne kreira zasebno kao što je bio slučaj sa Pod, Deployment i Service resursima već se specificiraju u opisu Pod-a i imaju isti životni vijek kao Pod-ovi. To znači da će prilikom kreiranja Pod-a biti kreiran i Volume resurs. Isto tako ukoliko se Pod uništi biti će uništen i Volume resurs. Prilikom ponovnog pokretanja containera zbog neispravnost, novo-stvoreni container će vidjeti sve datoteke spremljene od strane prethodnog containera jer se nalaze u istom Pod-u. Volume se stvara na razini Pod-a i zajednički je za sve containere unutar Pod-a. Da bi containeri mogli koristiti Volume Pod-a mora se u opisu točno specificirati koji containeri imaju pristup Volume resursu.

U poglavlju 5.1 rečeno je da jedino kod srodnih procesa ima smisla u isto Pod stavljati više containera. Naveden je primjer sa web serverom kao primarnim procesom i sekundarnim procesom koji dohvaća sadržaj koji će web server posluživati. Da bi ovo bilo moguće, primarni i sekundarni proces moraju dijeliti isti datotečni sustav. Ovo se postiže korištenjem Volume resursa (Slika 5.10). Na slici možemo vidjeti da unutar istog Pod-a postoje dva containera. Container 1 zaslužan je za dohvaćanje sadržaja koji će Container 2 posluživati. Container 1 dohvaćeni sadržaj spremi u vlastiti datotečni sustav u mapu „preuzimanja“ koja je povezana sa zajedničkim Volume resursom. Container 2 poslužuje sadržaj iz vlastite mape public/html koja je spojena na istu mapu kao i mapa „preuzimanja“ containera 1. Na ovaj način container 2 će vidjeti sve datoteke koje container 1 preuzme.

A screenshot of a cell phone

Description automatically generated

Slika 5.10 Korištenje istog disk prostora između dva različita containera unutar Pod-a

Primjer yaml opisa ovakvog Pod-a bi bio:

apiVersion: v1

kind: Pod

metadata:

 name: content-generator

spec:

 containers:

 - image: html-generator

   name: html-generator

   volumeMounts:

   - name: html

     mountPath: /preuzimanja

 - image: nginx:alpine

   name: web-server

   volumeMounts:

   - name: html

     mountPath: /usr/share/nginx/html

     readOnly: true

 ports:

 - containerPort: 80

 volumes:

 - name: html

   emptyDir: {}

Docker slika „html-generator“ je izmišljena za potrebe ovog primjera i vjerojatno ne postoji ali samo ime bi trebalo otkriti što ovaj container radi. Ovim opisom kreirali smo Pod s dva containera – html-generator container i web-server container. Na dnu datoteke kreiran je prazni Volume naziva html. Taj smo Volume specificirali da koristima u oba containera. Sa ključnom riječi „volumeMounts“ smo povezali datotečni sustav unutar containera sa Volume datotečnim sustavom koji je zajednički za oba containera. Postigli smo da sve što html-generator kreira u direktoriju /preuzimanja bude dostupnu web-server containeru u direktoriju /usr/share/nginx/html.

### Trajno skladište

Životni vijem Volume resursa koji smo kreirali u prethodnom primjeru isto je kao i životni vijek Pod-a u kojem se nalazi. To znači da ćemo prilikom ponovnog kreiranja Pod-a ili premještanja Pod-a na drugi radni čvor izgubiti sve dotadašnje podatke iz datotečnog sustava. Na primjer, ukoliko se radi o Pod-u koji izvršava bazu podataka, prestankom rada tog Pod-a svi podaci iz baze će biti trajno izbrisani. Ovo je pogotovo nepraktično u procesu testiranja kada se učestalije stvaraju i uklanjaju Pod-ovi.

Kubernetes sustav ima rješenje i za ovaj problem korištenjem trajne pohrane. Korištenjem Google-ovog Kubernetes sustava imamo mogućnost kreiranja trajnog disk prostora željene veličine.

Korištenje trajne pohrane je vrlo slično kao i korištenje običnog Volume resursa. U opisu Pod yaml datoteke moramo specificirati kojem containeru dozvoljavamo pristup trajnoj pohrani (koju smo prethodno ručno kreirali na GKE) i koji direktoriji povezujemo. Prilikom kreiranja novog Pod-a Volume unutar Pod-a neće biti prazan, nego će se napuniti sadržajem trajne pohrane. Isto tako, kada container unutar Pod-a napravi izmjenu unutar svog datotečnog sustava, ta će se promjena odraziti i na trajnu pohranu (Slika 5.11). Ovim načinom postigli smo da će sav prethodni sadržaj baze podataka biti dostupan i nakon ponovnog kreiranja Pod-a.

A screenshot of a cell phone

Description automatically generated

Slika 5.11 Logika korištenja trajne pohrane

## ConfigMaps i Secrets

Skoro sve aplikacije koje se koriste u produkciji zahtijevaju određene konfiguracijske parametre. Ukoliko se radi o bazi podataka, konfiguracijske parametri će vjerojatno biti ime baze, ime korisnika, lozinka korisnika itd. Za web server parametri mogu biti port, TSL certifikat itd. Konfiguracijske parametre nikako ne bi smjeli „zapakirati“ unutar same aplikacije. Samo ime „konfiguracijski“ naglašava da se radi o parametrima koji se mogu mijenjati ovisno o različitim verzijama aplikacije, okolini, da li se radi o produkcijskoj ili testnoj aplikaciji itd. Iako se konfiguracijski parametri mogu „zapakirati“ u samu Docker sliku prilikom kreiranja slike, ovo svakako nije preporučljivo i Kubernetes sustav pruža bolji način korištenja istih. Razlog više je i taj što je velika većina Docker slika javno objavljena na Docker registar slika te će svi moći vidjeti konfiguracijske parametre što svakako nije poželjno ukoliko se radi o osjetljivim informacijama kao što su korisničko ime i lozinka.

Kubernetes sustav nam omogućava da svakom containeru unutar Pod-a dodijelimo vlastite konfiguracijske parametre tj. okolinske varijable (engl. environment variables) (Slika 5.12).

A close up of a logo

Description automatically generated

Slika 5.12 Svaki container može imati svoje parametre [3]

Postoji više načina kako je ovo moguće napraviti, a u sklopu ovog diplomskog bit će objašnjen samo najpreporučljiviji način.   
Prvi korak je kreiranje ConfigMap resursa specificirajući yaml opisnu datoteku.

apiVersion: v1

data:

 PORT: 3000

kind: ConfigMap

metadata:

  name: my-config

Uočavamo da je opis ConfigMap resursa prilično jednostavan. Najvažniji dio datoteke je polje „data“ koje sadrži okolinske varijable. Tu se mogu specificirati sve potrebne varijable, a u ovom primjeru dana je samo jedna varijabla „port“ sa vrijednošću 3000. Datoteku je nakon kreiranja potrebno objaviti na Kubernetes glavni čvor sa već dobro poznatom naredbom: „kubectl apply -f ./[ime-datoteke.yaml]“.

Da bi koristili okolinsku varijablu PORT iz kreiranog ConfigMap resursa u opisu containera moramo dodati sljedeći dio koda:

spec:

 containers:

 - image: some-image

 envFrom:

 - prefix: CONFIG\_

   configMapRef:

     name: my-config

Novi dio koda je samo ovaj dio od „envFrom“. Na taj način kažemo containeru odakle da uzme okolinske varijable. Budući da smo ConfigMap resurs nazvali „my-config“ pod „configMapRef“ sekcijom smo stavili isto to ime. Polje „prefix“ je opcionalno i koristeći ovo polje sve okolinske varijable iz ConfigMap resursa će dobiti prefiks CONFIG\_. Sada ćemo moći koristiti varijablu PORT unutar containera tako da joj pristupimo preko imena CONFIG\_PORT. Ukoliko se radi o NodeJs aplikaciji, okolinskoj varijabli pristupamo na način: process.env.CONFIG\_PORT.

Korištenjem ConfigMap resursa možemo mijenjati vrijednosti okolinskim varijabli bez potrebe za ponovnim pokretanjem aplikacije tj. svih containera i Pod-ova. Na ovaj način znatno je olakšan i ubrzan proces testiranja i samog razvoja aplikacije, a isto tako okolinske varijable su zaštićene od neovlaštenog pristupa.

Ukoliko je potrebno veća doza sigurnosti okolinskih varijabli postoji resurs koji se naziva Secrets. Secret resurs je vrlo sličan ConfigMap resursu te se kreira i koristi na potpuno identičan način s dodatnim naglaskom na sigurnost. Tako se ovaj resurs kreira na radnom čvoru Pod-a koji ga koristi i nikad se ne zapisuje na disk nego se izvršava u radnoj memoriji. Također, Secret resurs je za razliku od ConfigMap resursa enkriptiran.

# AUTOMATSKO SKALIRANJE

# CHAT APLIKACIJA

# ZAKLJUČAK

# LITERATURA

[1] „Dive Into Docker“, s interneta, <https://diveintodocker.com/?utm_source=nj&utm_medium=youtube&utm_campaign=virtual-machines-vs-docker-containers>, 26. svibnja 2020.

[2] „10 companies that implemented the microservice architecture and paved the way for others“, s interneta, <https://divante.com/blog/10-companies-that-implemented-the-microservice-architecture-and-paved-the-way-for-others/>, 27. svibnja 2020.

[3] Marko Lukša, „Kubernetes in Action“, Manning, NY, 2018.

[4] „What is Kubernetes?“, s interneta, <https://linuxhint.com/what-is-kubernetes/>, 28. svibnja 2020.

# POPIS OZNAKA I KRATICA

Ops – Information-technology operations  
HTTP - HyperText Transfer Protocol  
TCP – Transmission Control Protocol  
AMQP – Advanced Message Queueing Protocol  
VM – Virtualna Mašina  
OS – Operacijski Sustav  
API – Application Programming Interface  
itd – i tako dalje  
sl – slično  
SSD - Solid-state Drive  
HDD – Hard Disk Drive  
GKE – Google Kubernetes Engine

# SAŽETAK