Redovisningar

# Kmom01

1. Vad var din uppfattning av devops för en vecka sen?

Min uppfattning bestod av att tillhandahålla ett repo för att dela med sig av källkoden. Denna kod ska sedan integreras i någon tjänst som bygger repot och testar det, precis som det sker lokalt. Man ska försöka automatisera dessa processer och underlätta så mycket som möjligt för hela teamet.

1. Har det ändrats efter denna veckan?

Inte någon större skillnad, då vi fått smaka lite på det i Emils jsramverk kurs. Vi har redan pushat till vårt repo, driftsatt på en server i något moln, och integrerat samma repo i en CI tjänst. Jag ser inte någon speciell skillnad ännu. Python har ersatt JavaScript. Flask med Jinja Node.js med Express. Azure istället för DigitalOcean. Men jag tror att vi kommer lära oss mycket mer i den här kursen.

1. Hur skulle du definiera devops?

Jag tror inte man kan riktigt bestämma en slutlig definition. För man hittar ständigt nya lösningar. Men om jag får välja hur jag ser på det; hitta ett sätt att automatisera och effektivisera delning av kod. Denna kod skall automatiskt byggas och testas för att se att den verkligen fungerar. När detta har skett skall det per automatik igen driftsättas. Så få manuella, mänskliga aktörer möjligt. Helt enkelt, automatisera och effektivisera vad kunden vill ha.

1. Finns det något speciellt du vill lära dig i denna kursen?

Kan inte svara på det. Det viktiga är väl att lära sig ett sätt att klara av föregående fråga så smidigt som möjligt. Annars, Python uppskattas alltid, och det med nya teknologier för att köra både på server- och klientsidan.

1. Vad tycker du om kmom01’s upplägg och storlek?

Det kan verka skrämmande. Långa scrollar brukar ge ett sådant intryck. Lång scroll dock, kan jag ta, för guiderna är alltid guld värda. Vad jag dock fruktar mer är utvecklingsmiljön eller sådant som måste fungera men strular, och det redan i början, och det pga. andra faktorer studenten inte kan påverka. Det viktigaste för läraren är att sätta sig in i studentens värld. Tex. se till att läraren skapar en liknande utvecklingsmiljö studentens. Om läraren inte tänkt på det, min TIL till honom vore: Skaffa ett konto på skolan som motsvarar en vanlig students. På detta sätt, testa skapa vad uppgifterna kräver på molnet, tex. Azure och se ifall processen funkar. Strular det slipper eleverna vänta och kanske hamna i viss frustration.

# Kmom02

1. Har du använt Docker förut? Gick det bra att använda det nu?

Lärde mig det i Kenneths kurs. Har börjat ogilla att utveckla i Windows miljön mer och mer. Ett tag tillbaka föredrog jag, om jag minns rätt, Windows miljön framför open source miljlön. Börjar njuta mera av Linux nu. Hade problem att installera Docker Desktop, så fick skapa en virtual image och gå ifrån WSL. Men igår efter jag installerade det på laptopen hoppade det även igång i min lilla NUC som jag använder till mina studier. Men installera i Linux har funkat bra. Annars funkade det bra att använda självaste Docker.

1. Valde du att bygga ny Docker image vid varje commit eller release? Varför?

Jag provade mig fram, för jag tyckte att vid en ny tag (release) borde det räcka med att bygga image:n. Men jag fick det inte att funka, fast jag kollade deras manualer. Jag testade bara att det skulle köras vid senaste taggen, v2.0.0 genom tag:\n\t only: /^v2/. Men då körde han det alltid för default är att köra alla branches. Svepte jag bort alla branches, tex. branches: \n\t ignore: /.\*/ och körde med tag kommandot nyss nämnt då stoppade det hela bygget, vilket är odugligt, för jag vill ju testerna ska gå igenom och bygget börja vid version 2. Kanske om jag börjar använda mig av olika branches? Jag tänkte även testa ren bash kod för att kolla Circles miljövariabler för branch och tag, men som min konfiguration ser ut, så kommer det inte att gå då ett fel ”exit 1” kommer matas ut ifall taggen inte stämmer, och då avbryts ju hela byggandet. Jag försökte olika workflows, men det verkar som det blir två skilda byggprojekt så att den ena inte har något med den andra miljön att göra.

1. Vad är Continuous Delivery?

Jag läste frågan som Continuous Deployment ett tag. Jag ser det som att automatisera flödet (pipeline) över hur man publicerar sin applikation. Det gäller att hitta ett effektivt sätt att testa koden och när den är godkänd transformera den till ett stadie där den är redo att bli driftsatt i produktion.

1. Uppdaterade du deploy skripten med Docker?

Jag förstår inte frågan? Jag chansar. Jag kickar igång min produktionsapp genom docker containers skapade i docker-compose filen som hänvisar till Dockerfile\_prod.

1. Hur var storleken på kursmomentet? Vad tycker du om upplägget på kursmomentet?

Det här momentet kändes ganska stort. Om man fastnar här så är det inte roligt. Jag fick tyvärr spendera antalet onödiga timmar på annat då Docker inte ville sig i Windows. Jag gillar inte en container i min utvecklingsmiljö. Jag försår för att förenkla för andra utvecklare. Men min definition av Separation of concerns är synonymt med Low Coupling och High Cohesion. Varje del på sin plats. Annars, att ha en runtime container som snurrar på servern är ljuvligt. Jag hade tänkt mig, enkla tankar från en enkel man, att om man skulle starta eget företag, så skulle man nog tjäna in mycket pengar genom att bygga stuket på sina servrar efter detta kursmoment (och givetvis, det betyder inte att senare moment uppdaterar detta stuk ännu bättre). Att ha olika VMs som kör sina appar i containers är billigare än att ha det äldre sättets servrar på. Denna slags devops gör att man smidigare kan hantera flera appar (flera kunder) på en och samma virtuell maskin.

1. Veckans TIL?

Måste vara produktionsappen i en container. Undvik Microsoft tjänster så mycket som möjligt.

# Kmom03

* Vad är IaC?

Infrastructure-as-Code betyder att skapa källkodsfiler som bygger upp ens olika utveklingsmiljöer, ens infrastruktur. Genom detta sätt får man ett enkelt och konsekvent sätt att från enkla filer bygga hela servrar med dess olika program från ingenting.

* Vad är CM?

När det handlar om att automatisera skapandet av sin infrastruktur använder man sig av configuration management (CM). Man kan även se det som att systematiskt hantera förändringar i sin infrastruktur som bevarar integriteten över sina system. Om man skulle göra några ändringar i någon server, så använder man sig av ett CM verktyg, vilket innebär att den servern, genom IaC, kommer bevara de ändringar gjorda till kännedom för alla, då man inte går in och pillar själv.

* Vad är Continuous Deployment?

För att ständigt uppdatera sina produktionsapplikationer efter godkända genomförda tester så slänger man upp den till respektive server. Givetvis, detta sker per automatik genom olika verktyg. Genom oftare leveranser pga. automatiken kan man tidigare upptäcka fel i sina produktionsapplikationer.

* Om du fick välja fritt hur hade du valt att bygga upp CD kedjan?

Inte så säker, väldigt ny i tekniken. Hade nog valt att dela upp flera applikationer i olika containers. Kanske se till att köra flera kopior av samma appar för att sedan stänga ner vissa och ersätta med de nya och uppdatera de resterande.

* OBS! Problem i kursmomentet nedtecknade.

1. Jag fick problem med att kommunicera min microblog app med databasen som kör en mysql docker container på databasservern (dbs). Ständigt när man besöker sidan får man ”502 Bad Gateway nginx/1.18.0”. Stänger jag ner databascontainer (dbc) funkar appen, utan att spara till db. När jag kollar i dbc så ser jag att databasen och tabellerna skapas som de ska, men det är som någon slags restriktion hindrar. Ibland fick jag kontakt med dbc genom appen, och då funkade det även att spara i db. Men detta var oftast genom att man gjorde en slags docker exec --it mysql mysql –u<…> -p<…> och sen körde något statemenet i servern, som tex. ”use database microblog” så fungerade det. Men efter en viss inaktivitet la uppkopplingen till dbs ner och jag fick samma felmeddelande i webbläsaren. Men nu fungerar det inte. Efter ett par dagars felsökande gav jag upp. Jag har dock lärt mig att genom IaC och CM skicka med en dbc på databasservern. Kanske om man kunde byta database provider skulle det gå lättare? Kommandot jag kör för att starta de olika containrarna finns i mina .yml filer för respektive server (database och appServer). Jag har även testat att köra/starta om containrarna direkt på servrarna.

2. Självaste testerna går igenom på CircleCi, men inte när jag ska deploya microblogsappen på appServer genom CircleCI. Jag har lagt till env. variablerna ”AZURE\_AD\_USER, AZURE\_PASSWORD, AZURE\_SUBSCRIPTION\_ID” i mina inställningar för projektet. Alla steg funkar förutom att deploya genom Ansible. Lokalt funkar det med samma ansible kommando. Det felet jag fick kan ha att göra med AZURE\_AD\_USER, då jag använt mig av först ”krmn18” och sedan hela email adressen ”krmn18@student.bth.se”. Vet inte vad det ska vara för värde? I min config.yml fil för CircleCI har jag även med:

- add\_ssh\_keys:  
 fingerprints:  
 - "b7:35:a6:4e:9b:0d:6d:d4:78:1e:9a:97:2a:66:6b:be"

för min deploy\_appServer build.

Felet jag får är:

ansible-playbook 2.9.13  
config file = /home/circleci/project/ansible/ansible.cfg  
configured module search path = ['/home/circleci/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']

ansible python module location = /home/circleci/project/.venv/lib/python3.8/site-packages/ansible  
executable location = /home/circleci/project/.venv/bin/ansible-playbook  
python version = 3.8.5 (default, Sep 28 2020, 18:14:32) [GCC 9.3.0]

Using /home/circleci/project/ansible/ansible.cfg as config file  
Parsed /home/circleci/project/ansible/hosts inventory source with ini plugin

PLAYBOOK: gather\_vm\_instances.yml \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
1 plays in gather\_vm\_instances.yml  
PLAY [local] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
META: ran handlers  
TASK [gather\_vm\_instances : Get facts by tags] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
task path: /home/circleci/project/ansible/roles/gather\_vm\_instances/tasks/main.yml:2  
Using module file /home/circleci/project/.venv/lib/python3.8/site-packages/ansible/modules/cloud/azure/azure\_rm\_virtualmachine\_info.py

Pipelining is enabled.  
 <localhost> ESTABLISH LOCAL CONNECTION FOR USER: circleci  
<localhost> EXEC /bin/sh -c '../.venv/bin/python && sleep 0'

CircleCI received exit code 2

# Kmom04

1. Beskriv vad som menas med Monitoring, olika saker som brukar övervakas och vad det används till.

Monitoring innebär att övervaka ett system med dess olika processer. Denna övervakning leder till en kännedom över vad som händer inom detta system. Saker som jag själv testat på att övervaka är webbservern, databasen, och applikationen. Detta används för att upptäcka när något händer i vårt system, tex. webbservern går segt eller någon funktion på sidan inte fungerar. En annan sak det kan användas till, oftast under en längre tid, eller om man väljer att gå tillbaka i tiden, är vad som sker i systemet eller hur användarna använder det.

1. Beskriv Log management och vad det används till.

Log management, eller hantering av loggar, handlar om att samla in, lagra, analysera och hantera logg data. Logghanterare hjälper till att bestämma vad man behöver logga, hur man ska logga det och tex. hur länge sådan information skall behållas. Det är ett bra sätt att ha koll och sköta sina loggar på.

1. Beskriv APM vad det används till.

Application performance monitoring (APM), handlar om att övervaka prestanda och användarupplevelsen hos applikationer för att möta vissa kriterier. Det används för att undersöka ifall en applikation inte beter sig som förväntat, varför den gör det. Man använder sig av olika APM tillvägagångssätt, såsom pinga applikationen, mäta data ifrån servern, tex. dess CPU, minne, mm.

1. Beskriv Observability och försök koppla det till ovanstående frågor.

Genom att observera de värden man får ifrån ett, tex. övervakningssystem, kan man avgöra hur ett system mår. Man vill ta reda på vad som försiggår genom att studera den data som är samlad. Detta kallas för observability. Övervakningssystemen klagar när de vet hur att klaga. De har fått värden redan förutbestämda som säger ”vid denna uppnådda gräns, klaga”. Men hur ska man klaga på fel vi inte känner till finns, till att börja med? Jag tror att man observerar värden för att förhindra just dessa ”unknown unknowns”.

1. Vad är dina tankar om Prometheus och Grafana?

Jag tycker det är coolt. Det här är första gången jag kommer i kontakt med någon form av övervakningssystem över mitt egna system. Och så har jag med lärarens hjälp implementerat det. Jag ser bara fördelar. Jag kan inte yttra mig så mycket heller om det, då jag är helt ny till dessa tekniker.

Grafana: https://manczak.me/grafana/  
Logins: Ange logins här.

https://www.manczak.me/  
<https://github.com/kryman0/devops>

# Kmom05

1. Varnade Snyk om några paket som ni behövde uppdatera?

Samma som guiden fick, musl-utils. Jag fösökte få till detta genom att använda en senare version av alpine. Anledningen var för i varningsmeddelandet stod det att en ordnad version skulle vara 1.1.24-r10. Denna kollade jag fanns i en senare version av alpine. Men jag fick fortfarande samma fel.

1. Ändrade ni något i er kod efter ni kört Bandit? Använder ni # nosec för att ignorera någon kod eller skippa något test? Varför?

Jag lade till nosec kommentaren genom att ändra i app/models.py rad 68. Jag fick även skapa en konfigurationsfil för att skippa B101 varningar. Det var dessa som tog upp flest varningsmeddelanden: ”The enclosed code will be removed when compiling to optimised byte code.” Man kanske använder assert på fel sätt?

1. Beskriv vilka Zap varningar ni fixade och hur ni löste dem.

WARN-NEW: X-Frame-Options Header Not Set [10020] fick jag bort genom att lägga till ”add\_header X-Frame-Options SAMEORIGIN;”.

WARN-NEW: X-Content-Type-Options Header Missing [10021] försvann när jag la till ”add\_header X-Content-Type-Options nosniff;”.

WARN-NEW: Strict-Transport-Security Header Not Set [10035] försvann när jag tog bort subdomänerna (har nog ingen betydelse) och lade till ”always” i slutet. Jag la till ”always” annars skickar han enbart ut ett svar när responskoderna är typ under 400.

WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] ordnade jag med “add\_header Content-Security-Policy "default-src https:;" always;”. Fast med denna tillkom ännu en WARN-NEW: CSP: Wildcard Directive [10055] som jag lät vara. Det kanske har att göra med att sätta de andra direktiven också, såsom script-src, img-src, mm.? De flesta borde dock följa med om man sätter en default directive. OBS! Jag blev tvungen att kommentera bort header:n den för jag kunde inte komma åt grafana.

WARN-NEW: Incomplete or No Cache-control and Pragma HTTP Header Set [10015] försvann genom “add\_header Cache-Control "no-cache, no-store, must-revalidate";”. Den här var valfri ”add\_header Pragma no-cache;” men de skriver att man ska lägga till den.

Om man ska få bort cookie varningarna behöver man installera cookie\_flag modulen som finns på https://github.com/AirisX/nginx\_cookie\_flag\_module.

1. Gick det bra med SSH konfigurationen?

När jag ändrade på loadBalancer frös min loadBalancer instans efter ett tag. Jag förstod inte varför så jag startade om servern, men det gick inte att komma åt den (kanske jag var för snabb och den inte startade igång riktigt?). Dock, en stund senare, av sig själv, hoppade den igång igen. Märkligt beteende.

1. Hur skulle du definiera DevSecOps och dess roll inom devops?

DevSecOps innebär att säkerheten blir en aktiv del av utvecklingsprocessen. Det betyder att säkra applikationen innan den byggs färdig. Vanligtvis brukade man tänka på att säkra produkten när den blev klar, men med DevSecOps vill man bygga in säkerheten i produkten.

1. Var skulle du säga att vi har den största säkerhets risken i vårt system och infrastruktur?

Jag tror elevated privileges är något man måste undvika. Hur uppkopplingen sker mot vår infrastruktur (instanser) är också något viktigt att tänka på. Och otillräcklig logging är något man måste undvika. Med otillräcklig menas också att inte ge ut några varningsindikationer vid misstänkt aktivitet.

# Kmom06

1. Vad är ert första intryck av Kubernetes? Skulle ni vilja använda det i framtiden?

Jag vill påminna läsaren om att jag är ganska ny inom K8s världen. Så en del av det jag skriver är ifrån andras åsikter, ifrån sidor läraren länkat till. Jag har inte den erfarenheten att praktiskt göra bedömningen och urskilja vad sidorna pratar om alltid är den bästa lösningen. Men det jag skriver ner förstår jag, inte nödvändigtvis allting, och tycker det låter förnuftigt.

Första intrycket lär nog ge en del komplexitet om det. Det är ganska nya termer och koncept man inte får med sig av att enbart använda Docker. Detta kan kännas svårt att skilja på de olika delarna för att få en fungerande deployment.

Om man inte vill använda det skulle man bli tvungen till det. Jag har inga problem att använda K8s. Desto mer man använder det, desto smidigare blir det.

1. Vad är Container orchestration?

När vi tittar på en hamn så ser vi att containrarna behandlas efter ett visst system, mönster och struktur (jag hoppas det iaf., då jag inte vill påstå jag är någon hamncontainerarkitekt). Man kan väl definiera detta på liknande sätt inom mjukvaruvärlden där mikrotjänster (microservices) körs som applikationer i runtime containrar. Dessa containrar behöver hanteras på ett visst sätt. Meningen är att hantera deras tillförlitlighet, minska/öka deras antal, förflyttandet av dem, hur mycket resurser de ska ta, mm. Med andra ord, kontrollera deras livscykel.

1. Varför är det svårare med stateful applikation jämfört med stateless i k8s?

Då stateful oftast handlar om att lagra data ifrån en applikation, så måste man tänka på hur man ska lagra denna data, och vart. Risken finns alltid att applikationen, poden, går ner och data förloras om man inte valt att spara data. Detta, när data lagras i en databas, skulle vara katastrofalt. En stateless applikation, som kunde bry sig mindre om hur många gånger den startas om, hoppar alltid igång till det stadie den var skapad till utan att någon användare verkligen känner av det, för den behöver inte lagra något ifrån sin sida vars information skulle vara viktig. En annan sak att tänka på, som är viktigare, när det kommer till en databas, handlar bla. om att synkronisera data ifrån de olika stateful applikationer, för att vara konsistenta med att ge ut senaste data.

1. Vad ska vi tänka på när vi designar ett projekt som ska köras i K8s?

Med K8s tror jag det handlar främst om förmågan att skala horisontellt, att justera antalet kopior av ens applikation som tar hand om belastningen och tillgängligheten. Då naturen av K8s handlar om containerisad miljö, så gäller det att satsa på, som jag kallar det för, containeriserad low coupling och high cohesion. Low coupling och high cohesion är inom objekt orienterad design ett sätt att låta varje klass utföra sin funktion den är menad till, och inte beblanda sig med andra, då det blir svårare annars att ändra i koden. Låt därför varje mikrotjänst sköta sin funktion den är menad till i sin egen container.

Sen handlar det om hur man ska tillhandahålla detta, och hur man ska gå tillväga när man bygger upp sitt projekt. Istället för att nämna alla punkter i de tolv faktorerna, där vissa vi redan lärt oss i DevOps, kanske man kan göra någon slags sammanfattning. Man ska fokusera på applikationernas huvudsakliga uppgifter, ta i beaktning driftförhållandena mellan komponenterna, och ha något slags förutsägande system hur containrarna kommer bete sig i K8s.

1. Vad är viktigt att tänka på när man ska köra K8s i produktion?

Att bla. inte försöka jobba på samma sätt som när man gör lokalt, eller i en dev/test miljö. Det gäller att styra upp sin K8s infrastruktur. Viktigt att tänka på är loggning och monitoring. Öka säkerheten följer med. Se till att inte använda inofficiella Docker images och se till att skaffa en privat registerserver för Docker images. Andra säkerhetsaspekter att tänka på är autentisering såsom multifaktor och specifika protokoll. Rollbaserad åtkomstkontroll får heller inte glömmas bort. Load Balancing och Ingress ska betänkas. Man måste även ha i åtanken hur man ska konfigurera sin infrastruktur när nya versioner släpps där man måste uppgradera sina produktionskluster och se till att undvika så mycket driftstopp som möjligt. Managed services ska tydligen enligt en sida vara något väldigt viktigt. Detta beror på hur mycket man känner till sin infrastruktur i K8s, anser jag.

1. Hur känns det efter att ni använt K8s, var det lika svårt som alla skriver/säger att det är?

I början kan det kännas tungt, med de olika koncepten och strukturen. Men desto mer man knappar på det och läser om det, desto enklare blir det. Jag förstår vad en Deployment är, varför man skapar Services för att utsätta sina applikationer för åtkomst utanför klustret. Ingress funkar som en fin routing för olika delar (paths) inom domänen. När jag skapade min Microblogg i K8s så försökte jag hålla mig till deras manual, API referens (https://kubernetes.io/docs/reference/generated/kubernetes-api/v1.20/). Jag föredrar referenser som är väldigt tydliga och säger vilka objekt/properties är obligatoriska att använda i sin konfigurationsfil. I det här fallet var K8s referens inte så duktig på just den biten.

Det kändes bra att jobba med K8s fast det tog några timmar att få till bloggen. Första steget var att få till en giltig konfigurationsfil utan valideringsfel. Det andra steget var sen att få filen att göra som man skapat den till att göra. Det sista steget var att få filen att kommunicera med andra filer. Dessa olika steg kan verka jobbiga, mindre jobbiga, att få till.