STATENS IT

Servicespecifikation

GovCloud

Februar 2024

Indhold

1 Formål og indhold

Dette dokument beskriver de kundevendte komponenter, som indgår i Statens Its GovCloud-platform, som udelukkende driftes internt i Statens Its egne datacentre. Dokumentet beskriver:

- GovCloud-arkitekturen
- De komponenter som udgør GovClouds eksekveringsplatform
- De komponenter som indgår i GovClouds toolchain.

Dokumentet retter sig særligt til projektledere, lead-udviklere og andre, som skal udvikle løsninger til GovCloud-platformen, fx i forbindelse med valg af udviklingsmetoder, udviklingsværktøjer og udviklingskompetencer i en projektplanlægningsfase.

2 GovCloud

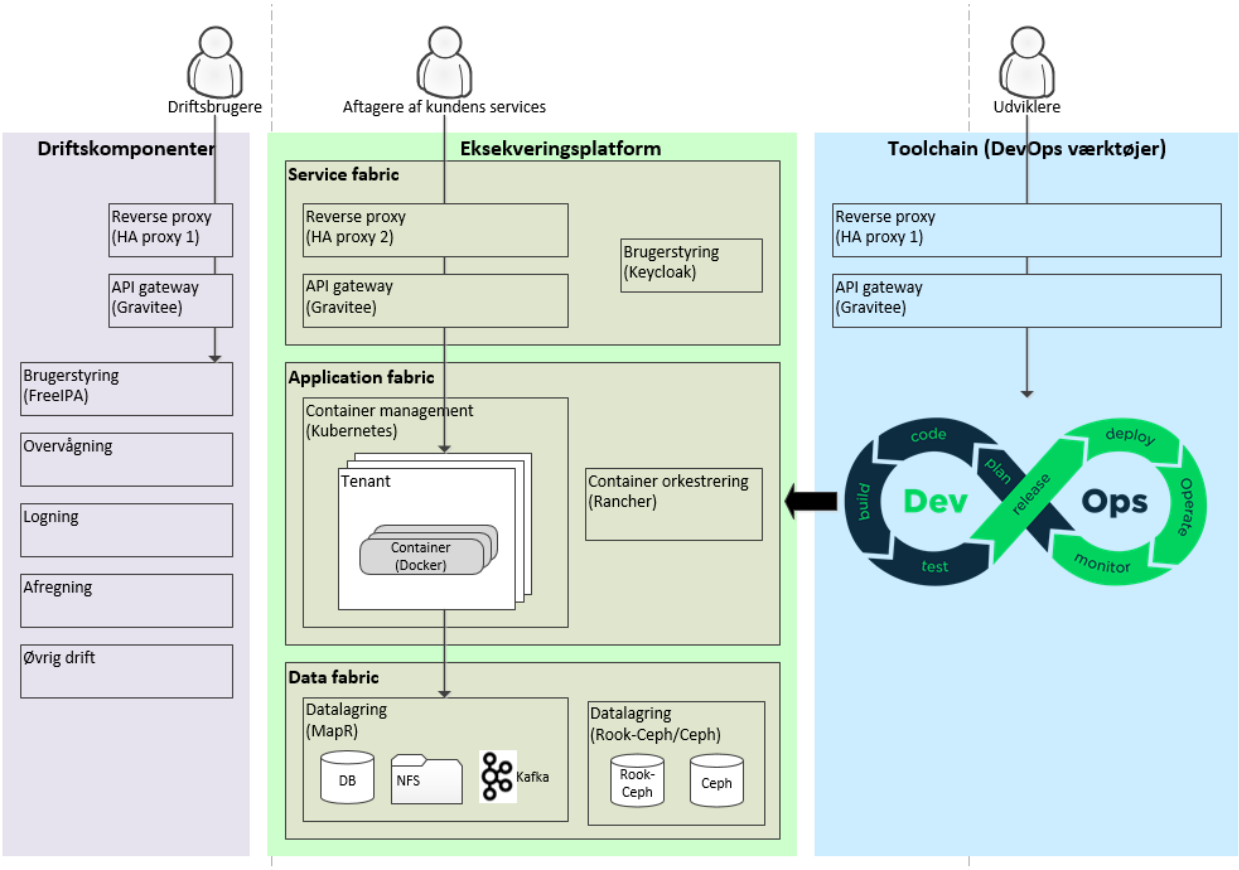
GovCloud er en Platform as a Service (PaaS), som tilbyder cloud-baseret on-premise-drift vha. container-teknologi. GovCloud tilbyder desuden en række værktøjer (toolchain), som kunderne kan benytte til at udvikle applikationer, eventuelt efter DevOps-metoden.

GovCloud består af mange forskellige komponenter, som primært bygger på open source-produkter. Platformen indeholder dog også nogle proprietære produkter, som er bygget på helt eller delvist open source-software.

GovCloud består overordnet af følgende dele:

- **Eksekveringsplatform** – den del, som står for at eksekvere container-baserede applikationer, gemme resultater og data og udbyde services via internettet
- **Toolchain (DevOps-værktøjer)** – værktøjer, som kunderne kan bruge til bl.a. at udvikle, teste og monitorere applikationer, som skal eksekveres på eksekveringsplatformen
- **Driftskomponenter** – komponenter som benyttes af Statens Its driftspersonale til at administrere og drive GovCloud-platformen.

Komponenterne og deres funktion fremgår af figur 1 nedenfor.



Figur 1 – GovCloud er sammensat af en række komponenter, hvor en del stilles til rådighed for Statens Its kunder, så de selv kan udvikle, deploy'e og drifte deres applikationer.

I de følgende kapitler er de kundevendte komponenter, som indgår i GovCloud-platformen (dvs. eksekveringsplatform og toolchain), beskrevet.

Driftskomponenterne, som ikke bruges af kunderne (men kun af Statens It), er ikke beskrevet i dette dokument.

3 Eksekveringsplatform

Eksekveringsplatformen giver mulighed for at eksekvere container-baserede applikationer, gemme og hente data, udbyde services fra kundeapplikationer til internettet og for at administrere platformen.

GovClouds eksekveringsplatform (også kaldt Compute Fabric) består af:

- Service Fabric, der muliggør at kundernes applikationer kan tilgås af eksterne serviceaftagere via internettet.
- Application Fabric, som står for deployment og eksekvering af container-baserede applikationer med automatisk skalering efter behov.
- Data Fabric, som gør det muligt for applikationerne i Application Fabric at gemme og hente permanente data i databaser og andre dataservices.

Kritiske komponenter er dublerede og indeholder en høj grad af redundans, hvilket muliggør en meget høj oppetid.

3.1 Service Fabric – for alle kunder

Dette afsnit beskriver indholdet af Service Fabric, der er tilgængeligt for alle kunder. Der kan tillige findes konkrete komponenter, der er knyttet til den enkelte kunde alt efter kundens behov. Statens It har ansvar for vedligehold af Service Fabric tilgængeligt for alle kunder.

3.1.1 HAProxy

HAProxy er en transparent reverse proxy, som giver eksterne serviceaftagere adgang til de kundeapplikationer, som udstilles via GovCloud. HAProxy anvendes således til at etablere adgang til interne services.

HAProxy indeholder desuden en load balancer, som kan fordele forespørgsler på tværs af flere containere beliggende på én eller flere hosts.

3.1.2 Keycloak

Keycloak er en Secure Token Service (STS), der kan udstede SAML-, OpenID/OAuth- og JWT-tokens til brug i de udstillede services. Keycloak muliggør single sign-on med identitetsstyring og adgangsstyring og kan således benyttes til at regulere brugernes adgang til kundernes udstillede applikationer.

Til styring og administration af kundernes applikationer vil Keycloak indeholde specifikke realms til hver kunde (tenant) med mulighed for opkobling til eksterne autentificeringsservices, såsom NemLogin.

Login til både GovCloud-services og til de services, der udvikles af kunden til eksterne serviceaftagere, kører så vidt muligt gennem en central login-service (Gravitee.io), som bestyres af Keycloak.

3.2 Application Fabric

3.2.1 Rancher

Parametrene til afvikling af containere styres gennem Rancher, der overfører disse parametre til Kubernetes, der så efterfølgende agerer efter de opsatte parametre, uafhængigt af Rancher. Kubernetes kan i GovCloud tilgås direkte via et command-line tool, kubectl, men administreres også gennem Ranchers user interface/UI eller command line interface/CLI. Rancher understøtter Role Based Access Control (RBAC) mod Kubernetes.

Rancher kan herudover monitorere/overvåge deployments i Kubernetes.

Rancher anvender Keycloak som adgangskontrol.

3.2.2 Kubernetes

Kubernetes står for deployment og eksekvering (drift) af kundernes applikationer i GovCloud. Applikationerne afvikles ikke på én host, men på en sværm af hosts, hvor applikationerne ikke er bundet til bestemte hosts.

Kubernetes anvender internt Docker til afvikling af Docker-containere. En Docker-container er den mindste enhed til eksekvering af en samlet løsning.

Containeren afvikler én proces og indeholder hele den stak, der skal til, for at køre processen; det vil sige styresystem, middleware, runtime environment mv. Hvis processen fejler eller på anden vis standser, kan Kubernetes selv starte en ny container op. Tilsvarende kan den enkelte container også skaleres op eller ned, hvis belastningen hhv. overstiger eller kommer under en vis grænse.

I Kubernetes samles Docker-containere i ”Pods”. En Pod er en samlet logisk enhed, bestående af én eller flere containere, der deploy’es sammen. Containerne i en Pod deler name space, netværk, og andre parametre. Pods har fastsat en række parametre for genstart og ressourceforbrug, som Kubernetes agerer ud fra. Deployment og den til tider komplekse sammenhæng mellem parametre og Pods indbyrdes styres af Rancher. Som udgangspunkt, for at undgå unødig kompleksitet, arbejdes der i GovCloud som regel med én container per Pod.

3.3 Data Fabric

Alle data, der ligger i en container, er flygtige (transiente) og vil forsvinde, når containeren genstartes. Containere indeholder således ikke selv permanente (persistente) data, men gemmer alle sine data uden for containeren i Data Fabric, som deles mellem alle containere i alle miljøer. Data Fabric i GovCloud udgøres af:

- MapR, der er et kommercielt storage system der understøtter blok, file og objekt lagring.
- Rook Ceph, der er et open source-storage system, der ligeledes understøtter blok-, file- og objekt-lagring. Ceph har et Backup-system knyttet, hvor der tages daglig backup af volume, som så opbevares i Statens Its backup-infrastruktur.
- Rook er en open source cloud-native storage-orchestrator, der leverer platformen, rammerne og supporten til Ceph storage til at integrere med cloud-native miljøer.

3.3.1 MapR

MapR er en overbygning på Apache Hadoop. I GovCloud tilbyder MapR følgende datalagringsfunktionalitet:

- NFS - Network File System, et distribueret filsystem, der tillader klienter at tilgå filer og volumes over et netværk.
- OJAI - Open JSON Application Interface, en såkaldt "no-SQL" database til strukturerede data. OJAI er baseret på JSON.
- Kafka - Apache Kafka er en distribueret streaming-platform.

Data ligger ikke på én bestemt harddisk eller én bestemt host, men lagres på en sværm af hosts, hvor data ikke er bundet til bestemte harddiske eller hosts.

MapR kører på 12 fysiske servere, som synkroniserer data. Denne synkronisering gør, at der så godt som ingen risiko er for datatab ved en driftshændelse på storage infrastrukturen. MapR kan betragtes som et high availability og high output storage-system.

MapR er dynamisk skalerbar op og ned. Dvs. kundernes applikation dynamisk kan forbruge af den lageringskapacitet, der er til rådighed i MapR-infrastrukturen. Ligeledes kan der slettes data gemt i MapR. Nærmer forbruget sig den fysisk tilgængelige kapacitet, øges denne proaktivt.

Afregning af MapR lagerforbrug sker på baggrund af et kvartalsmæssigt snapshot af det aktuelle forbrug, der så anvendes som "fladt forbrug" for det pågældende kvartal.

3.3.2 Ceph storage

Ceph er et open source-storagesystem, der understøtter blok-, file- og objekt-lagring.

Ceph storage allokeres til de enkelte containere/pods som en fast allokering. Typisk vil der i en applikation være en "service pod", der står for læsning/skrivning til Ceph storage, og det er denne "service-pod", hvortil der allokeres Ceph storage.

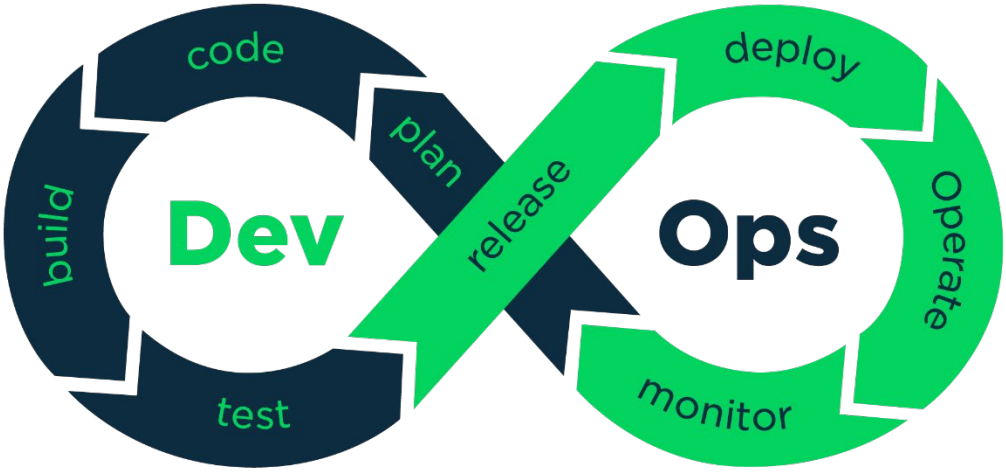
Storage-allokering kan på enkel vis øges via selvbetjening i Kubernetes K8S. Poden skal dog genstartes, før den øgede allokering er effektiv. Opmærksomheden henledes på, at applikationen kun kan anvende den allokerede storage, og det er derfor tilrådeligt, at der implementeres en overvågning af Ceph storage-forbrug i applikationen.

Afregning af Ceph storage sker på baggrund af den allokering, der er tildelt. Reduktion af Ceph storage er ikke muligt som selvbetjening i Kubernetes. Reduktion af Ceph storage kan kun foretages som en bestillingsopgave, og denne medfører nedetid for applikationen.

Ceph har et backup-system tilknyttet, hvor der tages daglig backup af volume, som så opbevares i Statens Its backup-infrastruktur.

4 Toolchain (DevOps værktøjer)

GovCloud udstiller en toolchain (en samling af værktøjer), som understøtter DevOps. DevOps er en sammentrækning af Development og Operations (udvikling og drift) og er en metode, som understøtter de processer, som indgår i udvikling og drift, fra planlægning, over udvikling og test til produktion og overvågning.



Figur 2 - GovClouds toolchain understøtter alle led i applikationsudviklings- og applikationsdriftsprocesserne.

De kunder, som bruger GovCloud, kan vælge helt eller delvist at benytte GovClouds toolchain til at udvikle, teste og monitorere applikationer, som skal eksekveres på GovCloud. De kan også benytte deres egen toolchain.

Værktøjerne i GovClouds DevOps toolchain understøtter følgende udviklings- og driftsprocesser:

- Kodning, build og test
- Release og deployment
- Drift og overvågning.

4.1 Planlægning

I planlægningsfasen defineres og dokumenteres de opgaver, behov og krav, som løsningen skal løse, så der løbende kan følges op på fremdriften. Ud fra et vidensdelingsperspektiv kan det desuden være en fordel at dokumentere beslutninger og designløsninger for at gøre dem let tilgængelige for alle, som på et tidspunkt skal arbejde med løsningen.

4.2 Kodning, build og test

GovClouds toolchain stiller værktøjer til rådighed for bl.a. kildekodeintegration, test, versionsstyring, build, dokumentation og issue tracking.

Til understøttelse af kildekodeintegration udbyder GovCloud værktøjer, der understøtter merge requests og systematisk review af kode, hvor deltagere i et udviklings-team kan vurdere ændringer i kildekoden, give feedback til udvikleren og enten godkende eller afvise ændringerne.

Til understøttelse af automatiseret test kan en build server være anvendelig. Et komplet miljø med testdata kan deploy'es og startes automatisk, og fejlende tests meldes tilbage til de udviklere, der har foretaget ændringerne i den testede version af softwaren.

4.2.1 GitLab

GitLab tilbydes som software repository med indbyggede funktioner for versionsstyring, dokumentation og issue tracking samt indbygget CI/CD[1] pipeline.

I GovClouds toolchain tjener GitLab flere formål. GitLab bestyrer først og fremmest det centrale Git repository og stiller funktionalitet til rådighed til at administrere dette repository. Disse funktioner dækker bl.a. over:

- Adgangskontrol – som sikrer, at identiteten af kilden til ændringerne er kendt
- Brugeradministration – som sikrer, at kun de af kunden godkendte ressourcer (brugere, systemer etc.) kan foretage ændringer
- Repository browser – som tillader visning af ændringer til kildekode-review uden anden installation af software end en browser.
- Merge request – som er en metode til forespørgsel om integration af en software-ændring i kildekoden, og som kan danne grundlag for et kode-review af ændringen.

GitLab indeholder desuden GitLab Runner, som indeholder en del funktionalitet, der til dels er dækket af andre værktøjer, men som her tilbydes i en letvægtsudgave. Disse inkluderer bl.a.:

- Problemhåndtering/Issue tracking – dette overlapper noget med Jira, men GitLab Runner er simplere og nemmere at tilgå, dog på bekostning af reduceret fleksibilitet
- Build server – denne funktionalitet overlapper med Jenkins, men GitLab Runner er enklere og mere direkte integreret med GitLab.

Adgang til det centrale Git repository i GovCloud (GitLab) foregår ved hjælp af Statens Its B- og X-konti og GovClouds STS (Keycloak). Herefter skal der tilføjes en SSH-nøgle, alternativt en adgangskode til basic authentication (https).

4.2.2 Git

Git anvendes til versionsstyring af det kildemateriale eller de artefakter, der udarbejdes manuelt af udviklingsteamet, såsom kildekode, grafik, websider, skabeloner, konfigurationsfiler, versionsafhængigheder, build jobs og scripts.

[1] Continuous Integration (CI) og Continuous Delivery (CD), er en praksis hvor udvikleren løbende (flere gange om dagen) integrerer kode til et fælles arkiv (repository) som straks, efter automatiseret test og build, bliver deploy'et i produktion.

Git kan vise ændringer i et udviklingsforløb, vise hvem der har lavet hvad, og der kan søges på, hvilke ændringer der er foretaget tættest på introduktion af en fejl. Git bliver på den måde ikke blot et redskab til versionsstyring, men et redskab til at kommunikere mellem udviklere om ændringer.

Git kan håndtere såvel tekstbaseret kildemateriale som binære filer (dvs. billeder, ikoner mv.). Selvom Git kan håndtere binære filer, så bør Git dog udelukkende anvendes til at lagre materiale, der er udviklet i projektet og ikke kan genskabes ad anden vej.

Git bør ikke anvendes til materiale, der er hentet fra nettet, binære moduler, færdig-build'ede komponenter, container images osv. Til disse artefakter er andre værktøjer som f.eks. jFrog Artifactory og Harbor bedre egnede.

Git er et produkt, der installeres på de enkelte udviklings-pc'er, som en del af den lokale udviklingsplatform. Det er således ikke et produkt, GovCloud leverer.

Adgang til det centrale Git repository foregår gennem GitLab.

4.3 Release og deployment

I en release (frigivelse) udvælges en bestemt version af applikationens underliggende software til at definere en ny applikationsversion, hvilken herefter kan deploy'es (idriftsættes/installeres) i et miljø (fx et udviklings-, test- eller produktionsmiljø). Release- og deployment-processen kan enten være manuel eller fuldt automatiseret.

En (produktions-)release er en færdig version af softwaren, som kan sættes i produktion og benyttes af slutbrugerne.

4.3.1 Harbor

Harbor er et container repository til Docker images, hvor container images lagres for senere deployment på en eller flere eksekveringsplatforme. Images i Harbor kan danne grundlag for nye images eller deploy'es direkte i Kubernetes enten via Rancher eller direkte via kubectl (Kubernetes kommandoprompt).

Når en løsning i GovCloud sættes sammen til en container-baseret service, består denne løsning af én eller flere containere, der hver for sig indeholder en komplet stak af software til én komponent, en pod. En sådan samlet stak, kaldet et image, gemmes i et særligt repository, så det let kan deploy'es i et miljø senere, uden at build'e komponenterne igen.

Harbor anvender Keycloak som adgangskontrol.

4.3.2 Rancher

Se afsnit 3.2.1 Rancher.

4.4 Drift og overvågning

Efter at en version er blevet deploy'et, afvikles applikationen i Kubernetes med de parametre, der er opsat via kubectl eller Rancher. I drift kan kunderne selv opsætte logning og overvågning af applikationen. Toolchain'en tilbyder desuden værktøj til koordinering og vidensdeling samt performance- og fejlanalyse.

4.4.1 Zabbix

Zabbix er et overvågningsværktøj til flere it-komponenter, herunder netværk, servere, virtuelle maskiner og cloud-services. Zabbix leverer overvågningsmetrikker til blandt andet netværksudnyttelse, CPU-belastning og diskpladsforbrug.

4.4.2 Grafana

Grafana visualiserer data i form af dashboards med tabeller og grafer. Grafana bruges i GovCloud til at udstille de overvågningsdata, som indsamles af Zabbix.

4.4.1 ElasticSearch

ElasticSearch er et log management-værktøj, der indsamler en del af de lokale logs, som GovCloud-platformen genererer. ElasticSearch indeholder også en søge- og analysemotor til logdata. Analyser af logdata kan dog med fordel foretages i Kibana.

4.4.2 Kibana

Kibana er et log-management-værktøj og en grafisk front-end til ElasticSearch. Med Kibana kan logdata i ElasticSearch visualiseres med diagrammer og grafer.