UiO : Universitetets senter for IT

Overvåkning av Cerebrum

Cerebrum-seminar 2019

Kai Vaade, Cerebrum-Drift

Agenda

- Overvåking av Cerebrum (hovedsakelig fra et drifts-perspektiv)
- Eksempel på avvik i Cerebrum, 2. feb 2019.

Overvåkning av Cerebrum

- Hvordan har vi oversikt over at ting fungerer slik de skal?
  Hvordan oppdager USIT problemer?
  Er overvåkingen god nok?
- Overvåkes av ukevakt i kjernetid; kl 09:00 - 14:30. Ukevakt-ordning; én person har ansvar for å følge med. Utenfor kjernetid vil det variere når feil fanges opp.
- Prøver å være proaktiv i stedet for reaktiv, men det er mange forskjellige integrasjoner og utfordring i at det er mye automatikk, integrasjoner, data som ikke lett å teste…

Konfigurasjons- og kodeendringer legges ut i Produksjon

a)
- Konfigurasjonsendringer gjøres hovedsakelig av Drift.

b)
- Kodeendringer uføres av utvikler, testes lokalt
- Godkjennes av én eller flere utviklere
- Prodsettes av utvikler

I koden kan det legges inn sjekker på at resultat ser riktig ut, men vanskelig å sjekke for alt som kan skje.

De ulike overvåkingskanaler vi har på kode i Produksjon

- **RT**

Ticketbasert system hvor brukere melder inn problemer/utfordringer (reaktivt)

- **Mattermost**

Lynmeldinger mellom IT-ansatte ved UiO (har overtatt etter XMPP).
- Varslinger mellom utviklerne og drifterne, og også med driftssentret samt øvrige UiO-brukere.

- **Zabbix**

Monitoreringssystem hvor man kan kjøre tester nesten på hva som helst, og sette opp alarmer (e-mail, ELK, Jabber, Mattermost, SMS)
Oppgradert til ver. 4.0 den 5. mars - mistet dashboard, bør opprettes igjen.

De ulike overvåkingskanaler vi har på kode i Produksjon (forts)

- **Zabbix (forts)**

Utover en basic overvåkning (load, disk, cpu etc) av servere er det satt opp alarmer på:
Felles
- bofhd
- job_runner
- antall filer i job_runner directory
- antall filer eldre enn 2 år

UiO
- consumer_SAP
- exchange_daemon
- radius-karantene-fil
- git (versjonering av cerebrum-koden)

De ulike overvåkingskanaler vi har på kode i Produksjon (forts)

- **Sentry**

Akkumulerer opp feil i Cerebrum. Har erstattet gammelt "system" der cerebrum-feil i logger ble sendt ut på e-post.
Ingen alarmer, må sjekkes manuelt.
Generell overblikk og søk etter nøkkelord slik som: too many, failed processing, person, similarsizewriter, manual intervention, multiple, exit_code=1, etc.

- **ELK - Elasticsearch Logstash og Kibana**

ELK brukes til mottak, prosessering, lagring, analyse og visualisering av loggdata. Vi har brukt mye ressurser på å sette opp ELK, men bruker det kanskje i for liten grad.

Eksempel på avvik i Cerebrum, 2. februar 2019

- Avviksrapport (Cerebrum fjernet fnr, studenter mistet tilgang).

  Problem oppdages IT-drift hos Høgskolen i Østfold (HiØ) merker at overførte filer fra Cerebrum (LDAP og ABC) har blitt markant mindre, og sender e-post til Cerebrum-drift om problemet (RT-sak).

- **Tiltak**
  - USIT hjemmevakt har opprettet en egen kanal på Mattermost for intern koordinering ved slike større hendelser. [Gjort]
  - USIT reviderer prodsettingsrutinene for Cerebrum slik at det blir tydeligere hvordan en endring må testes før den settes i produksjon. [Under arbeid]
  - USIT reviderer interne rutiner for varsling ved uforutsette hendelser for Cerebrum. [Under arbeid]
  - USIT vurderer hvilke automatiske varsler som kan settes opp for å oppdage om noe lignende skjer igjen. [La oss begynne med dette nå, kom med innspill!]
  - USIT forbedrer loggingen, så den inneholder relevant informasjon, og med riktig loggnivå. [Utviklingsjobb, står i kø]