IT-webinaari 9.5.2025

OPIN.FI

Lokitus, monitorointi ja hälytykset opin.fi-palvelussa

Sisältö

- Yleistä
- Lokitus
- Monitorointi
- Hälytykset
- Nykyhetki ja tulevaisuus
- Sanasto

OPIN.FI

Yleistä

- Vaatimus saatavuudelle on 99,5 %
- Miten lokitus, monitorointi ja hälytykset on hankkeessa rakennettu
- Miten häiriöt kulkevat läpi järjestelmän palvelutuotannolle asti
- AWS GuardDuty

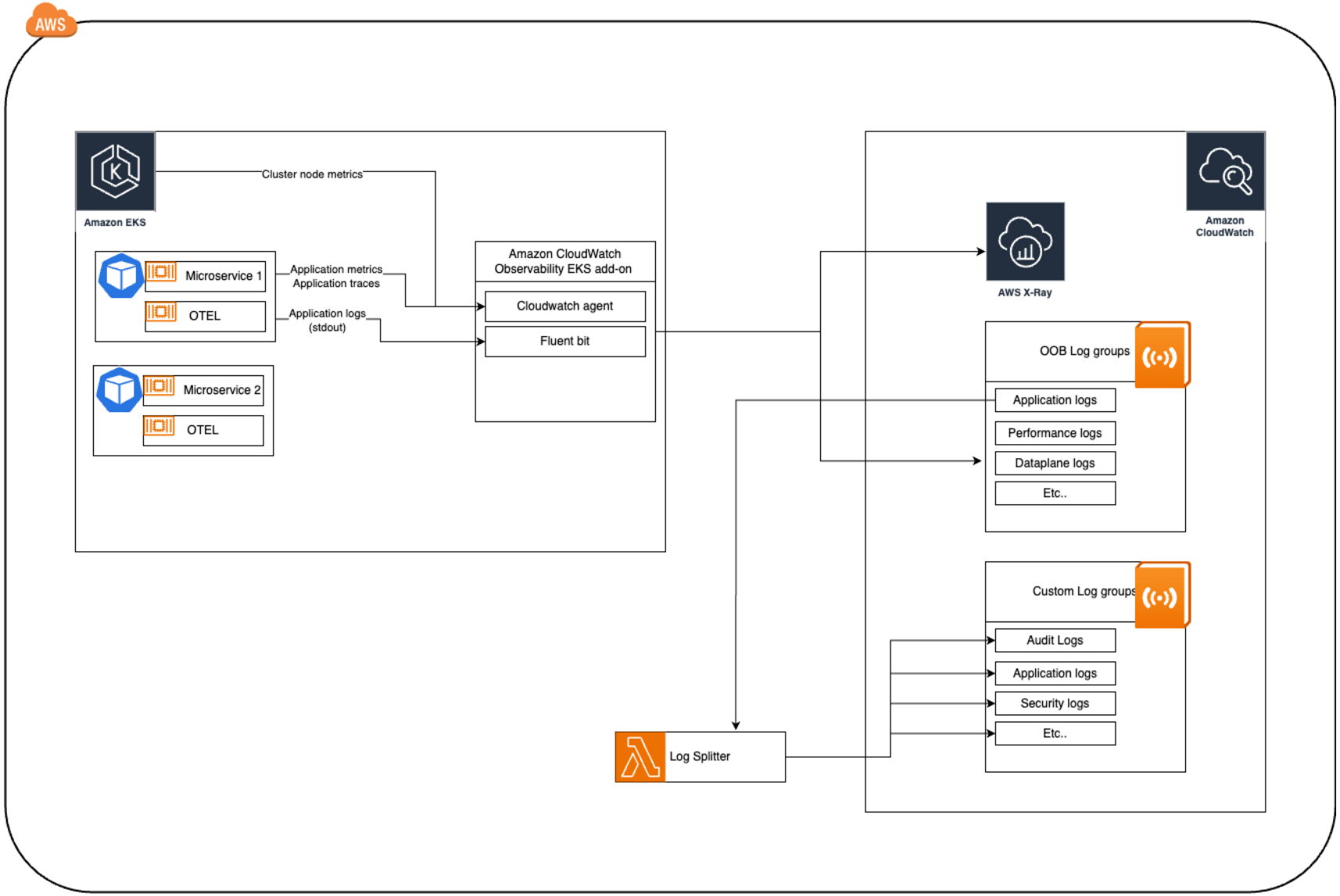
OPIN.FI

Lokitus

- Sekä opin.fi-sovellus ja siihen liittyvät komponentit, kuten IDM, lokittavat
- Kullakin lokiriveillä on kategoriatieto
  - Audit, **GDPR**, metric, software, integration, other
- AWS Lambda –funktio jaottelee lokirivit kategorioiden perusteella eri lokiryhmiin
- Infrapalvelut lokittavat omiin lokiryhmiin
  - Esim. Kubernetes, Karpenter (skaalaus)
- Lokien perusteella kerätään *metriikkaa*, joiden pohjalta syntyy *hälytyksiä*

OPIN.FI

Lokitus

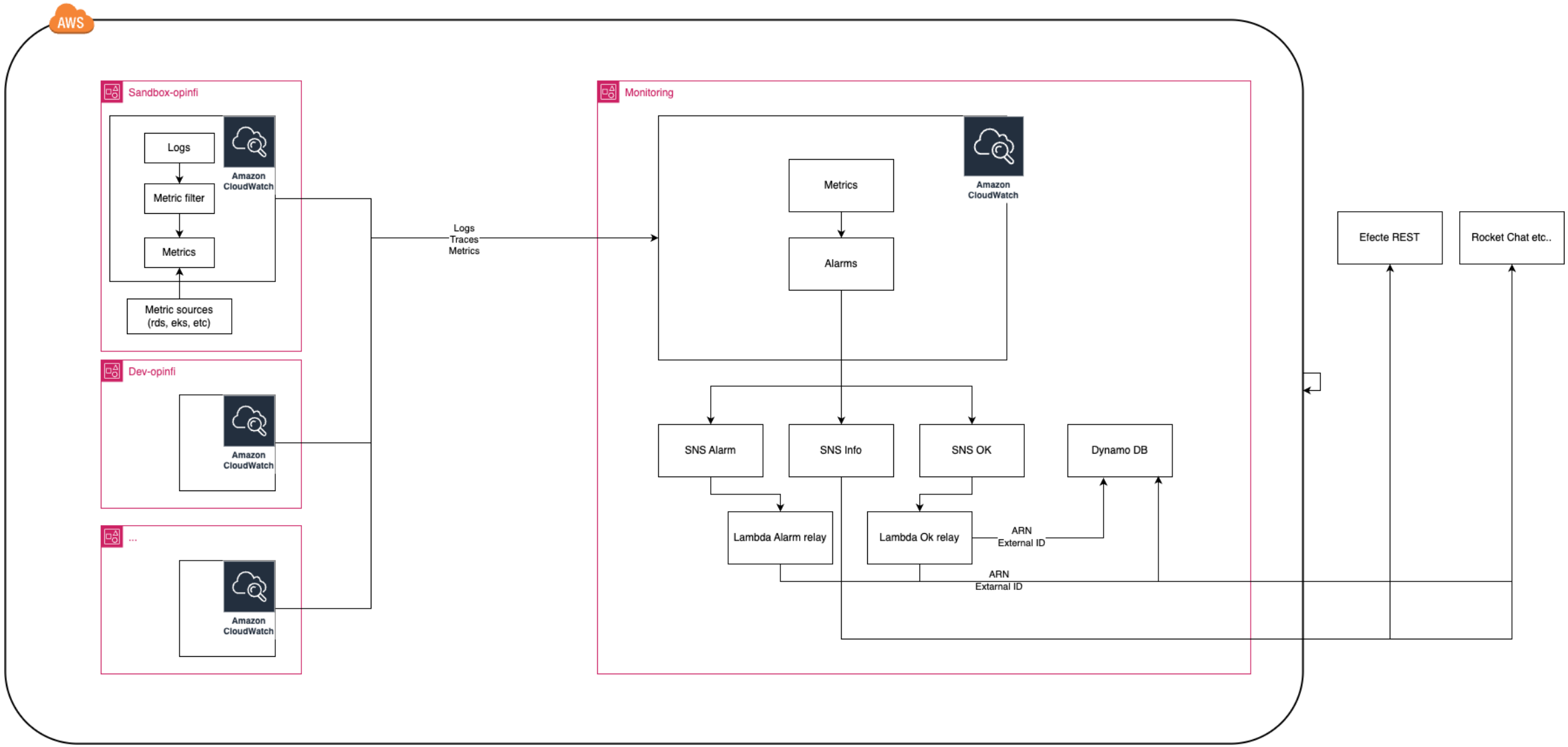

AWS
Amazon EKS
Cluster node metrics
Microservice 1
OTEL
Application metrics
Application traces
Application logs
(stdout)
Microservice 2
OTEL
Amazon CloudWatch
Observability EKS add-on
Cloudwatch agent
Fluent bit
Amazon
CloudWatch
AWS X-Ray
OOB Log groups
Application logs
Performance logs
Dataplane logs
Etc..
Custom Log groups
Audit Logs
Application logs
Security logs
Etc..
Log Splitter

Monitorointi

- Ympäristöillä on omat monitorointitilinsä
- Lokien pohjalta kerätään metriikkaa, mutta *suurin osa metriikasta tulee muualta*
- **Application Signals** monitoroi opin.fi-palveluiden saatavuutta ja suorituskykyä
    - Käyttää hyväkseen myös telemetriikkatietoa (Open Telemetry) eli palvelujen sisäistä toimintaa
- Service Level Objects (SLO)
    - Määriteltyjen palvelutasojen seuranta joko endpointteja kutsumalla tai lokeista
    - Syntyy metriikoita ja hälytyksiä
    - Säännöllinen pollaus metriikoiden saamiseksi (varmistettava, ettei sotke analytiikkaa)

OPIN.FI

Monitorointi ja hälytykset



Esimerkki: Canary-ajot

- Synthetics Canary eli Canary-ajot on AWS:n palvelu, joka tekee viiden minuutin välein sivulatauksia web-selaimesta
- Kohteena opin.fi-palvelun pääsivu
- Keräämme jatkuvaa dataa saavutettavuudesta
- Tarvittaessa syntyy hälytys
- Sivulataus ei sotke analytiikkaa (kävijämäärät)

OPIN.FI

Hälytykset

- Hälytykset on jaettu neljään eri prioriteettiin kriittisestä alhaiseen
    - Mitä korkeampi prioriteetti, sitä nopeammin tilanne tulkitaan hälytykseksi
    - Ei yleensä ensimmäisestä havaitusta tilanteesta, esim. HTTP 500 –statuksesta
    - Tällä hetkellä 28 erilaista hälytystä
- Hälytysviestit siirtyvät API-kutsuina HEHF:n Efecte-palveluun *eventeiksi*
    - Hälytys *päälle* ja myös *pois*
- Efectessä on myös logiikka sille, milloin eventistä syntyy *hälytys* palvelutuotannolle
    - Mahdollisuus antaa tilanteen nollautua

OPIN.FI

AWS GuardDuty

- Seuraa aktiivisesti palveluun ulkoa tulevia uhkia
- Seuraa *anomalioita*
  - Epätavallisia kirjautumisyrityksiä
  - Epätavallista verkkoliikennettä
  - Epätavallista tallennusta
- Skannaa viruksia
- Oppiva

OPIN.FI

Nykyhetki ja tulevaisuus

- Pohjat on rakennettu ja toimivaksi havaittu
- Tuotannossa ei ole ollut dramatiikkaa
  - botteja
  - perusskannauksia
- Hälytyksiä tulossa lisää
- Nykyisten prioriteetteja säädettäneen
- Palveluohjeistuksen kirjoittamista

OPIN.FI

Sanasto

- **Cloudwatch** – resurssien seuranta, logien kerääminen, hälytysten asettaminen ja suorituskyvyn analysointi
- **Application Signals** – suorituskyvyn seuranta, virheiden ja poikkeamien havaitseminen
- **Container Insights** – suorituskyvyn seuranta ja lokien kerääminen EKS-klustereissa. Palvelua käytetään analysoimaan ekosysteemin sisällä toimivien konttien sekä palvelujen suorituskykyä ja käyttäytymistä.
- **X-Ray** – jäljitettävyys (traceability), suorituskyvyn seuranta, virheenetsintä
- **Efecte** – palvelunhallintapalvelu, jonne lähetämme hälytykset

OPIN.FI

Kiitos!

Kevätkauden viimeinen IT-webinaari pidetään 10.6.2025

OPIN.FI