IT-webinaari 14.3.2025

OPIN.FI

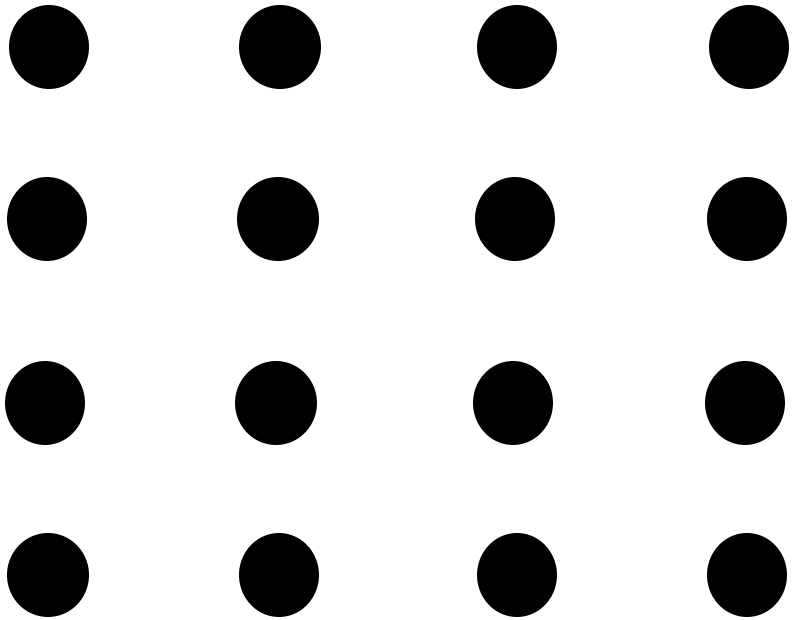
Digivisio pilvessä

Digivisio pilvessä

- Taustaa: miksi pilvi, kilpailutus ja Kubernetes?
- Infrastructure as Code (IaC)
- Skaalattavuus
- Turvallisuus
- Iso kuva
- Tulevaisuus
- Sanasto

OPIN.FI

Taustaa



- Miksi pilvi?
- Miksi oma kilpailutus?
- Miksi hallittu Kubernetes?

Miksi pilvi?

- Pitkäaikainen hanke, potentiaalisesti usean palvelun sijoituspaikka
- Virtuaalipalvelinpohjainen ympäristö ei vastannut tarpeisiin
- *Benchmarking* (DVV, Valtiokonttori, OPH, Funidata) antoi luottamusta
- Kehittäjille mielekkäämpi ympäristö
- Korkeakoulujen yhteisten palvelujen kehittämisen kompetenssin lisääminen

OPIN.FI

Miksi oma kilpailutus?

- Tunnistettuja vaihtoehtoja olivat CSC:n pilviympäristö, GÉANT/OCRE ja Valtori
- CSC:n jaettu ympäristö Rahti ei soveltunut hankkeen tarpeisiin (feature, ei bugi)
- GÉANT/OCRE 2020 -puittari ei sopinut meille (OCRE 2024 tuli voimaan 3.2.2025)
- Aivan ensimmäiseksi liikkeelle Digital Oceanin pilvellä 2022
- Valtorin kilpailutus liikkeelle 2023, valituksi kumppaniksi Gofore ja alustaksi AWS
    - Rajoituksia pilvialustatarjojalle ei ollut, ainoastaan hallittu Kubernetes

OPIN.FI

Miksi Kubernetes (1/2)?

- Kubernetes on pitkäaikaisin ja kehitetyin pilvihallintapalvelu/työkalusto laajojen kontitettujen palvelujen hallintaan
- Hallitussa Kuberneteksessa palvelutarjoaja ylläpitää itse sitä alustallaan, me ”vaan” käytämme sen toiminnallisuuksia
  - Keskittyminen olennaiseen
  - Economies of scale
- Otamme palvelutuotannon vuosikellon mukaan käyttöön uusia Kubernetes-versioita kolme kertaa vuodessa

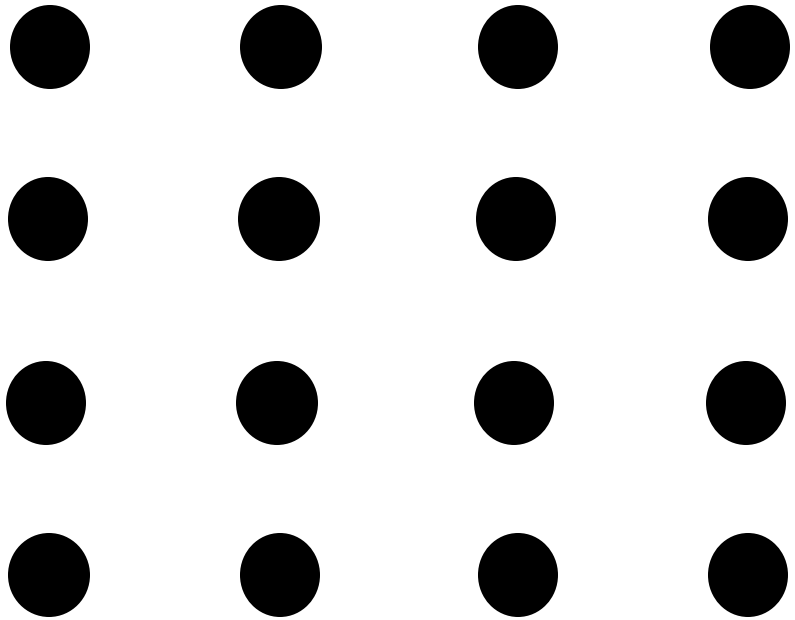
OPIN.FI

Miksi Kubernetes(2/2)?

- *Siirrettävyyden* kulmakiviä ovat hallittu Kubernetes, IaC (Infrastructure as Code) ja toimittajalukottomuus
- Kubernetes on tuettuna (käytännössä) kaikilla pilvitarjoajille
- Se on open sourcea ja toimittajalukoton
- Se ja IaC sopivat täydellisesti yhteen
- Voi tarjota hyvää HA-palvelutasoa epävakaalla alustallakin (esim. AWS:n spot-instanssit)

OPIN.FI

Palaset



- Infrastructure as Code
- Skaalautuvuus
- Turvallisuus
- Käyttäjähallinta
- Muita

Infrastructure as Code 1/2

- Lähes kaikki hankkeen konfiguraatiot ovat koodina versionhallinnassa (IaC)
- IaC on myös kuvaus ajossa olevasta ympäristöstä
    - Dokumentaatiota samalla
- Koko infraa ei voi 100-prosenttisesti asentaa ”nappia painamalla”, vaan joitain manuaalisia välivaiheita on

OPIN.FI

Infrastructure as Code 2/2

- Ympäristöjen konfiguraatioita ylläpidetään Terraform-työkalulla
  - Ylläpitää tilaa, osaa laskea päivitysmuutokset ja ajaa ne sisään
- Terragrunt hyödyntää Terraformia hyödyntämään samaa koodia eri ympäristöissä
  - Sandbox, dev, test, staging ja prod
  - Samat konfiguraatioelementit, mutta ympäristökohtaiset muuttujat ja kustomoinnit
  - Nimentä- ja muut käytännöt kaikilla tasoilla!

OPIN.FI

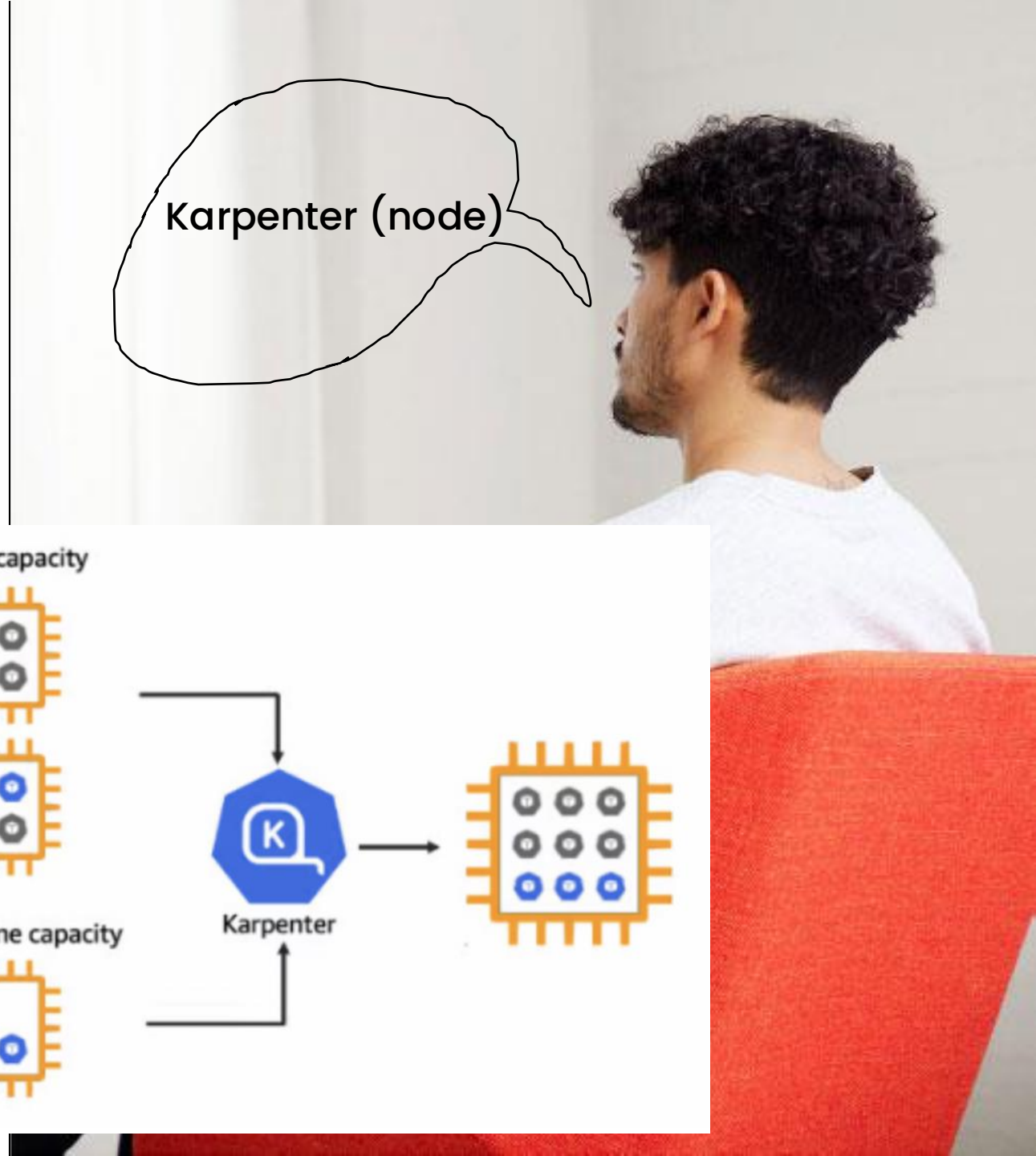
Skaalautuvuus (1/2)

- Keda luo mikropalvelutasolla uusia rinnakkaisia **podeja** kuorman mukaan
- CPU:n kulutus, muistin käyttö ja kutsujen määrä ovat parametreja, joilla Kedan toimintaa palvelukohtaisesti voidaan säätää ylös- tai alaspäin
- Kaikissa palveluissa on oletuksena kolme (3) podia, jotka on jaettu eri AZ:lle
  - Matalalla kuormassa pysytään kolmessa
  - Korkealla kuormalla nostetaan lisää
  - Rajat säädetään (IaC)

OPIN.FI

Skaalautuvuus (2/2)

- **Karpenter** tehostaa skaalausta tarkastelemalla sovellusten tarpeita ja klusterin kokonaiskapasiteettia (nodet)
    - nodejen luokittelu (kapasiteetti, spot/on-demand, affinity..., EC2NodeClass)



OPIN.FI

Turvallisuus

- Monesta osasta koostuva:
- AWS: WAF, ALB, VPC
- AWS Best Practises
- IaC-käytännöt
- Opin.fi – vaihteleva IP (pilven feature)
- Säännölliset tietoturva-auditoinnit
- CI-putkien laadunvarmistus
- Valvonnan SecurityHub ja GuardDuty (valvonnoista IT-webinaari 9.5.2025)

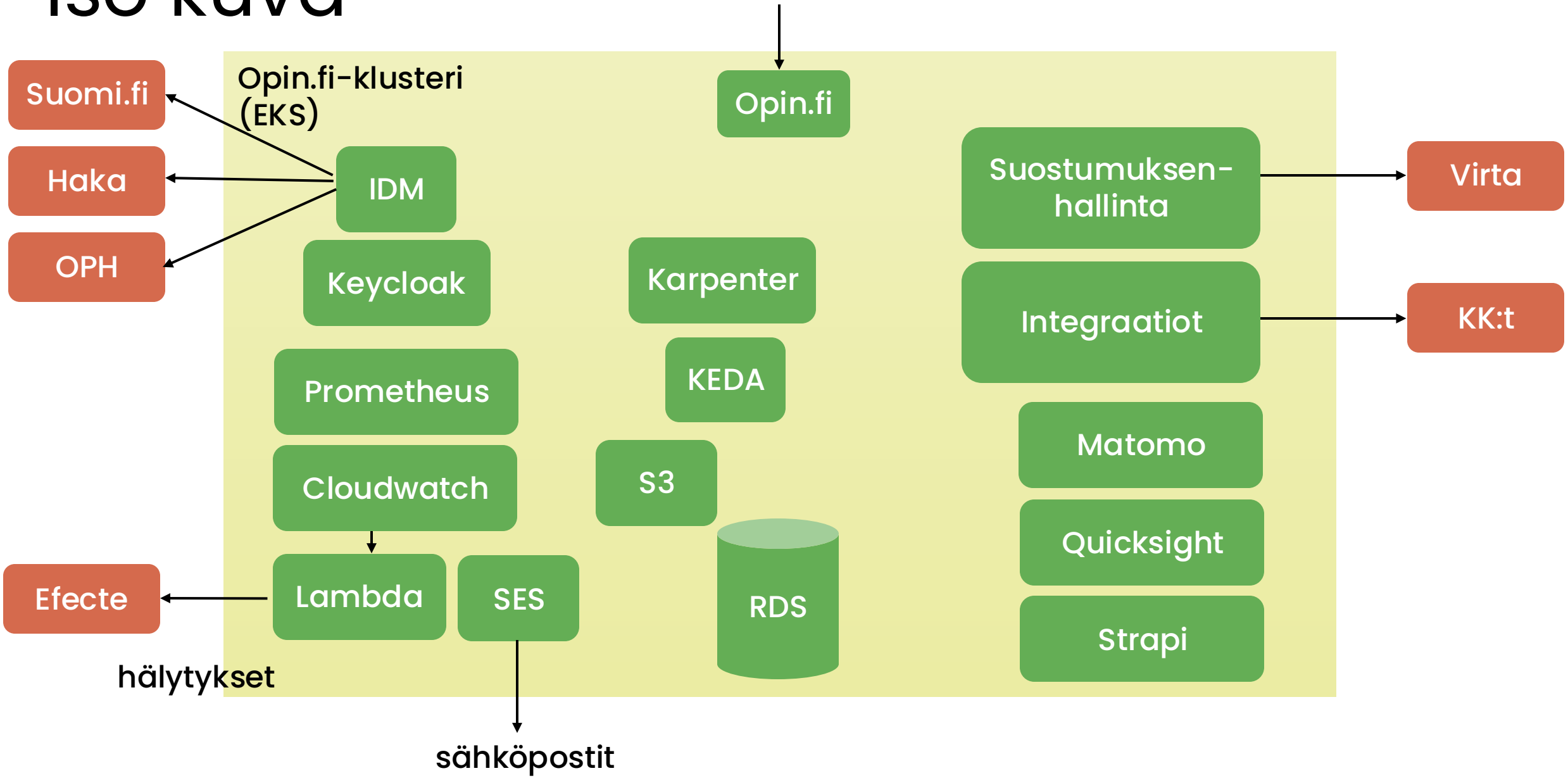
OPIN.FI

Käyttäjähallinta

- IDM
  - Suomi.fi
  - Haka
- Keycloak
  - Admin
  - Matomo
  - ArgoCD
  - Quicksight
  - mikropalvelujen autentikaatioklientteja
- Strapissa oma käyttäjähallinta

OPIN.FI

Iso kuva


Opin.fi-klusteri
(EKS)
Opin.fi
Suomi.fi
Haka
OPH
IDM
Keycloak
Prometheus
Cloudwatch
Karpenter
KEDA
S3
RDS
Suostumuksen-
hallinta
Integraatiot
Matomo
Quicksight
Strapi
Virta
KK:t
Efecte
Lambda
SES
hälytykset
sähköpostit

Tulevaisuus

- Tuotantokäytön alkaminen (aina yhtä jännää!)
- Hälytysten ja monitorointien hienosäätöä
- Ympäristöjen säätöjä
- Kustannusoptimointeja
- DevOps-toiminnan kehittämistä
- Mietintää: mikä – jos ylipäätänsä mikään – on *alusta* jota tarjoamme, ja mihin suuntaan sitä pitäisi viedä

OPIN.FI

Sanasto

- **Kubernetes** – avoimen lähdekoodin ohjelmisto säiliöiden hallintaan suuressa mittakaavassa
- **Hallittu Kubernetes** – palveluntarjoajan(esim. AWS) ylläpitämä Kubernetes
- **Pod** - pienin ajettava looginen yksikkö, ajetaan Nodeissa. ~kontitettu palvelu
- **Node** – virtuaalinen tai fyysinen palvelin
- **HA** – high availability (korkea käytettävyys)
- **AZ** – availablity zone (fyysisesti eri paikassa sijaitseva palvelujen sijoituspaikka)

OPIN.FI

Kiitos!

The IT webinars will return…

OPIN.FI