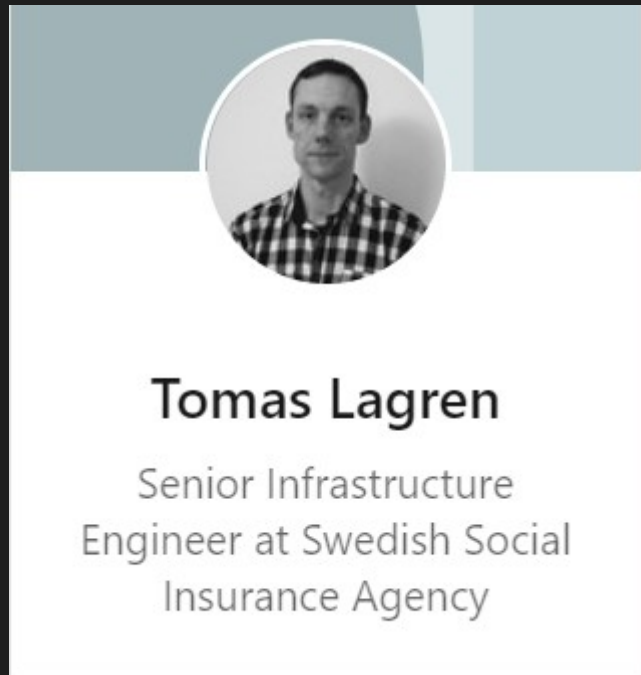




OpenShift @ FK

Bygga, leverera och leva med OpenShift ur ett infrastrukturperspektiv

Hej och tack för att ni vill lyssna på mig



<https://www.linkedin.com/in/tlagren/>

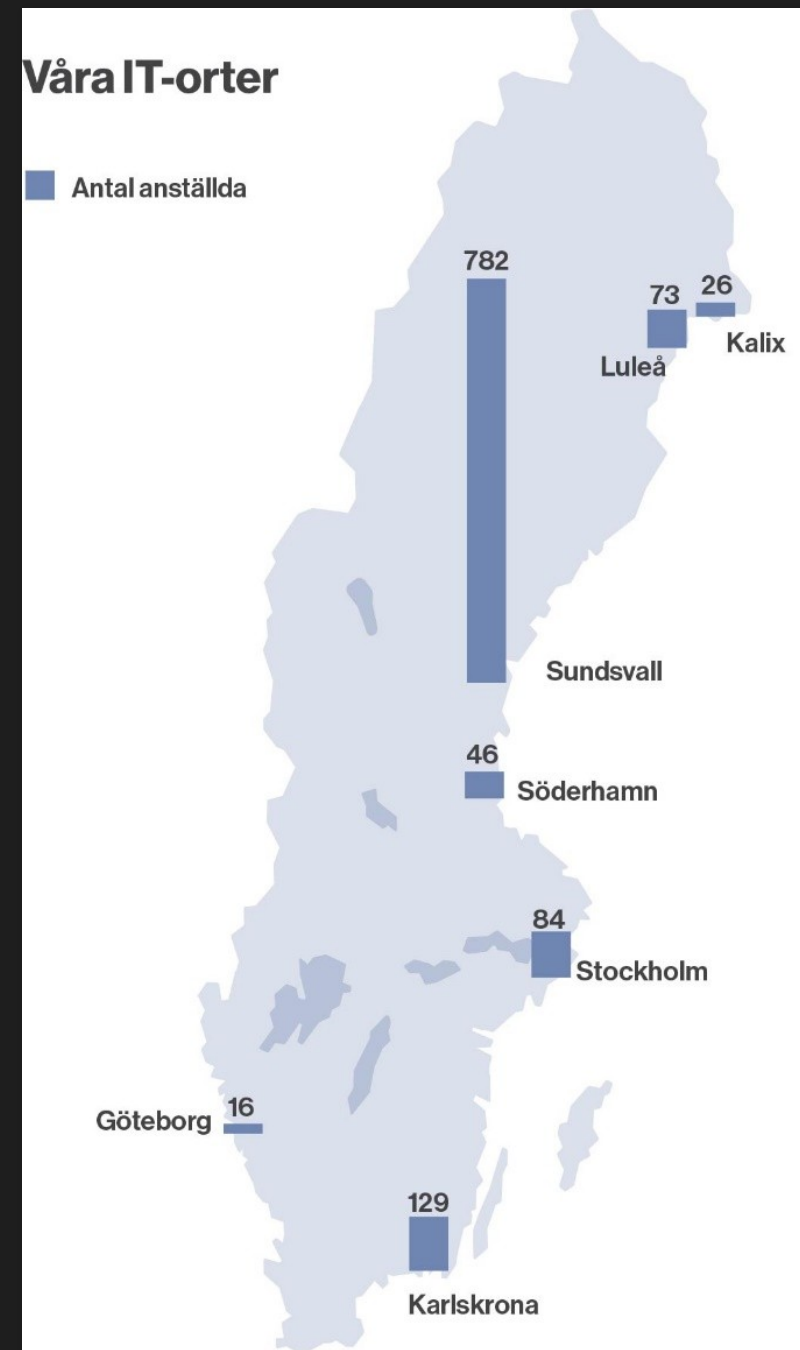
Linuxnörd som brinner för öppen källkod och trivs bäst i datacentersammanhang.

Designar och ritar gärna smarta lösningar på arkitekturnivå men värnar om att aldrig lämna terminalprompten för länge.

Riktlinje om öppen källkod på Försäkringskassan
<https://github.com/Forsakringskassan/riktlinje-oppenkallkod>

Lite fakta om it-avdelningen

- Utveckling för ca 700 miljoner kr i 100 parallella projekt årligen.
- Drift av mer än 13 000 servrar, 6 000 terabyte data och 20 000 it-arbetsplatser.
- It-tjänsterna hanterar årligen:
 - 485 miljarder kr i utbetalningar
 - 39 miljoner besökare på mina sidor
 - 99 miljoner samtal och digitala interaktioner
- Avdelningen omsätter 2,1 miljarder kronor och har mer än 1200 anställda verksamma på 7 orter.
- It-direktör Peter Haglind.



En myndighet, två roller



SLUTKUND



Red Hat

Ready

Business Partner

Certified Cloud and
Service Provider

Samordnad och säker statlig it-drift

🔍 Sök

[Erbjudanden](#) [Kundmyndigheter](#) [Uppdraget](#) [Samverkan](#) [Anslutning](#)

[Startsida](#) / [Erbjudanden](#) / [Enstaka tjänster](#)



Enstaka tjänster

Försäkringskassans it-avdelning erbjuder en egen portfölj av enstaka tjänster. Dessa ligger i egna serverhallar i Sverige och uppfyller alla juridiska- och säkerhetskrav för användning av svenska myndigheter. Vi bygger snabbt ut vår portfölj av enstaka tjänster.

Kapacitetstjänst CAP

CAP, Container Application Platform, är en molnlik kapacitetstjänst för container och micro-tjänster. En infrastruktur som möjliggör snabb utveckling och realisering av applikationer och micro-tjänster. Den bygger på samma industriledande teknik som många av dom publika molntjänsterna använder, men levereras fullt ut av svensk säkerhetsklassad personal inom Sveriges gränser.

Tjänsten kombinerar smart teknik tillsammans med beprövade processer och bygger på standardiserade komponenter utan inlåsningsseffekt.

Hur och vad kör vi?

2,4TB

RAM

4 686

vCPU

30+

kluster

249

users i FK dev

479

workernoder

Produkter och lösningar

Infoblox 

Red Hat



Quay



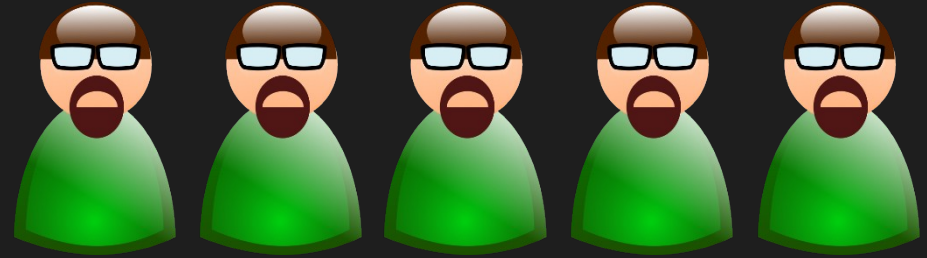
 NetApp

vmware®

Disconnected mode - UPI



OpenShift Infra Team



- Fem tekniker med Linuxbakgrund
- Infrastrukturutveckling och drift
- Beredskap 24/7 (var 5'e vecka)
 - Allt utanför kontorstid
 - Incidenter och löpande ärenden dagtid
 - Den som jobbar på sommaren
 - Utveckling och projekt i mån av tid
- Produktansvarig i teamet
- FK Intern leverans → Containerplattform
- Extern leverans → Samverkansmyndighet

Arbetssätt - Struktur

- Planerade aktiviteter i Jira (Kanban)
- Morgonmöte mån, ons, fre
- Prioriterar måndag morgon
- "Onsdagsdemo" inom teamet
- Dokumentation i Confluence
- Löpande chatt i Mattermost

- Tips på bra arbetssätt:

En som bygger nytt och gör initial dokumentation och en annan som provkör och fixar dokumentationen.



Infrastrukturkod och automation

- Standardisering!!
 - Undviker "specialare"
 - Hitta standarden i kundens unika behov
- Automatisera allt – Inget manuellt fix
- Försöker lösa så mycket som möjligt inom teamet
 - Bättre förståelse och kontroll
 - Ofta snabbare leverans
 - Kan lösa oförutsedda saker smidigt
 - Det är roligt – Vi är geeks ☐
- Vi kodar mot alla gränssnitt
 - vCenter
 - NSX Manager
 - Infoblox
 - Op5
 - F5
 - AVI



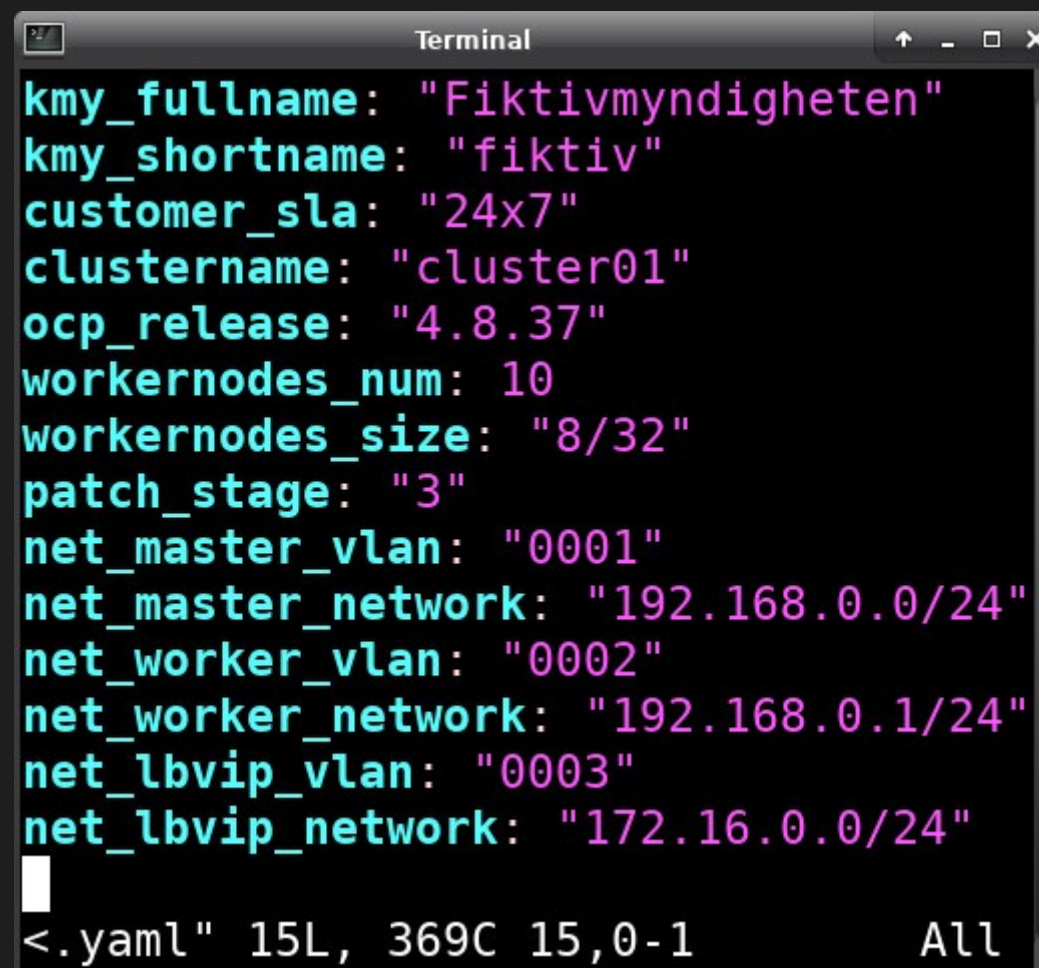
ANSIBLE



GitLab

Infrastrukturkod och automation

- Gör det så enkelt som möjligt, men inte enklare än så.
 - Vi är duktiga men alla i teamet ska klara av att hantera lösningarna vid en pressad akutsituation.
- Definiera så få saker som möjligt, klura ut det med kod istället.
- Genererar inventory

A terminal window titled "Terminal" with standard window controls (up arrow, minus, square, X). It displays a YAML configuration for a cluster. The configuration includes fields for fullname, shortname, customer SLA, clustername, OCP release version, number and size of worker nodes, patch stage, and network settings for master, worker, and load balancer VIP. At the bottom, it shows a status bar with file information: "<.yaml" 15L, 369C 15,0-1 and "All".

```
kmy_fullname: "Fiktivmyndigheten"
kmy_shortname: "fiktiv"
customer_sla: "24x7"
clustername: "cluster01"
ocp_release: "4.8.37"
workernodes_num: 10
workernodes_size: "8/32"
patch_stage: "3"
net_master_vlan: "0001"
net_master_network: "192.168.0.0/24"
net_worker_vlan: "0002"
net_worker_network: "192.168.0.1/24"
net_lbvip_vlan: "0003"
net_lbvip_network: "172.16.0.0/24"

<.yaml" 15L, 369C 15,0-1 All
```

Driftmässigt ”out of the box”

- Driftstödjande funktioner vid leverans
 - Playbook som automatiskt konfigurerar
 - Övervakning (baserat på SLA)
 - Logghantering
 - Mätvärden
 - Playbook som automatisk kör backup av klusterconfig på samtliga kluster
- **Gör det sedan**
Kommer aldrig ske
 - **Det är nästan klart**
Ej påbörjat
 - **Restlista**
Saker man skulle gjort

Utmaningar

- Lagring
 - Långsamt på NFS för vissa laster
 - Säkerhetsutmaningar med NFS
 - Behov av Read-Write-Many även på block
 - Failovertid för block
- Säkerhet
 - Befintliga principer för segmentering blir svåra att realisera i OpenShift.
 - NetworkPolicy är smidigt, men saknar logging
 - Separation mellan applikationer och systemfunktioner
- Övrigt
 - Machine Config kan fastna
 - Pod'ar som inte avslutas korrekt
 - Pod'ar som saknar limits

Övriga findings

- Det är svårt att samtidigt vara intern it-avdelning och extern leverantör.
- Övervakning, falsklarm.
- Produkter som vill integrera mot underliggande OS.
- Stora programvaruleverantörer vill styra över installationen av OpenShift.
- NodePort, EgressIP, ExternalIP mm ställer till det.

Kom och jobba på FK



https://www.forsakringskassan.se/omfk/jobba_hos_oss/lediga_jobb