

# Performance overvågning af KGW

**Author:** Henrik Thuesen  
**Date:** 16-Jan-2014 19:47  
**URL:** <https://www.nspop.dk/pages/viewpage.action?pagelId=28871299>

# Table of Contents

---

1	Antagelser	4
2	"Points of Interest"	5
3	Behandling	6
4	Implementation	7

Dette dokument indeholder overvejelser og anbefalinger omkring overvågning af performance af kommunernes Gateway installationen. Disse har til formål at varsle om for høj belastning, sådan at man kan nå forbedre situationen inden anvendere påvirkes. Derudover ønskes der også at indsamle viden omkring brug og udnyttelse af installationen.

# 1 Antagelser

---

Jvf. [performance rapporten](#) så kan et 2 søjle setup håndtere 70 request/sek. Som beskrevet i rapporten kan der ikke regnes med en faktor 2, når yderligere 2 søjler bruges. Der vælges derfor her 1.7. (med nuværende målinger lader der desværre ikke til at være den store forskel på 1 og 2 søjler setup)

## 2 "Points of Interest"

Eller POI, beskriver hvilke målepunkter, der er interessant mht. at overvåge performance. Nedenstående tabel beskriver hvad der skal måles samt hvilken "trigger", der anbefales opsættes:

POI	Trigger	Visualisering	Gruppe
Request/sekund	$120 * 90\% = 108$	graf	w
Request/minut	$7200 * 90\% = 6480$	graf	w
Request/time	$432000 * 90\% = 388800$	graf	e
CPU utilisation/minut	-	graf	-
CPU utilisation/time	95%	graf	e
Memory/5m	90%	graf	e
gns. svartid per minut	5 sekunder	graf	w
gns. svartid per time	4 sekunder	graf	e
Request fordelt på path per time	-	graf	-
Proxy requests fordelt på wsa/soapaction per time	-	liste	-
gns. svartid per endpoint	-	liste	-

Når en trigger nåes, så baseres handlingen på hvilken gruppe POI findes i:

- **warning:** mange af disse bør give anledning til bekymring
- **error:** en af disse bør give anledning til bekymring.

Disse POI triggers kunne f.eks. behandles teknisk ved at sende en mail til relevante parter. F.eks. kunne 5 warnings give anledning til en mail, mens 1 error altid vil gøre dette.

Udover notifikation baseret på triggers, så burde POI graferne udstilles et passende sted, f.eks. confluence. På disse grafer kunne trigger værdierne ligeledes illustreres ved en enkelt konstant linje – hvor dette giver mening.

## 3 Behandling

---

Valget af POI er baseret på erfaring med performance testen samt generelt logindsigt i NSP miljøer.

Requests over tid skal sammenlignes med max TP målt. Da der kan være peaks, så er situationen kun alarmerende hvis trigger per time nåes. Derudover burde peaks kunne nåes indhentes.

CPU og memory målinger skal bruges til at vurdere hvad miljøet forbruger af resourcer. Disse værdier kan også bruges til at planlægge hvordan installationen kunne skaleres.

Svartidsmålingerne er medtaget, da dette direkte kan ses af anvendere. Derudover kan sammenligningen mellem request over tid og svartid give et indblik i hvad systemet foretager sig.

Fordelingen af requests er medtaget, da det er nødvendigt at vide hvad resourcer bliver brugt til.

## 4 Implementation

---

Dette afsnit beskriver hvordan POI kan findes via diverse logfiler.

- Requests over tid kan lettes fåes via NSP Valve loggen (`sourcetype="json_auto_timestamp"`)
- CPU forbrug: hertil findes der en `sourcetype`.
- Når der her refereres til "Memory" menes der java heap. Der findes en JMX log, hvori memory stats logges inkl. max og udnyttelse.
- Svartider burde ideelt set beregnes ud fra klienten, men da dette ikke er muligt, burde load-balancerens log kunne bruges. Her skal svartider indeles ifht. path.
- Antal requests fordelt på path kan laves ud fra NSP Valve loggen. Af interesse findes:

1. `/sosigw/browsersign/invoke`
2. `/sosigw/proxy/soap-request`
3. `/sosigw/service/sosigw`

- Antal request fordelt på `wsa/soapaction`: hvis en `soapHeaders.To` er angivet (udtryk i nuværende NSP valve konfiguration), så skal denne bruges. Hvis den ikke findes, så skal `httpHeaders.SOAPAction` bruges. En liste af disse samt antallet for hver time.
- For at finde svartiderne for bagvedliggende service ved proxy requests, kan sla-loggen bruges. Her findes logpunkter, `SOSIGWProxyRequestHandler.invokeRemoteService()`. Dette logpunkt indeholder både svartiden (`duration`) og `TargetSOAPEndpoint`.

Hvis ikke andet er angivet eller giver mening, så skal graferne beskrive de seneste 24 timer.

Alt data, der ligger til grund for beskrevne POI, burde allerede findes i eksisterende log filer.

Sammen med graferne og listerne burde der være links til tilhørende splunk-søgninger. Dermed vil der være muligt med disse som udgangspunkt, at lave andre undersøgelser.