Minlog – Splunk opsamling og udstillelse

Design og Arkitektur

Indhold

[1 Formål 3](#_Toc328726967)

[2 Arkitekturoverblik 4](#_Toc328726968)

[2.1 Splunk job 4](#_Toc328726969)

[2.1.1 Opbygning 4](#_Toc328726970)

[2.1.2 Yderligere oplysninger 5](#_Toc328726971)

[2.2 WebService 5](#_Toc328726972)

[2.3 Oprydningsjob 5](#_Toc328726973)

[3 Ændringslog 6](#_Toc328726974)

# Formål

Nærværende dokument giver et overblik over komponenterne med fokus på design og arkitektur. Dokumentet har som formål at give et indblik i det underliggende design, de udstillede snitflader på det overordnede niveau samt særlige forhold vedrørende de udstillede registre. Både aftagere af services samt NSP operatør/driftsleverandør kan med fordel læse dette dokument.

# Arkitekturoverblik

Minlog består af 3 komponenter og 1 database der skal replikeres mellem DoDi og NSP

**NSP**

**DoDi**

Splunk

API

**Splunk Job**

**Webservice**

(DGWS)

**Oprydning**

## Splunk job

Dette job deployes på DoDi platformen, og er ansvarlig for at trække data fra Splunk indexet over i en MySQL database.

Scriptet mapper data fra Splunk til Skema i MySQL. Mapning er som følger

Splunk MySQL

------------------------------------------------------------------

PersonCivilRegistration cprNrBorger

UserIdentification bruger

UserIdentificationOnBehalfOf ansvarlig

HealthcareProfessionalOrganization orgUsingID

SourceSystemIdentifier systemName

Activity handling

SessionId sessionId

"2012....." tidspunkt

Baseret på følgende input format til Splunk

2012-06-18 13:38:10,239Z PersonCivilRegistrationIdentifier="100000003" EventDateTime="2012-06-18T13:38:10.109Z" UserIdentifier="0101001000" UserIdentifierOnBehalfOf="0101001000" HealthcareProfessionalOrganization="SOR:12345678" SourceSystemIdentifier="System name" Activity="Opslag på NPI" SessionId="urn:uuid:145d6c9c-b873-47ab-9203-8eaa306013ad"

### Opbygning

Jobbet gør følgende:

* Forbinder til Splunk med et konfigurerbart interval
* Udfører søgning i Splunk udfra hvor langt man er nået - hvis det er første gang jobbet kører vil det tage op til ”nu” minus 30 sec. Ellers hentes alt der er indexeret siden sidste kørsel til ”nu” minus 30 sec.
* Overfører data til MySql og opdaterer hvor langt jobbet er nået i samme transaction.

### Yderligere oplysninger

Jobbet henter data ud fra tidspunktet de er indexeret på i Splunk, da man ikke kan være sikker på at datoen i logs vil være fortløbende - nogle servere kan f.eks. være offline og først aflevere log-opsamlinger til central behandling på et senere tidspunkt end data faktisk er logget. Dette er med til at sikre at alle data opsamles i MySQL databasen.

Desuden er der et delay på (default) 3 sekunder der sikrer at man ikke henter data op til det sekund som scriptet kører.

## WebService

Webservicen deployes på NSP platformen, og udstiller de opsamlede logs til aftagersystemerne.

Webservicens opgave er at søge i logninger, ud fra et given cpr nummer, og evt. et dato interval. Alle logninger der opfylder de angivne kriterier returneres. Webservicen udstiller denne funktionalitet via en SOAP webservice, beskyttet med DGWS og whitelist filtrering på CVR nummer.

## Oprydningsjob

Jobbet deployes på DoDi platformen.

Oprydningsjobbet kigger i databasen med et konfigurerbart interval og slette alle logs der er ældre end 2 år.

# Ændringslog

| Version | Dato | Ændring | Ansvarlig |
| --- | --- | --- | --- |
| 0.1 | 2012-06-28 | Initielt dokument | Trifork |