Minlog – Splunk opsamling og udstillelse

Installationsvejledning

Indholdsfortegnelse

[1 Formål 3](#_Toc329181527)

[2 Krav til driftsmiljø 4](#_Toc329181528)

[2.1 Krav til applikationsservere 4](#_Toc329181529)

[2.2 Krav til operativsystem 4](#_Toc329181530)

[2.3 Krav til database 4](#_Toc329181531)

[2.4 Krav til hardware 4](#_Toc329181532)

[3 Artefakter 5](#_Toc329181533)

[3.1 Minlog-ws 5](#_Toc329181534)

[3.2 Minlog-export 5](#_Toc329181535)

[4 Konfiguration 6](#_Toc329181536)

[4.1 Standard indstillinger 6](#_Toc329181537)

[4.2 Logning 7](#_Toc329181538)

[4.3 Database 7](#_Toc329181539)

[5 Ændringslog 8](#_Toc329181540)

# Formål

Vejledning til installation og konfiguration af Minlog splunk komponenter.

Dokumentet indeholder komponentens krav til det omliggende miljø, herunder krav til operativsystem, standard applikationer som f.eks. applikationsservere, databaseservere, java-versioner mm., angivet på version og service pack niveau.

Eksterne applikationer defineres som applikationer det kræver netværksadgang at tilgå, herunder også adgang til andre virtuelle miljøer residerende på samme hardware som komponenten.

Vejledningen skal tillige indeholde information om evt. konfiguration af standard applikationer og lign.

Footprint på hardware angives, dvs. mængden af RAM, harddisk, CPU, netværk osv. komponenten forventeligt anvender.

# Krav til driftsmiljø

## Krav til applikationsservere

Komponenterne er udviklet og testet på den version af JBoss 6.0, der findes på nsp-in-a-box VMWare imaget, og kan deployes i produktion på samme.

Applikationsserveren kræver SUN/Oracle Java 6.0 eller højere.

## Krav til operativsystem

Der stilles ingen krav til operativsystemet, ud over det åbenlyse krav om at Java er understøttet på operativsystemet. Ubuntu Linux bruges som operativsystem på NSP’en. Til udvikling af komponenten er OS X anvendt.

## Krav til database

Komponenten er testet mod MySQL version 5.5.11. Det er den samme MySQL version som bliver brugt på NSP platformen (NIAB version 1.1.3).

## Krav til hardware

Der er nogle minimumskrav for at kunne afvikle komponenten fornuftigt til test formål. Dog skal man forvente at bruge high-end hardware (både cpu, ram, netkort & diske) for at kunne opfylde svartidskravene på NSP platformen.

Minimumskravene, for fornuftig performance på et test-setup er:

* Intel Core 2 eller lignende CPU
* 8+ GB ram
* Nødvendig harddisk plads for at kunne håndtere alle logfilerne (100+ GB)
* Hurtig harddisk setup (RAID og/eller SSD) for at sikre god performance på SQL databasen

# Artefakter

MinLog er baseret på 2 projekter, der danner en WAR fil hver.

## Minlog-ws

Dette projekt danner webservicen, der skal deployes på NSP platformen.

## Minlog-export

Dette projekt danner splunkjobbet og oprydningsjobbet, der skal deployes på DoDi platformen.

Detaljer omkring navne på warfiler og servicesnitflader og overvågning findes i Driftsvejledningen.

# Konfiguration

De fleste af konfigurationsfilerne skal ligge i jBoss serverinstansens conf bibliotek - f.eks. server/default/conf/log4j-minlog.xml.

Desuden er web-applikationen konfigureret med standard indstillinger, der kan overskrives ved at ligge minlog."brugernavn".properties og/eller jdbc."brugernavn".properties i conf. Hvor "brugernavn" er brugeren der kører web-applikationen - f.eks. server/default/conf/minlog.**jboss**.properties som brugeren hedder på NIAB imaget.

## Standard indstillinger

minlog.splunk.host=localhost

minlog.splunk.port=8089

minlog.splunk.user=admin

minlog.splunk.password=minlog

minlog.splunk.schema=http

minlog.splunk.query=search index=main sourcetype=minlog (\_indextime > %d AND \_indextime < %d) | fields %s | sort by \_indextime asc

minlog.import.sleep=2000

minlog.import.cron=0 \* \* \* \* ?

minlog.import.delay=30000

minlog.cleanup.cron=0 0 \* \* \* ?

sosi.production=0

sosi.canSkipSosi=0

jdbc.url=jdbc:mysql://localhost:3306/minlog

jdbc.username=minlog

jdbc.password=

min.splunk.\\* Bestemmer opsætningen til splunk forbindelsen.

min.import.sleep Splunk requestet kører asynkront, der bliver derfor lavet buzy-spinning for at undersøge hvornår jobbet er færdigt. Sleep er tiden jobbet sover imellem hvert tjek.

min.import.cron Cron til start af splunk.

min.import.delay Splunk henter data fra nu - delay

minlog.cleanup.cron Cron til start af oprydningsjobbet.

sosi.production bestemmer om koden bruger SOSIFederation eller SOSITestFederation.

sosi.canSkipSosi bestemmer om hvorvidt sikkerhedstjekket fejler hvis securityheaderen ikke er korrekt.

jdbc.\\* Opsætning af database forbindelse.

Bemærk at der til minlog.import.cron og minlog.cleanup.cron bruges Quartz - CronTrigger notation <http://www.quartz-scheduler.org/documentation/quartz-2.x/tutorials/tutorial-lesson-06>

## Logning

Minlog kræver, at der ligger en log4j-minlog.xml og en log4j.dtd i conf, disse bruges til at konfigurere Minlogs log4j.

For at SLALog skal fungere skal der ligge en nspslalog-minlog.properties i conf. SLALog konfiguration er for minlog-ws projektet alene.

default.properties, jdbc.default.properties, log4j-minlog.xml, log4j.dtd samt nspslalog-minlog.properties ligger alle sammen i artifakten under WEB-INF/classes eller i repositoriet under hhv minlog-ws/src/main/resources og minlog-export/src/main/resources

## Database

Minlog kræver en mysql database og er testet imod MySQL 5.5.11.

Database opsætningen ligger i minlog-export/src/main/resources/db/migration og skal køres efter versionsnummer. Scriptsene antager at der i forvejen er oprettet en database ved navn minlog.

# Ændringslog

| Version | Dato | Ændring | Ansvarlig |
| --- | --- | --- | --- |
| 0.1 | 2012-06-28 | Initielt Dokument | Trifork |
| 1.2 | 2012-11-22 | Tilføjet minlog.splunk.query property | Trifork A/S |