Minlog – Splunk opsamling og udstillelse

Driftsvejledning

Indholdsfortegnelse

[1 Formål 3](#_Toc329173869)

[2 Indeholdte komponenter 4](#_Toc329173870)

[2.1 Splunkjob & Oprydningsjob 4](#_Toc329173871)

[2.2 Webservice 4](#_Toc329173872)

[3 Logning 5](#_Toc329173873)

[3.1 SLA Logning 5](#_Toc329173874)

[3.2 System Logning 5](#_Toc329173875)

[4 Adgangskontrol / Whitelisting 6](#_Toc329173876)

[5 Overvågning 7](#_Toc329173877)

[6 Yderligere informationer 8](#_Toc329173878)

[6.1 Manglende øvre grænse af antal records. 8](#_Toc329173879)

[6.2 Transaktionsproblematik 8](#_Toc329173880)

[7 Ændringslog 9](#_Toc329173881)

# Formål

Dokument målrettet systemadministratorer og driftspersoner, som skal kunne håndtere driftsmæssige aspekter af komponenten.

Driftsvejledningen skal indeholde information om komponentens version, standard placering af logfiler og konfigurationsfiler, eksterne afhængigheder, og evt. krav til genstart af applikationer hvis komponenten bliver ikke-responsiv.

Start/stop vejledning for komponenten beskrives, herunder hvilke andre applikationer der evt. skal genstartes.

Kendte fejlkoder som skrives i logfiler dokumenteres, så disse evt. kan overvåges, og tillige danne baggrund for fejlsøgning. En generel læsevejledning til logfiler vedlægges.

Det bør angives hvorledes komponenten bedst lader sig overvåge, dvs. en generisk beskrivelse af overvågningen, der ikke er værktøjsafhængig.

Evt. specielle krav til backup beskrives, ligesom procedure ved reetablering af komponenten ud fra backup beskrives.

# Indeholdte komponenter

Der er 3 logiske komponenter, bygget som 2 fysiske WAR filer, der skal deployes på hhv. DoDi og NSP platformene.

## Splunkjob & Oprydningsjob

Disse komponenter skal deployes på DoDi platformen

Binære fil: minlog-export.war

Overvågnings URL: <context-root>/checkall.jsp

## Webservice

Denne komponent skal deployes på NSP platformen

Binære fil: minlog-ws.war

Overvågnings URL: <context-root>/checkall.jsp

# Logning

## SLA Logning

Til SLA logning anvendes NSP-Util, og selve logfilen kan findes i JBoss serverens log folder, såfremt konfigurationen nspslalog-minlog.properties er blevet lagt i JBoss conf folderen.

## System Logning

Til almindelig systemlogning anvendes log4j, og konfigurationen af samme gøres via filerne log4j-minlog.xml og log4j.dtd, der skal lægges i JBoss conf folderen.

# Adgangskontrol / Whitelisting

Adgang til webservicen styres via whitelisting af CVR nummer. Der er oprettet en tabel der indeholder de CVR numre der har adgang til servicen.

For at give en ny bruger adgang, kan man anvende følgende SQL statement. Værdien ’12345678’ skal erstattes med det faktiske CVR nummer

INSERT INTO whitelist (legal\_cvr, name)

VALUES (’12345678’, ’minlog’);

# Overvågning

Der kan køres en SmokeTest på /jsp/checkall.jsp, som tjekker interne afhængigheder. Hvis der returneres andet end http status 200, betyder det at applikationen ikke virker som den skal.

# Yderligere informationer

Dokumentet ’Installationsvejledning’ indeholder en lang række oplysninger der er relevante i forbindelse med både installation og drift af kompontenen.

## Manglende øvre grænse af antal records.

Udtrækket fra splunk medtager ALLE records som er nyere end et givet tidspunkt. Der er ikke nogen øvre grænse for antallet af records der behandles. Kørslen sker som en databasetransaktion. Dette kan teoretisk give problemer, såfremt splunk-udtrækket er nede i en periode, så antallet af records der mangler at blive behandlet er stort. Problemer kan enten være i form af hukommelsesforbrug på den JBoss der afvikler jobbet - eller ved at overskride den øvre grænse for hvad databasen kan håndtere i en transaktion.

Såfremt dette problem opstår i praksis kan det formentlig løses af driften ved at flytte entries fra splunk til en temporær placering, starte jobbet, og herefter løbende flytte entries tilbage til splunk. Men det vil naturligvis være forbundet med ekstra nedetid, før jobbet atter kommer op.

## Transaktionsproblematik

Kode inspektionen afslørede en fejl med hensyn til håndtering af transaktioner. Fejlen kunne have medført at sporingen af hvilke indgange der var hentet fra splunk, ikke blev opdateret korrekt. Så fejlen kunne have medført at handlinger optræder flere gange i Min Log - men altså ikke til tab af data. Fejlrettelsen er verificeret ved kodeinspektion, men er ikke blevet testet.

# Ændringslog

| Version | Dato | Ændring | Ansvarlig |
| --- | --- | --- | --- |
| 0.1 | 2012-06-28 | Initielt Dokument | Trifork |
| 1.2 | 2012-11-22 | Fixed mindre typo | Trifork |