DIGITAL SUNDHED
SAMMENHÆNGENDE DIGITAL SUNDHED I DANMARK

SOSIGW

- **Driftsvejledning for SOSIGW 1.2**

Indeks

Revisionshistorik

Version	Dato	Ændring	Ansvarlig
1	09/10/09	Initiel version af dokument	jre
2	15/10/09	Formattering	jre
3	06/12/10	Bootstrap snitflade	bbg
4	29/08/13	Segmentering af anvendere	CHE

Introduktion

Dette dokument beskriver hvilke driftsovervejelser, der er i forbindelse med SOSIGW. Desuden indeholder dokumentet en sikkerhedsvejledning, der beskriver hvilke sikkerhedsovervejelser, der bør indgå i driften.

Det anbefales derudover at læse ”Installationsvejledning for SOSI-GW – NSP”, idet dette dokument indeholder yderligere instrukser i forhold til segmentering af anvendere og ændrede muligheder ved placering af GW **foran** DCC.

Kontrol af korrekt driftstilstand

Følgende er tegn på en god drift

- Der bør ikke forekomme linier med teksten ”ERROR” i logfilerne.
- Det bør være muligt at logge på administrationskonsollen. På en default installation ligger konsollen på http://localhost:8080/sosigw/console/
- Hvis systemet benyttes af brugerne, ligger nyligt gennemførte webservice-requests i audit-loggen i databasen. Disse kan ses i administrationskonsollen.
- Der bør ikke være linier, der ligner følgende i loggen:

  ```
  ”WARN  [IntercomImpl] Server silent:
  10.0.0.44.3491112d08cf3ed9”
  ```

  De kan dog forekomme, nemlig ved rullende opgradering og andre kontrollerede begivenheder uden at det er tegn på fare. Hvis de kommer i større mængder uden at årsagen til hver af dem kendes, bør det undersøges nærmere. Sandsynlige årsager er overbelastning af serverne eller pakketab på intra-cluster nettet.
- Følgende besked tyder også på, at noget er galt. Med stor sandsynlighed er forbindelsen til den lokale database forsvundet:

  ```
  ”ERROR  [AuditLog] Unable to audit-log due to overflow in
  queue”
  ```

En korrekt kørende SOSIGW-knude har både en servlet container, fx Tomcat eller Trifork T4, og en PostgreSQL-database kørende. Hver knude er desuden forbundet

til en central logningsdatabase. Den centrale logningsdatabase kan tages offline uden at de enkelte knuder påvirkes, da de automatisk vil koble på den igen når den kommer op.

Ændring af statisk konfiguration

SOSIGW indeholder en række statiske konfigurationsmuligheder, der primært henvender sig til tuning af clustering-mekanismen. Disse indstillinger ligger i en properties-fil et af følgende steder:

- Tomcat: $CATALINA_HOME/conf/sosigw-staticconf.properties
- Trifork T4: $DOMAIN_DIR/config/$SERVER_NAME/sosigw-staticconf.properties

Ændringer i denne fil kræver genstart af serveren. Filen gælder kun lokalt, så hvis statisk konfiguration skal være ens på alle knuder i et cluster, skal filen manuelt kopieres rundt, fx via rsync eller lignende.

Se ”Appendix A - Statiske konfigurations parametre” for en beskrivelse af hver enkelt parameter.

Logfil

Der logges til en SOSIGW-specifik logfil samt til stdout på serveren. SOSIGW-loggen hedder sosigw.log og ligger det sted, hvor serveren blev startet fra. Ønskes en anden placering, kan log4j-sosigw.xml tilpasses. Placeringen af denne fil er beskrevet under installationsproceduren.

Som standard roteres logfilen automatisk når den fylder 20 MB. Dette kan ligeledes tilpasses i log4j-sosigw.xml. Ændringer i filen aktiveres automatisk uden at serveren skal genstartes.

Til fejlfinding kan debug levels kobles til. Det gøres ved at sættes level til DEBUG på de category-elementer, der ligger under com.trifork.sosigw.

Backup

Følgende elementer bør der tages backup af løbende:

- Den globale databaseinstans, der indeholder auditlog for det samlede cluster
- Mindst en af de lokale databaser, primært med henblik på at have en backup af den delte konfiguration
- Der kan også tages backup af alle de lokale databaser, med det formål at sikre audit-data hvis den globale instans bryder sammen. Bemærk dog, at hvis der fx tages backup en gang i døgnet, så er sandynligheden for at miste audit-data ved nedbrud på de lokale knuder formentligt ikke mindsket væsentligt. Sørg i stedet for at køre et RAID1-disksystem på knuderne.

- Det er ikke kritisk at tage backup af filsystemerne, da der ikke opbevares tilstand her. Af hensyn til reetablering kan det dog være en god ide.

Start/genstart af service

En SOSIGW-instans kan frit genstartes uden at skulle klargøre genstarten på andre knuder. Genstart foregår via containerens normale mekanismer.

For at en knude er fuldt funktionel, kræves det at der både er en kørende applikationsserver og Postgresql database. De to komponenter kan dog godt startes hver for sig, og en bestemt start/stop-rækkefølge er ikke påkrævet. Selve applikationen kan også fungere i en periode uden lokal database, dog er der en mulighed for at audit-beskeder går tabt hvis den interne beskedkø bliver fyldt. Sker det vil loggen indeholde linjer med ”Unable to audit-log due to overflow in queue”

Opgradering

SOSIGW understøtter rullende opgradering. Det betyder, at i et cluster kan hver knude opgraderes enkeltvis uden at tage hele clusteret ned. Rullende opgradering kan kun foregå mellem to versioner – dvs et cluster i version 1 kan opgraderes til version 2, men for at komme til version 3, så skal alle knuder være på version 2.

Sikkerhedsvejledning for SOSI-Gateway

SOSI-GW ventes benyttet til at videresende personfølsomme oplysninger og skal derfor beskyttes passende mod misbrug.

Netværksforbindelser

SOSI-GW skal tilkobles et beskyttet net, hvor der er tillid til alle maskiner med adgang til at sende pakker til SOSI-GW. Dette er nævnt som en forudsætning i krav-specifikationen for SOSI-GW. Det er en del af grundlaget for løsningen, at nettet er sikkert og der er derfor ikke indbygget nogen form for beskyttelse i form af f.eks. kryptering i kommunikationen.

Det er sikkerhedsmæssigt strengt nødvendigt (og performancemæssigt en god ide) at benytte to netkort (eller VLAN) i serverne, og konfigurere dem til at benytte et separat, lukket, net til intra-cluster kommunikationen. Dette gøres ved at specificere et IP-prefix for det lukkede net i den statiske konfiguration af SOSI-GW, ved at sætte ”cluster.ip.prefix” i filen ”sosigw-staticconf.properties” til det prefix, der entydigt identificerer det lukkede net. Herefter lytter SOSI-GW kun på det net efter nye medlemmer af clusteret. Dette er vigtigt, da medlemmerne af clusteret stoler på at alle andre på multicast-kanalen også venligtsindede medlemmer af samme cluster, og derfor ikke laver nogen validering af det de modtager over multicast. Man kan derfor let overtage kontrollen med clusteret, hvis ikke cluster-trafikken udveksles på et separat lukket net.

Det anbefales at benytte en HTTP-loadbalancer, der kan filtrere på URL'en og benytte en opsætning med følgende egenskaber: (Url'erne er præfikser af det, som de default er sat til i web.xml)

- Kald til ”/browsersign/” skal tillades fra alle klientmaskiner, da den benyttes til at underskrive ID-kort fra browsere, der af natur afvikles på klientmaskinerne.
- Kald til ”/proxy/soap-request/” og ”/service/sosigw” bør kun være mulige fra udvalgte maskiner, formentlig EPJ-system servere. Hvis det er nødvendigt at benytte webservices gennem SOSI-GW fra klient-maskiner på nettet, bør der anvendes restriktioner i SOSI-GW til at begrænse hvilke services, der må kaldes fra klienterne. Disse opsættes gennem administrationskonsollen.
- Kald til ”/service/sosigw-restricted” kan til gengæld udstilles til et bredere publikum, da denne snitflade kun udstiller enkelte håndtag til at oprette nye idkort. Det er meningen at denne snitflade skal bruges fra SignOn Biblioteket.
- Kald til ”/com.trifork.sosigw.console.ConsoleApp/”, ”/console/” og ”/login/” skal kunne benyttes fra maskiner, hvor man skal kunne komme til administrationkonsollen. Selve konsollen beskytter sig selv ved at kræve login med OCES digital signatur, men det er god praksis at begrænse adgangen mest muligt.

Adgang til administrationskonsollen i SOSI-GW

Adgangen til administrationkonsollen er beskyttet ved at kræve at brugeren logger in med sin digitale signatur i den browser, der benyttes. Der gemmes en ”session cookie” i browseren og sessionen lever dermed indtil browser-vinduet lukkes.

Gennem administrationkonsollen opsættes hvilke brugere, identificeret ved deres CPR-nummer, der har lov at benytte administrationskonsollen. Som beskrevet i installationsvejledning er det muligt at omgå dette login ved at starte SOSI-GW i ”bootstrap mode”, så man kan få den første bruger eller to registreret. Bemærk at dette også kan benyttes til at tilføje uautoriserede brugere, hvis det er muligt for en fjentligt sindet bruger at sende pakker ind på ”intra-cluster” nettet.

Adgang til filsystemet på serverne

Filsystemet indeholder som udgangspunkt ikke noget følsomt, men det bør naturligvis ikke være muligt for uautoriserede personer at rette i konfiguration eller program. Der logges normalt ikke følsomme data til filsystemet, med mindre dele af systemet sættes til at logge på niveau ”DEBUG”.

Adgang til databaser

Som beskrevet i installationsvejledningen benyttes to databaser, en ”lokal” og en ”global”. De indeholder begge følsomme oplysninger og bør beskyttes mod uautoriseret adgang. Den lokale database bør sættes til kun at ville kommunikere med lokale processer, da det begrænser angrebsmulighederne til personer, der kan få adgang til maskinen. Den globale bør ligeledes begrænses til kun at ville kommunikere med maskiner, der kører SOSI-GW, eller i det mindste et begrænset netværk.

Der bør oprettes brugere med ”bedre” adgangskoder, end de, der er brugt som eksempler i konfigurationsfilerne. Eksemplerne er kun tænkt til udvikler-brug.

Logning

SOSI-GW logger i den globale database nøgleoplysninger om hvert webservice-kald, der gennemføres gennem den til service-udbydere. Disse kan fremsøges i administrationskonsollen. Denne logning er nødvendig i tilfælde af misbrug, da serviceudbyderen kun kan føre kaldet tilbage til SOSI-GW, som så må konsulteres for at opklare hvilken IP-adresse kaldet oprindeligt kom fra.

Brug af SOSI-GW som ”webservice-firewall”

Man kan forestille sig at man har et net, man ønsker at beskytte mod uautoriserede webservice-kald, f.eks. sundhedsdatanettet. En anvendelse af SOSI-GW er at konfigurere sit netværk, så kun medlemmer af SOSI-GW clusteret kan sende webservice-kald ud på sundhedsdatanettet, og så benytte adgangskontrollen indbygget i SOSI-GW til at styre hvilke applikationer og maskiner, der får lov til at kalde hvilke services på sundhedsdatanettet.

Appendix A - Statiske konfigurations parametre

Nedenfor beskrives de forskellige parametre der kan indstilles og hvad de gør.

cluster.ip.prefix

Afgør hvilket interface der benyttes til intra-cluster kommunkation, hvis der ikke er sat nogen værdi lyttes på alle interfaces.
Det anbefales at intra-cluster kommunikation foregår på et separat IP-subnet eller endnu bedre et separat VLAN.
Da det er et prefix kan værdien fx være "10.", "192.168.", "172.17."

cluster.multicast.ip.address

Intra-cluster multicast adresse, skal i kombination med port være unik for hver SOSI-GW cluster.

cluster.multicast.ip.port

Port der benyttes til intra-cluster multicast

sosigw.mode

Hvad "mode" skal sosi-gw køre i, kan antage en af værdierne 'production', 'test', 'developer' eller 'bootstrap'

sosigw.mode=developer

En nem måde at få sosi-gw til at køre lokalt.
Slår brugen af database, auditlogging, clustering og login tjek på konsollen fra, derudover slås adgangstjek for webservices for både klient og server.
Bruger TEST-STS service, og kommunikere ikke med andre clustre medlemmer.

sosigw.mode=production

Slår fuld funktionalitet til og benytter produktions STS service.
Kræver at lokal og global database er korrekt konfigureret, og kører i et cluster hvis mere end en node er tilstede.

sosigw.mode=test

Som produktion men benytter TEST STS.

sosigw.mode=bootstrap

Får sosi-gw til at starte i begrænset mode, hvor kun konsollen er tilgængelig og der ikke kræves autorisation.
Det er ment som en måde at få sosi-gw gjort klar første gang den startes, eller ved nødstilfælde hvor der ikke findes et gyldigt login.
Kræver lokal database for at konfigurationsændringerne gemmes.
Kan ikke servicere requests og benytter ikke STS i denne mode.

sosigw.slalog

Slå sla-logging til, bemærk at når sosi-gw er i produktion mode vil denne indstilling ignoreres da sla-logging altid er aktiv i produktion.

fmk.isalive.url

Bruges fra "check pages", til at validere at FMK er oppe.

dgws.version
Hvilken version af DGWS som supporteres, gyldige værdier er 1.0 eller 1.0.1, skal matche den version som klient applikationerne benytter.
Hvis begge versioner ønskes, er det nødvendig at have to parallele sosi-gw kørende.

jdbc.driver
Hvilken JDBC driver der skal benyttes, følgende er understøttet:
jdbc.driver=org.gjt.mm.mysql.Driver
jdbc.driver=org.mysql.Driver
jdbc.driver=org.postgresql.Driver
jdbc.driver=org.hsqldb.jdbcDriver

jdbc.datasource
Navnet på den datasource der slåes op i jndi.

global.auditlog.enabled
Hvis slået til vil sosi-gw samle audit log linjer fra alle sosi-gw instanser til en global auditlog database.
Bemærk, auditlog søgning i konsollen benytter den globale auditlog database, så hvis denne slås fra, vil auditlog søgning også slås fra.

auditlog.to.db.enabled
Om der skal auditlogges til database, bemærk log4j altid er slået til.

restricted.webservice.enabled
Slå den begrænsede version af signon webservicen på /service/sosigw-restricted til eller fra.
Den begrænsede webservice er beregnet til brug med "Signon Library" og er et duplikat af den fulde webservice /services/sosigw med logout og getValidIdCard fjernet.

runtimeconfig.storage.type
Kan sættes til db eller properties
Hvis db vælges læses konfigurationen fra den lokale database, for de forskellige instanser.
Hvis properties vælges læses konfigurationen fra sosigw-staticconf.properties, konsollen slås fra og konfigurationen bliver ikke propageret mellem de forskellige cluster medlemmer.

runtimeconfig.general.browsersigning.url
Url klienten skal benytte for at få browsersigning på denne sosi-gw cluster.
Hvis cache partitionering er slået til kan man sætte url op for hver partition som sådan her:
runtimeconfig.general.browsersigning.url.1=partition1.url
runtimeconfig.general.browsersigning.url.2=partition2.url
osv.

runtimeconfig.general.sts.service.url
Url til den STS service der skal benyttes, kan være en liste url'er der prøves i rækkefølge, url'erne skal være adskil med mellemrum.

runtimeconfig.general.globaldb.jdbc.url
Jdbc connection streng til den globale auditlog database.

runtimeconfig.general.globaldb.jdbc.username
Brugernavn til den globale audit log database.

runtimeconfig.general.globaldb.jdbc.password
Password til den globale audit log database

runtimeconfig.general.globaldb.transmit.interval
Hvor tit audit logs flyttes fra den lokale audit log til den globale, i millisekunder.

runtimeconfig.general.careprovider.cvr
CVR på den organisation der kører sosi-gw, brug 19343634 til test.

runtimeconfig.general.careprovider.cvr.name
Navnet på den organisation der kører sosi-gw, benyt SOSITEST i test.

runtimeconfig.general.idcard.signing.timeout
Antal sekunder der må gå fra man har bedt om en digest/url til man skal have startet en browser signerings session.

runtimeconfig.general.browser.signing.timeout
Antal sekunder der må gå fra man har startet browser signerings appletten til browseren skal have sendt det signerede digest.

runtimeconfig.general.sts.number.failures.before.open.cb
Antal gange kald til STSen må fejle før circuit breakeren åbner.

runtimeconfig.general.sts.millis.before.attempting.close.cb
Antal millisekunder der skal gå før circuit breakeren igen forsøger at lukke.

runtimeconfig.general.sts.timeout.millis
Tid(i millisekunder) der ventes på svar på STS forespørgsler.

runtimeconfig.general.cache-partitioning.enabled
Skal idkort cachen være partitioneret, baseret på indholdet af en http-header (se nedenfor)

runtimeconfig.general.cache-partitioning.http-header.name
Navnet på den http-header der indeholder det partionId der skal bruges (ignoreres hvis partitionering er slået fra).

runtimeconfig.general.decoupling-component.url
Url til den "Decoupling Component" der skal modtage forespørgsler der ikke indeholder en WSAddressing i headeren.

runtimeconfig.general.pass-through-on-signature.enabled
Hvis denne er slået til vil sosi-gw ikke udskifte idkort på forespørgsler der allerede har en, signatur med digest, signatur værdi og certificate element.

*runtimeconfig.clientaccesswhitelist.**
Klient whitelisting liste, kan forekomme mere end en gang, * udskiftes med et unikt alias for den klient der ønskes whitelistes.
Formatet på værdien er "IP-adresse, Salt, Kommentar" IP-adressen behøver ikke være en hel IP, der matches på begyndelsen, så fx hvis 10.0. er valgt vil den matche alle ip'er der starter med 10.0.
Hvis både IP-adresse og Salt er angivet tjekkes begge dele.
Eks på en klient whitelist:
runtimeconfig.clientaccesswhitelist.fromthelb=9.0.5.,,From the LB

*runtimeconfig.servicepreservewsa.**
Liste med services hvor To og Action i WSAddressing ønskes bevaret, kan forekomme mere end en gang, * udskiftes blot med et unikt alias.
Indeholdet skal være en komma separeret liste med formatet "WS-Addressing-to regexp, WS-Addressing-action regexp, Kommentar".
WS-Addressing-to & WS-Addressing-action skal indeholde regex som matches med det der kommer i forespørgsler.

Eksempel hvor alt der er til trifork.lms.trifork.com eller ip 195.80.250.83, ikke vil få fjernet To og Action:
`runtimeconfig.servicepreservewsa.fmk=.*(trifork\\.lms\\.trifork\\.com|195\\.80\\.250\\.83).*,.*,FaellesMedicinKort`

runtimeconfig.serviceaccesswhitelist.openaccess=.,.*,Open access*
Liste med services der er whitelistet, kan forekomme mere end en gang, * udskiftes blot med et unikt alias.
Indeholdet skal være en komma separeret liste med formatet "WS-Addressing-to regexp,WS-Addressing-action regexp, Comment".
WS-Addressing-to & WS-Addressing-action skal indeholde regex som matches med det der kommer i forespørgsler.

Eksempel der åbner for alle services:
runtimeconfig.serviceaccesswhitelist.openaccess=.*,.*,Open access

runtimeconfig.general.nspflowid.http-header.name
Navnet på den http header proxy'en læser og sender videre til den kaldte service.
Default værdien er X_NSP_FLOWID.

runtimeconfig.general. proxy-requestid.http-header.name
Navnet på en http header proxy'en genererer og sætter ind som http header til den kaldte service.

Default værdien er X_NSP_PROXY_REQUESTID.