hyväksymispäivä arvosana

arvostelija

Valvonta palvelusuuntautuneissa järjestelmissä

Sampo Lehtinen

Helsinki 12.5.2009

Seminaarityö

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Tietojenkäsittelytieteen laitos

Tekijä — Författare — Author
Sampo Lehtinen

Työn nimi — Arbetets titel — Title

Valvonta palvelusuuntautuneissa järjestelmissä

Oppiaine — Läroämne — Subject
Tietojenkäsittelytiede

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Seminaarityö	12.5.2009	11 sivua

Tiivistelmä — Referat — Abstract

Tiivistelmä. Tämä kirjoitetaan lopuksi.

ACM Computing Classification System (CCS):

Avainsanat — Nyckelord — Keywords
keywords

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

Sisältö

1 Johdanto

Keskittyminen ydinosaamiseen, ulkoistaminen, ketteryys, just-in-time ja verkostot ovat olleet vahvoja trendejä viime vuosina yritysmaailmassa. Yritykset ovat karsineet palveluita, jotka ne tuottivat ennen itse itselleen ja keskittyneet ydinosaamiseensa. Sellainen tukitoiminto tai ydinosaamisen kannalta välttämätön palvelu, joka itse tuotettuna ei tuota markkinoiden muihin toimijoihin nähden kilpailuetua, voidaan ulkoistaa. Ulkoistettu palvelu hankitaan avoimilta markkinoilta joko pitkäaikaisin sopimuksin tai kulloisenkin tarpeen mukaan.

Erikoistuminen ja keskittyminen eivät ole aivan uusia asioita. Harvempi yritys menneisyydessäkään perusti pankkia, vaikka pankin palveluita olisikin tarvinnut. Nämä sähköistä kaupankäyntiä ja Internetiä edeltäneenä aikana ulkopuolelta hankitut palvelut ovat kuitenkin organisaation kannalta katsottuna saman tapaisessa asemassa kuin muut ulkoistettavaksi soveltuvat palvelut: ne sähköistyvät, muuttuvat paperittomiksi ja niiden automaatioaste nousee.

Ulkoistamisella pyritään hankkimaan yritykselle kilpailuetua. Keskittyminen ydinosaamiseen voi kuitenkin synnyttää uusia riskejä tai kasvattaa jo aiemmin olemassa olleiden riskien toteutumisen todennäköisyyttä ja seurauksien vakavuutta.

Jos aiemmin jonkin tietyn asian valmistumisen odotettiin kestävän esimerkiksi neljä viikkoa, ei muutaman päivän viipeestä ollut merkityksellistä haittaa, sillä niin raaka-aineiden kuin valmisteidenkin varastot olivat nykyistä suurempia. Työntekijät hoitivat tarvittavan valvonnan omien töidensä ohessa. Nykyaikainen huipputehokas kokoonpanolinja muistuttaa kuitenkin enemmän logistiikkakeskusta, koska juuri mitään ei varastoida. Organisaatioiden riippuvuus erilaisten palveluiden toimintavarmuudesta on siis kasvanut. Toimimaton palvelu aiheuttaa entistä nopeammin ja entistä suurempia ongelmia. Jo yhdenkin komponenttitoimituksen viivästyminen saattaa aiheuttaa suuret vahingot komponenttien sujuvista toimituksista kokoonpanolinjalle riippuvaiselle yritykselle.

Palveluiden, niitä tuottavien järjestelmien tai verkoston kumppanien valvonta ja poikkeuksien havaitseminen sekä niihin oikealla tavalla reagoiminen on yhä oleellisempi osa yhä useamman nykyaikaisen organisaation toimintaa.

Tässä seminaarityössäni pureudun erilaisiin tapoihin toteuttaa palvelusuuntautuneesti toimivissa organisaatioissa ja niiden järjestelmissä tarvittavaa automatisoitua valvontaa ja poikkeustilanteisiin reagoimista. Tarkastelen valvontaa sekä järjestelmän ylläpidon että palvelusuuntautuneisuuden kannalta. Käsittelen myös valvon-

taan ja reagointiin liittyviä ongelma.

2 Sosioteknisten ja palvelusuuntautuneiden järjestelmien valvonnasta

Sosioteknisillä järjestelmillä tarkoitetaan jonkin tarkoituksen täyttämiseksi olemassa olevia tietokonejärjestelmistä ja niitä käyttävistä ihmisistä muodostuvaa kokonaisuutta [Som07, s. 21-22].

Palvelusuuntautuneilla järjestelmillä tarkoitetaan avoimia, hajautettuja ja löyhästi kytkettyjä järjestelmiä [Som07, s. 747]. Palvelusuuntautuneisuus on nykyaikainen järjestelmien suunnittelussa ja toteutuksessa käytetty paradigma. Sitä pidetään yleisesti merkittävänä askeleena ohjelmistotekniikalle, erityisesti liiketoimintajärjestelmille (business application systems) [Som07, s. 744]. Palvelusuunntautuneisuus perustuu kuvauskeskeisyyteen ja toteutukseltaan W3C:n määrittelemiin WDSL-kuvauskieleen [W3C01] ja SOAP-protokollaan [W3C07].

Mikäli tarkastelemme vain palvelusuuntautuneen järjestelmän teknisiä osia emmekä mahdollisia inhimillisiä osia, ei palvelusuuntautuneessa järjestelmässä ole valvonnan kannalta suuria eroja muunlaisten järjestelmän valvontaan. Selkeimmän eron www-palvelimen valvontaan verrattuna muodostaa tiedon kulkeminen SOAP-sanoman sisällä eikä suoraan http-yhteyden kuormassa. Tämä vähentää mahdollisuuksia hyödyntää www-palvelimen tai http-protokollan tasolla toimivasta valvonnasta lokitiedostojen kautta saatavaa tietoa, sillä suuri osa oleellisista tiedoista ei päädy lokitiedostoihin [dCL04]. Myös asennuksen osalta järjestelmässä voi olla suuria eroja tavalliseen www-palvelimeen verrattuna, koska varsinainen palvelun suoritus saattaa tapahtua piilossa jollain muulla palvelimella WS-rajapinnan takana.

Näistä eroista huolimatta perinteiset järjestelmien valvonnassa käytetyt työkalut, esimerkiksi Big Sister [Big09] tai Nagios [Nag09], riittävät ominaisuuksiltaan varsin pitkälle. Nagioksen ominaisuuksia on mahdollista laajentaa esimerkiksi Webinject-nimisellä moduulilla, joka mahdollistaa WS-rajapinnan yli tarjottavien palveluiden yksityiskohtaisen ja tilatietoja huomioivan valvonnan [Web09]. Myös nimenomaan palvelusuuntautuneiden järjestelmien valvontaan suunniteltuja tapoja on olemassa [dCL04] [LJH06].

Yritysten tarve valvoa omaan toimintaansa liittyviä riskejä on suuri. Sähköisen toiminnan nopeus ja mahdolliset hyvinkin vakavat seuraukset, jotka pahimmillaan aset-

tavat organisaation olemassaolon jatkumisen kyseenalaiseksi, asettavat tarpeen valvoa organisaation omien teknisten järjestelmien lisäksi organisaation työntekijöiden tekemisiä sekä kumppanien järjestelmiä. Tällaisen valvonnan tarve ei liity pelkästään palvelusuuntautuneisiin järjestelmiin. Organisaation omiin toimiin liittyvää valvontaa kutsutaan sisäiseksi valvonnaksi. Esimerkiksi sisäisen valvonnan epäonnistumiseta käy lontoolaisen Barings Bankin ajautumista konkurssiin johdannaiskaupan johtajan, Nick Leesonin, tekemien luvattomien futuurikauppojen seurauksena vuonna 1995 [Wik09b] [Wik09a]. Hyväkään valvonta ei kuitenkaan ikinä pysty poistamaan kaikkia riskitekijöitä, sillä vaikka valvonta olisi kaikenkattavaa, mikään ei takaa, etteikö valvonnassa voisi olla virheitä.

Yrityksen kannalta yksittäiseen kauppaan tai yksittäiselle asiakkaalle annetujen luottojen suuruudella on merkitystä. Vaikka liikepalveluväyliä käyttämällä sanomat voidaan reitittää siten, että päätöksen luotottamisesta tekee sellainen henkilö, jolla on valtuus ja velvollisuus asiasta päättää, joissain tilanteissa voi olla oleellista tarkastella sanomia myös palomuureihin verrattavilla tekniikoilla. Valvonnan kannalta merkitykselliset tiedot eivät siis rajoitu vain siihen, miten sanomat kulkevat, vaan myös niiden sisältöön. Tällaisessa valvonnassa valvontaan käytettyjen järjestelmien on kyettävä seuraamaan valvomiensa järjestelmien lähettämien ja vastaanottamien sanomien sisällön merkitystä. Valvojan kannalta joissain tilanteissa on myös tarpeen pystyä pysäyttämään ohjeiden vastaiset sanomat eikä vain tyytyä ilmoittamaan niistä eteenpäin. Verrattuna tavallisiin verkkoliikenteen valvonnassa käytettyihin palomuureihin tämä tarkoittaa tilallisuutta ja sovellustason protokollan sanomien sisältöön perustuvia päätöksiä.

3 Monitoroinnista tekniikan näkökulmasta

Valvonnan toteuttamiseen on olemassa useita erilaisia tapoja. Kaikki tavat eivät pysty vastaamaan kaikkiin tarpeisiin, joten valvonnalle asetut vaatimukset vaikuttavat siihen, mitkä tavat tulevat kyseeseen.

3.1 Valvonnalle asetetut vaatimukset

Jaan vaatimukset kahteen luokkaan: reaktiivisiin ja proaktiivisiin. Reaktiiviset vaatimukset voidaan täyttää ilman mahdollisuutta vaikuttaa sanomien kulkuun. Proaktiivisten vaatimuksien täyttämiseksi saatetaan joutua pysäyttämään sääntöjä rikko-

vien sanomien eteneminen. On olemassa myös muita tapoja jakaa valvonta luokkiin, kuten viivästettyyn, aktiiviseen ja proaktiiviseen [MBB95]. Tässä luokittelussa viivästetyllä tarkoitetaan tapahtumien tallentamista lokitiedostoihin ja jälkikäteistä analysointia, aktiivisella lähes reaaliaikaista käsittelyä ilman mahdollisuutta estää tapahtuman toteutumista ja proaktiivisella reaaliaikaista tarkastelua siten, että tarkasteltavan tapahtuman toteutuminen on mahdollista estää.

Jaan reaktiivisen luokan edelleen kahteen osaan sen perusteella, kohdistuuko valvonta myös sanomien sisältöön vai rajoitutaanko seuraamaan järjestelmän kykyä vastata palvelupyyntöihin. Mikäli valvonta ei kohdistu sanomien sisältöön, se ei juurikaan eroa tavallisen www-palvelimen valvonnasta.

Proaktiivisella valvonnala pyritään aktiivisesti estämään ongelmien syntymistä tai pienentämään syntyvistä ongelmista aiheutuvia vahingollisia seurauksia. Reaktiivisessa valvonnassa tyydytään ilmoittamaan ongelmista eteenpäin esimerkiksi operaattorille, keräämään tilastotietoa järjestelmän tai järjestelmän käyttäjien toiminnasta ja näyttämään kootusti tietoja järjestelmien kulloisestakin tilanteesta.

Valvonnan avulla saatuihin tuloksiin pitää kuitenkin suhtautua kriittisesti. Vaikka yrityksen verkko, yhteydet yrityksen verkosta Internet-verkkoon ja Internet-verkon kautta ulkopuolisille tarjottu palvelu läheltä tehdyn mittauksen perusteella olisi saavutettavuudeltaan ja viipeeltään loistava, voi todellisten loppukäyttäjien käyttökokemus erota tästä suurestikin [MeP02]. Tilastollinen tieto joka koskee pelkästään WS-rajapinnan kautta tarjottavan palvelun saavutettavuutta ei myöskään auta mahdollisten vikojen paikantamisessa. Suurimmaksi osaksi www-palveluiden saavuttamattomuus näyttäisi johtuvan muista kuin www-palvelun tarjoajaan liittyvistä syistä [MeP02].

3.2 Erilaisia valvontatapoja

Järjestelmävalvontaan käytettävissä olevia tekniikoita on olemassa useita: lokitiedostojen analysointi, välittäjät ja sovellustason palomuurit, aktiivinen näytteenotto sekä reflektio. Tämä jaottelu erilaisiin luokkiin perustuu siihen, millä keinoin eri tekniikat saavat tietoa valvonnan kohteena olevasta järjestelmästä.

3.2.1 Lokitiedostojen analysointi

WS-rajapinnan kautta tarjottavien palvelujen käyttämät SOAP-sanomat välitetään yleensä http-yhteyden avulla. Http-yhteyksistä huolehtiva palvelinkokonaisuuden osa yleensä tallettaa erilaisia tietoja niin sanottuihin lokitiedostoihin. Www-sivun lataamisesta tai WS-palvelun kutsumisesta jää siis jälki.

Tavallista www-palvelua käyttävän käyttäjän toimia pystytään analysoimaan näiden tietojen perusteella. Käyttäjäkohtaisen klikkausvirran, eli käyttäjän liikkumisen www-sivustolla, muodostaminen onnistuu helposti. Koska WS-palvelun kutsuun liittyvät tiedot kulkevat kuitenkin SOAP-sanomassa, ei www-palvelimen lokitiedostoista yleensä saada tarpeeksi tietoja [dCL04].

Mikäli WS-rajapinnan kautta asiakkaille tarjotun palvelun lähdekoodi on muokattavissa, on mahdollista muokata palvelun toteutus tuottamaan lokitietoja riittävän tarkalla yksityiskohtaisuuden tasolla [dCL04]. Useasti tilanne on kuitenkin se, että tämä ei ylipäänsä ole mahdollista tai riittävän kustannustehokasta.

Lokitiedostoihin perustuvissa malleissa ei valvoja varsinaisesti pääse suoraan tutkimaan sanomia, vaan ainoastaan sanomista tuotettua lokitietoa.

3.2.2 Välittäjät ja sovellustason palomuurit

Palomuureja voidaan käyttää kerättäessä tietoa sen sen kautta kulkevasta liikenteestä. Tarvittaessa liikenne voidaan myös estää, mikäli se on sääntöjen vastaista.

Verkon turvallisuutta lisäämään tarkoitettu palomuuri toimii yleensä ip-, tcp- ja mahdollisesti sovellusprotokollan, esimerkiksi http:n tai ftp:n, tasolla. Tällaisen liikennettä tarkastelevan tavallisen palomuurin avulla ei kuitenkaan ole mahdollista tutkia SOAP-sanomien sisältöä. Ongelma on vastaava kuin analysoitaessa www-palvelimen lokitiedostoja eli se, ettei tarpeellsia tietoja voida tarkastella. Vaikka palomuuri mahdollistaisi http-yhteyden parametrien tarkastelun, se ei ole riittävää, sillä WS-rajapinnan kannalta oleelliset parametrit liikkuvat palvelua kutsuttaessa http-pyynnön POST-metodilla välitetyn SOAP-sanoman sisällä [DdV02]. Vaikka jotkin palomuurit, kuten Linux-järjestelmien Netfilter-palomuuri ip_queue-moduulin avulla, mahdollistavat liikenteen välittämisen palomuurin ulkopuoliselle ohjelmistolle, ei niitä käyttämällä voida helposti ratkaista WS-rajapinan palvelupyyntöjen suodatukseen tai tietojen keräämiseen liittyviä tarpeita.

Palomuuri, joka toimii ip- ja tcp-protokollien tasolla, mahdollistaa WS-rajapinnan

kautta palveluja tarjoavan palvelimen näkyvyyden rajoittamisen. Http-protokollan tasolla toimiva palomuuri tai välittäjä pystyy rajoittamaan näkyvyyttä käyttäen rajaustekijänä yksittäisen palvelun nimieä.

WS-rajapinnan kautta tarjottavan palvelun edustalle voidaan asentaa välittäjä, joka asiakkaan suunnalta katsottuna näyttää palvelulta [DdV02]. Palvelun suuntaan se näyttelee olevansa asiakas. Välittäjän on pelkän tarkkailun lisäksi mahdollista muokata kauttaan kulkevia sanomia tai estää niiden kulkeminen [dCL04]. Välittäjä voi pitää näkemistään sanomista lokitiedostoa tai muutoin mahdollistaa tietojen toimittamisen valvontajärjestelmälle.

3.2.3 Aktiivinen näytteenotto

Aktiivista näytteenottoa valvottavan järjestelmän tai sen tietyn osan toimivuudesta käytetään järjestelmävalvonnan välineissä yleisesti. Esimerkiksi Bigsister [Big09], Nagios [Nag09] ja Smokeping käyttävät tätä tapaa. Valvontajärjestelmä siis lähettää palvelupyynnön valvottavaan järjestelmään ja päättelee saamansa vastauksen perusteella tietoja valvotun järjestelmän tilasta. Yksittäisten kutsujen osalta voidaan olla kiinnostuneita esimerkiksi siitä, saatiinko vastausta ylipäänsä, millaisia viipeitä vastauksen saamiseen liittyi tai palauttiko valvonnan kohteena oleva järjestelmä jonkin virhetilaa ilmaisevan tiedon, johon pitäisi reagoida.

Perinteiset järjestelmävalvonnan työkalut kokoavat tietonsa yleensä valvottavien palvelimien itse keräämistä ja verkon kautta näytteitä ottamalla saaduista tiedoista. Koska tällainen valvonta tapahtuu varsin läheltä valvonnan kohteena olevaa järjestelmää, on huomioitava, ettei se välttämättä kuvaa valvottavan järjestelmän tilaa loppukäyttäjän kannalta [MeP02].

Perinteiset järjestelmävalvonnan työkalut eivät myöskään ilman laajennoksia pysty valvomaan riittävän yksityiskohtaisesti palvelusuuntautuneiden järjestelmien toteutuksessa käytettyjen SOAP-sanomien sisältöä [Web09]. Koska tämänkaltainen valvonta toimii kokonaan valvottavan palvelun ulkopuolella, mutta ei asiakkaan ja valvottavan palvelun välissä, se ei luonnollisestikaan pysty vaikuttamaan yksittäisten sanomien kohtaloon. Se ei siis voi tarvittaessa estää ei-toivottujen sanomien pääsyä läpi.

3.2.4 Reflektio

Reflektiolla tarkoitetaan järjestelmän omaa toimintaansa koskevaa ja mahdollisesti siihen vaikuttavaa toimintaa [Mae87]. Reflektiviinen järjestelmä tarjoaa ulkopuolisille tahoille mahdollisuuden tarkkailla toimintaansa ja vaikuttaa siihen. Ulkopuolisille tarjottujen tietojen tulisi aina olla ajantasaisia [Mae87].

Reflektio kattaa määritelmänsä mukaan huomattavasti enemmän asioita kuin ensisilmäyksellä tulee ajatelleeksi. Muun muassa järjestelmän tehokkuutta koskevan tilastoaineiston kerääminen, virheiden etsinnässä (debuging) käytettyjen tietojen kerääminen ja rajapinnat ovat reflektioita järjestelmästä [Mae87]. Palvelusuuntautuneiden järjestelmien valvonnan kannalta asiakkaalle tarjottua rajapintaa ei kuitenkaan voida pitää reflektiona, sillä sen käyttäminen järjestelmävalvonnassa menisi tässä luokittelussa aktiivisen näytteenoton puolelle.

Reflektiota ovat WS-rajapinnan toteuttamisessa käytettävän sovelluspalvelimen itsestään keräämät ja ulkopuolelle näyttämät tiedot, joiden perusteella voidaan päätellä palvelimen tilaa koskevia tietoja. Yksittäisistä sanomista tai palveluiden toimivuudesta nämä tiedot eivät kuitenkaan kerro mitään.

Palvelusuuntautuneen järjestelmän valvonnan kannalta haluttu reflektio on mahdollista toteuttaa esimerkiksi liittämällä WS-rajapinnan tarjoavan sovelluspalvelimen yhteyteen ohjelmakomponentti, joka saa käsiteltäväkseen palvelupyynnöt ja niihin liittyvät vastaukset. Palvelupyynnöt ohjataan reflektion toteuttavalle komponentille ennen kuin ne päätyvät varsinaiselle palvelun toteutukselle. Vastaavasti palvelun toteutuksen antamat vastaukset ohjataan reflektion toteuttavalle komponentille ennen niiden lähettämistä asiakkaalle. Tapa, jolla reflektion toteuttava komponentti voidaan toteuttaa ja liittää WS-rajapinnan toteuttavaan palvelimeen, vaihtelee eri palvelinten välillä.

3.3 Tarkastuksien taso

Valvonnalla pyritään saamaan tietoa toisaalta valvottavan järjestelmän kulloisestakin tilasta, toisaalta mahdollisista väärinkäytöksistä. Väärinkäytöksien tarkkailussa järjestelmän palvelusuuntautuneisuus asettaa omat vaatimuksensa.

Järjestelmän tilaa kuvaavia muuttujia on useita. Niiden arvoista voidaan muodostaa aikasarjoja, joista taas voidaan nähdä arvon muuttumisen suuntaa ja muutoksen nopeutta. Ongelmatilanteissa valvontajärjestelmän tietojen avulla pyritään arvioi-

maan, mistä ongelma saattaisi aiheutua, ja kohdentamaan vian määritys sen mukaan.

Luotettavuus ja saavutettavuus auttavat ennustamaan mahdollisuuksia selvitä sovitusta palvelun tasosta. Luotettavuudella tarkoitetaan tilastollista todennäköisyyttä sille, toimiiko järjestelmä oikein [PeY07, s 44]. Koska ongelmatilanteet ja viat eivät jakaudu tasaisesti kaikkialle valvottavaan ohjelmistoon, luotettavuden arvo riippuu käyttötavasta [PeY07, s. 44]. Käyttötapakohtaisuuden vuoksi luotettavuudelle saadut arvot ovat suuntaa-antavia, koska valvontajärjestelmän tapa käyttää valvottavaa järjestelmää eroaa todellisten käyttäjien tavasta. Luotettavuus saa erilaisia arvoja esimerkiksi sen mukaan, tehdäänkö mittaus asiakasjärjestelmän lokitiedostoja analysoimalla vai WS-rajapinnan tarjoavan palvelimen reflektoimaa tietoa tarkastelemalla. Asiakkaan ja palvelun välissä olevan verkon toiminnan häiriöt näkyvät asiakkaan näkökulmasta epäluotettavuutena. Tavallisten www-palvelimien epäluotettavuudesta huomattavan suuri osuus aiheutuu välissä olevan verkon ongelmatilanteista [MeP02].

Saavutettavuudella tarkoitetaan sen ajan, jolloin asiakas olisi halutessaan voinut käyttää palvelua, suhdetta siihen aikaan, jolloin asiakkaan olisi pitänyt voida käyttää palvelua [PeY07, s 44]. Esimerkiksi klo 8-16 välillä säätietoja palvelevan järjestelmän, jonka toiminnassa on joka päivä tunnin katko, saavutettavuus on 7/8 eli 87,5 prosenttia. Mikäli säätietoja on tarkoitus palvella vuorokauden ympäri, sama katko vaikutaisi saavutettavuuteen vähemmän (23/24 eli noin 96 prosenttia).

Saavutettavuuden ohella valvonnassa kerätään tietoja muun muassa vasteajoista, palvelun toteuttamiseen osallistuvien palvelimien kuormituksesta verkon, levyjärjestelmän, prosessorin ja muistin osalta, palvelimien lämpötiloista, palvelupyyntöjen lukumäärästä ja palveltujen pyyntöjen yhteydessä annetuista statustiedoista.

Palvelusuuntautuneiden järjestelmien valvonnassa kiinnostuksen kohteina on myös välitettyjen sanomien sisältö.

3.4 Reagointi

Reagointi on joko proaktiivista tai reaktiivista. Proaktiivisella reagoinnilla tarkoitetaan sanoman kulkuun tai sisältöön vaikuttamista. Reaktiivisen valvonnan keinoin sanomien kulkuun tai sisältöön ei voida vaikuttaa. Reaktiivisella valvonnalla voidaan kerätä tilastotietoa järjestelmän tilasta tai sanomista, tallettaa sanomia myöhempää tarkastelua varten tai hälyyttää mahdollisista ongelmista eteenpäin, esimerkiksi jär-

jestelmän ylläpidolle tai jostain tietystä asiasta vastaavalle taholle. Proaktiiviseen valvontaan kykenevä ohjelmakomponentti voi toimia kuten reaktiivinen; se vain ei estä sanomien kulkua tai muuta niiden sisältöä.

4 Yhteenveto ja johtopäätökset

Palvelusuuntautuneisuus ja palvelujen ulkoistaminen helpottavat organisaation keskittymistä ydinosaamiseensa. Valvonnan merkitys korostuu palvelusuuntautuneissa järjestelmissä. Valvonnan merkitystä ja mahdollisuuksia voidaan pohtia toisaalta ylläpidon, toisaalta sanomien tai toimijoiden kannalta.

Palvelusuuntautuneiden järjestelmien valvonta eroaa perinteisten järjestelmien valvonnasta, sillä palvelusuuntautuneissa järjestelmissä on samanaikaisesti kyse sekä organisaatioiden välisestä toiminnasta että toiminnasta, jonka osana on ihmisiä. Järjestelmien valvonnassa ylläpidon kannalta ei ole tarvinnut perinteisesti välittää sanomien sisällöstä tai sen merkityksestä. Tarkastelun kohteena ovat olleet kysymykset siitä, onko järjestelmä saatavilla, ovatko sen vasteajat lyhyitä tai kohtuullisia ja se, ettei kukaan ole käyttänyt järjestelmiä ilman käytön oikeutusta.

Tekniikan näkökulmasta suhtautuminen palvelusuuntautuneen järjestelmän valvontaan on kahtalainen. Valvonnalla voidaan palvelusuuntautuneen järjestelmän kohdalla tarkoittaa joko järjestelmän tilan valvontaa tai yksittäisten sanomien kulun ja sisällön valvontaa. Valvonnan toteutamiseen on useita erilaisia mahdollisuuksia. Osaa näistä voidaan käyttää tuottamaan tietoa tai kontrolloimaan sekä yksittäisten sanomien kulkua että koko järjestelmän tilaa.

Jatkossa olisi mielenkiintoista tarkastella, voitaisiko järjestelmän ylläpidon kannalta tarvittava valvonta toteuttaa perinteisillä järjestelmävalvonnan apuvälineillä riippumatta siitä, onko kyseessä palvelusuuntautunut järjestelmä vai ei. Sanomien kulun ja sisällön kannalta tapahtuvan valvonnan osalta olisi oleellista selvittää, riittävätkö nykyisten liikepalveluväylän toteuttavien tuotteiden ominaisuudet, tai ovatko ne jotenkin laajennettavissa, kattamaan valvonnan tarpeet.

Lähteet

Big09 About big sister, 5 2009. URL http://www.bigsister.ch/bigsister.html. Tarkistettu 9.5.2009.

dCL04 da Cruz, S. M. S., Campos, M. L. M., Pires, P. F. ja Campos, L. M., Monitoring e-business web services usage through a log based architecture. *Web Services, 2004. Proceedings. IEEE International Conference on*, Jul 2004, sivut 61–69, URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1314724.

DdV02 Damiani, E., di Vimercati, S. D. C., Paraboschi, S. ja Samarati, P., Securing soap e-services. *International Journal of Information Security*, 1,2(2002), sivut 100–115. URL http://www.springerlink.com/content/ggk9e2fwg3xq1j14/.

LJH06 Li, Z., Jin, Y. ja Han, J., A runtime monitoring and validation framework for web service. *Software Engineering Conference, 2006. Australian*, Apr 2006, URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1615040.

Mae87 Maes, P., Concepts and experiments in computational reflection. *ACM SIGPLAN Notices*, 22,12(1987), sivut 147–155. URL http://doi.acm.org/10.1145/38807.38821.

MBB95 Milosevic, Z., Berry, A., Bond, A. ja Raymond, K., Supporting business contracts in open distributed systems. *Services in Distributed and Networked Environments, 1995., Second International Workshop on*, 1995, URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=470462.

MeP02 Merzbacher, M. ja Patterson, D., Measuring end-user availability on the web: practical experience. *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, 2002, sivut 473–477, URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1028932.

Nag09 Nagios, 2009. URL http://www.nagios.org/. Tarkistettu 9.5.2009.

PeY07 Pezze, M. ja Young, M., *Software Testing and Analysis: Process, Principles, and Techniques*. Wiley, 2007.

Som07 Sommerville, I., *Software Engineering*. Pearson Education Limited, 8. painos, 2007.

W3C01 W3C, Web services description language (wsdl) 1.1, Mar 2001. URL `http://www.w3.org/TR/wsdl`.

W3C07 W3C, Soap version 1.2, Apr 2007. URL `http://www.w3.org/TR/soap12-part1/`.

Web09 Monitoring web applications/services with nagios and webinject, 5 2009. URL `http://www.webinject.org/plugin.html`. Tarkistettu 9.5.2009.

Wik09a Wikipedia, Barings Bank, 5 2009. URL `http://en.wikipedia.org/wiki/Barings_Bank`. Tarkistettu 9.5.2009.

Wik09b Wikipedia, Nick Leeson, 5 2009. URL `http://en.wikipedia.org/wiki/Nick_Leeson`. Tarkistettu 9.5.2009.