Tampereen ammattikorkeakoulu

Valvontajärjestelmän suunnittelu asiantuntijaorganisaatiossa

Juha Huusko

OPINNÄYTETYÖ
Kesäkuu 2021
Tietojärjestelmäosaamisen tutkinto-ohjelma

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojärjestelmäosaamisen ylempi AMK-tutkinto

HUUSKO, JUHA:
Valvontajärjestelmän suunnittelu asiantuntijaorganisaatiossa

Opinnäytetyö 51 sivua, joista liitteitä 0 sivua
Kesäkuu 2021

Tavoitteena oli luoda perusteet valvontajärjestelmän käyttöönotolle asiantuntijaorganisaatiossa. Valvontajärjestelmän avulla tavoite on vähentää häiriöitä ja kyetä ennakoimaan niitä sekä nopeuttaa viankorjausta. Toimivalla valvontajärjestelmällä voidaan löytää heikkouksia palveluissa ja komponenteissa sekä parantaa asiakastyytyväisyyttä havaitsemalla ongelmat mahdollisesti jo ennen asiakasta. Opinnäytetyön yhteydessä ei luotu valvontajärjestelmää vaan tehtiin edellytyksiä sen luomiselle. Opinnäytetyötyyppi oli toiminnallinen ja sisälsi työelämään liittyvää suunnittelu- ja selvitystyötä.

Opinnäytetyön tarkoituksena oli selvittää tärkeimmät tehtävät, jotka tulee organisaatiossa tehdä ennen valvontajärjestelmän käyttöönottoa. Tarkoitukseen kuului myös saada käsitys siitä, mitä valvontajärjestelmältä vaaditaan sekä kartoittaa hieman minkälaisia valvontajärjestelmiä on olemassa. Valvontajärjestelmien soveltuvuutta tutkittiin vertailemalla muutamaa tunnettua ohjelmistoa erilaisten valvontaan liittyvien ominaisuuksien osalta. Opinnäytetyön annettua perusteet valvontajärjestelmän käyttöönotolle suunniteltiin tiekartta jatkokehitykselle.

Valvontajärjestelmien vertailuun valikoitui muutama hyvä ohjelmisto, ja valinnat perustuivat sekä muutamien asiantuntijoiden kokemuksiin että Internet-hakuihin. Tällä tavalla ei saada välttämättä parasta mahdollista lopputulosta, vaan kokemuksia pitäisi kysyä suuremmalta joukolta asiantuntijoita tai peilata valintaa jo aiemmin aiheesta tehtyyn tutkimukseen. Valvontajärjestelmien koeluontoinen asennus olisi tuonut myös paljon lisätietoa järjestelmien soveltuvuudesta ja ennen kaikkea toimivuudesta, mutta valitettavasti testiasennuksen toteutus ei ollut tällä kertaa mahdollista.

Asiasanat: valvontajärjestelmä, palvelutuotanto, verkonvalvomo, palvelupiste

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Master's Degree Programme in Information System Competence

HUUSKO JUHA
Planning a Monitoring System in an Expert Organization

Master’s thesis 51 pages, appendices 0 pages
June 2021

The aim of the thesis was to create the basis for the introduction of a monitoring system in an expert organization. The eventual goal is to use the monitoring system to reduce and anticipate disturbances and speed up troubleshooting. A functioning monitoring system can be used to identify weaknesses in services and components and to improve customer satisfaction by detecting problems potentially before the customer. In connection with the thesis, no monitoring system was created, but conditions were created for its creation. The thesis type was functional and included planning and study work related to working life.

The main tasks of what should be done in the organization before the introduction of the monitoring system and what is required of the monitoring system were clarified in the thesis. The suitability of the monitoring systems was examined by comparing a few well-known software for different monitoring-related capabilities.

The selection of the compared software was based on the experience of both a few experts and Internet searches. Experimental installation of monitoring systems would have provided much additional information about the suitability and, above all, functionality of the systems, but unfortunately test installation was not possible.

Key words: monitoring system, service production, network operation center, service desk

SISÄLLYS

LYHENTEET JA TERMIT

ITIL	Information Technology Infrastructure Library
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
XML	Extensive Markup Language
JSON	JavaScript Object Notation
MTTR	Mean Time To Repair
MTRS	Mean Time To Restore Service
MTBSI	Mean Time Between Service Incidents
MTBF	Mean Time Between Failures
CSF	Critical Success Factor
KPI	Key Performance Indicator
WMI	Windows Management Instrumentation
SSH	Secure Shell
HTTPS	Hyper Text Transfer Protocol Secure
WinRM	Windows Remote Management
OMI	Open Management Infrastructure
CIM	Common Information Model
REST	Representational State Transfer
API	Application programming interface
SQL	Structured Query Language
IIS	Internet Information Services
HPE	Hewlett-Packard Enterprise
TCP	Transmission Control Protocol
HASH	Tiedoston merkkijonotiivistelmä

1 JOHDANTO

Tietojärjestelmien ja tietoteknisten ympäristöjen kasvaessa on tärkeää, että tiedetään mitä ympäristössä tapahtuu. Valvontajärjestelmän avulla tämä on mahdollista. Valvontajärjestelmä on käytännössä ohjelmisto, joka auttaa keräämään tapahtumat yhteen paikkaan ja suodattamaan, lajittelemaan ja käsittelemään tapahtumia. Ohjelmisto itsessään ei hoida valvontaa riittävän laadukkaasti, vaan valvovan organisaation tulee suunnitella ja tehdä järjestelmän käyttöönotto siten, että siinä otetaan tärkeimmät asiat huomioon. Tässä työssä on pyritty löytämään nuo asiat.

Suunnitteilla olevan valvontajärjestelmän ytimessä on arvon tuottaminen. Opinnäytetyön tavoitteena on suunnitella valvontajärjestelmän käyttöönotto siten, että suunnitelman avulla voidaan ottaa käyttöön läpi organisaation arvoa tuottava valvontajärjestelmä. Tietojärjestelmien käyttäjille arvoa tuottaa etenkin parempi käyttökokemus, lyhyemmät tai harvinaisemmat katkot, järjestelmissä tuotettujen tuotteiden laadun paraneminen sekä nopeammin saapuvat häiriötiedotteet. Päivystäjät saavat vähemmän vikailmoituksia, kun vioista ehditään tiedottamaan ennen kuin asiakkaat huomaavat vian olemassaoloa. Organisaation ja etenkin päivystäjien ja järjestelmäasiantuntijoiden tilannetietoisuus paranee, kun tieto on keskitetymmin saatavilla. Järjestelmäasiantuntija voi paikantaa vian nopeammin valvontanäkymän avulla ja pystyy ennakoimaan komponenttien vikaantumisia tai tulevia suorituskykyongelmia. Tietohallintokin saa tilannetietoa ja se voi tarkastella myös, miten palvelutasosopimus, eli SLA (Service Level Agreement) kohtaa toteumaa, kun se saadaan luotettavasti mitattua valvontajärjestelmän avulla. Johdon suuntaan voidaan raportoida, kuinka luotettavasti palveluita pystytään tukemaan.

Palvelutasosopimuksissa käytetään erilaisia mittareita, esim. saatavuutta jollakin aikavälillä (Overby, Greiner & Gibbons Paul 2017). Pitää myös varmistaa, että osapuolet ymmärtävät mitä SLA tarkoittaa eli kuinka kova vaatimus on esimer-

kiksi palvelun 99,9 % saatavuus. Overby, Greiner & Gibbons Paul (2017) mainitsee, että esim. 99,999 % saatavuus ei ole epätavallinen vaatimus sivustolle, joka tuottaa miljoonia dollareita tunnissa.

Opinnäytetyön tarkoitus on, että opinnäytetyössä tehtävä suunnitelma mahdollistaa valvontajärjestelmän käyttöönoton mahdollisimman sujuvasti ja siten, että valvontajärjestelmä nostaa tietojärjestelmien, verkon ja teknisen alustan valvonnan uudelle tasolle niin, että tiedetään mitä tietoteknisessä ympäristössä tapahtuu ja niin, että kyetään ennakoimaan tulevaa.

Valvontajärjestelmä voi olla sekä reaktiivinen että proaktiivinen. Reaktiivisuus tarkoittaa sitä, että järjestelmä havaitsee vikoja mutta ei osaa ennakoida niitä. Proaktiivisuus puolestaan tarkoittaa, että sen avulla pystytään ennakoimaan tulevia vikoja tai resurssitarpeita. (Prescient 2016.) Tässä työssä tavoitteena on, että suunniteltavan valvontajärjestelmän avulla voidaan havaita korjausta kaipaavia prosesseja, palveluita ja komponentteja sekä käynnistää havaintojen perusteella tarvittavat prosessit.

Hyvän valvontajärjestelmän kautta pystytään myös havaitsemaan ja vähentämään järjestelmien monimutkaisuutta. Monimutkaisuus tulee ilmi viimeistään palveluiden ja järjestelmien valvonnan säännöstöjä luotaessa. Säännöstöjä luotaessa joudutaan miettimään mitä prosesseja ja komponentteja tulee valvoa, ja kokonaisuus joudutaan tuolloin jakamaan pienempiin osiin etenkin monimutkaisen järjestelmän osalta. Monimutkaisuuden avaamista voidaan verrata auton rakenteeseen, yhdelläkään auton osalla ei tee keskenään mitään, vaan olennaista on osien yhteistoiminta. Mitä monimutkaisempi, sitä vika-alttiimpi. Tämä sama logiikka pätee myös IT-järjestelmiin. (Cannon 2011, 365.)

Sopivien mittarien avulla saadaan tietoa järjestelmien toiminnasta tai toimimattomuudesta. Mittaaminen voi kuitenkin helposti jäädä muun toiminnan varjoon, otetaan järjestelmiä käyttöön, mutta ei huomioida, miten mitataan esimerkiksi järjestelmän kustannuksia, resurssitarpeita ja järjestelmästä saatavia hyötyjä tai sen aiheuttamia haittoja. Valvontajärjestelmää kannattaa käyttää myös mittaamiseen (Ellingwood 2017), joten tässä työssä suunnitellaan mittareitakin.

Riskit liittyvät olennaisesti mittaamiseen - riskejä halutaan nimenomaan mitata. Uhkan todennäköisyys, kohteen haavoittuvuus kyseistä uhkaa kohtaan ja uhkan toteutuessa sen vaikuttavuus ovat riskin mittareita. (Cannon 2011, 367). Järjestelmissä piilevät riskit täytyy kartoittaa, että saadaan priorisoitua valvottavia komponentteja, prosesseja ja palveluita. Teknisessä alustassa voi olla esimerkiksi joku komponentti, mistä useampi palvelu on riippuvainen. Valvontajärjestelmän luonnista on sekin hyöty, että voidaan havaita luonnin ohessa myös tietojärjestelmien rakenteisiin, arkkitehtuuriin tai komponentteihin liittyviä riskejä. Toisaalta, jos riskejä on jo toisaalla kartoitettu, on niistä hyötyä valvontajärjestelmän luonnissa.

Valvontajärjestelmää ei ole järkevää lähteä suunnittelemaan valitsemalla käytettäviä sovelluksia ja järjestelmiä vaan tulee ensin suunnitella, miten järjestelmää käytetään ja mitä siltä vaaditaan ja halutaan. Suunnittelun apuna käytetään ITIL (Information Technology Infrastructure Library) -kirjastoa. ITIL-kirjastosta saadaan apua mm. prosessien, menetelmien ja mittarien suunnitteluun (Axelos 2020). ITIL-kirjaston käytännöt eivät sovi kuitenkaan suoraan organisaation käyttöön, vaan niitä on pakko soveltaa. Työssä ei käydä kuitenkaan organisaation prosesseja, järjestelmiä ja käytänteitä tarkemmin lävitse vaan ratkaisuja haetaan yleisellä tasolla.

2 OPINNÄYTETYÖN PERUSTA

Opinnäytetyössä käsitellään valvontajärjestelmäkokonaisuutta etenkin verkonvalvomon ja palvelupisteen näkökulmista keskittyen toiminnallisuuden, palvelutason sekä häiriöiden valvontaan.

Kokemus on opettanut, että IT-alalla ei kannata keksiä käytäntöjä omasta päästään vaan kannattaa käyttää hyväksi jo olemassa olevia käytäntöjä. Valmiita käytäntöjä tarjoaa esimerkiksi tässäkin opinnäytetyössä lainattu ja jo johdannossa mainittu käytäntökirjasto: Information Technology Infrastructure Library (ITIL).

ITIL-kirjastoa käyttävät miljoonat ammattilaiset maailmanlaajuisesti ja se tarjoaa kattavan, sertifioidun ohjeistuksen IT-palvelutuotannon käyttöön. Sitä käytetään työkaluna esim. liiketoiminnan muutos- ja kasvutilanteissa. (Axelos 2021.) Käytäntöjä ei kuitenkaan oteta käyttöön ilman kriittistä tarkastelua vaan käytäntöjä muokataan ja sovelletaan tarpeen mukaan organisaatiolle sopiviksi.

Järjestelmien valvontaa verrataan elävän organismin elintoimintojen seurantaan eli toiminta on normaalia, mikäli elintoiminnoissa ei ole muutoksia havaittavissa (Steinberg 2011, 48). Palveluista ja laitteista siis haetaan tiettyjä merkkejä siitä, että järjestelmä toimii hyvin tai huonosti. Kiinnostavin on tietenkin se tilanne, kun toiminta on epänormaalia. Tämä tapa valvoa on kevyt, mutta tämä ei mahdollista esimerkiksi komponenttien vikaantumisen ennakointia vaan lisäksi tarvitaan myös syvällisempiä tarkistuksia (Steinberg 2011, 49). Tämäntyyppinen tietoteknisen terveyden seuranta voisi olla lähtökohta valvonnan suunnittelulle, mutta se vaatii omien järjestelmien hyvää tuntemusta, että nuo normaalit elintoiminnot ovat tiedossa ja saadaan määriteltyä sopivat hälytysrajat. Hälytysrajojen määritys vaatii myös seuranta-aikaa, että saadaan normaalit raja-arvot selville. Paljon työtä jää tehtäväksi siis myös valvontajärjestelmän käyttöönoton jälkeenkin, puhumattakaan iteratiivisesta kehittämisestä mitä toiminta vaatii.

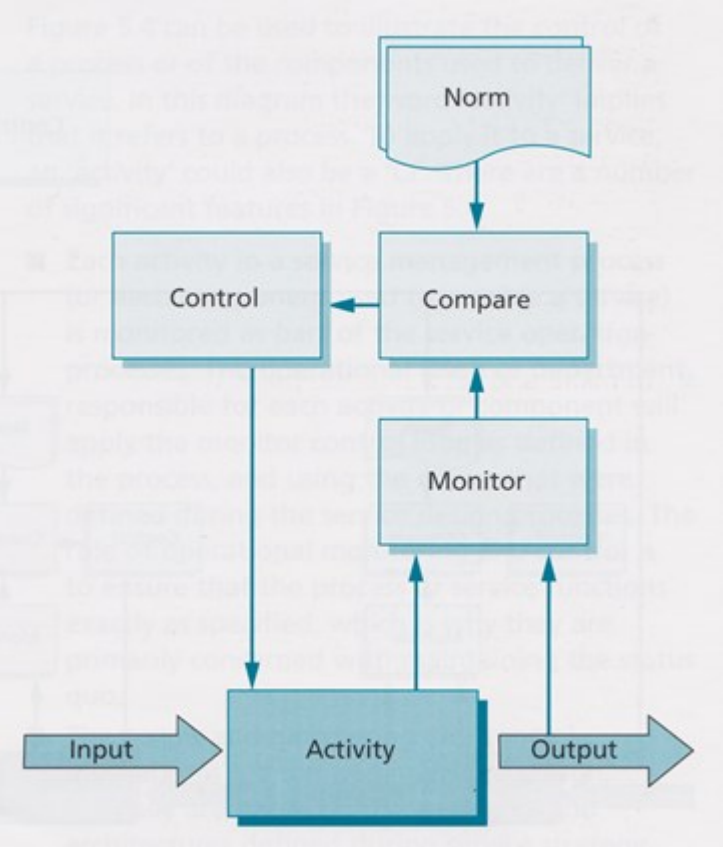
Palveluille löydetään yhteisiä nimittäjiä, kuten eläville organismeillekin, ja kuten elävillä organismeilla myös palveluilla on omat heikot kohtansa, joita voidaan tarvittaessa valvoa tarkemmin. Palvelutason määrittäminen kullekin palvelulle auttaa tässä eteenpäin ja sen perusteella voidaan määritellä, kuinka tarkasti mitäkin palvelua tarvitsee valvoa ja se auttaa myös hälytysrajojen määrittämisessä. Kun palvelutasot ovat määriteltynä, on helpompaa valita tärkeimmät järjestelmät palvelutasojen perusteella ja tärkeimmille järjestelmille voidaan tehdä sovelletut vikapuuanalyysit. Vikapuuanalyysin avulla voidaan löytää kriittisiä komponentteja (Salo, 2007). Kriittisten komponenttien etsimiseen on muitakin tapoja, mutta tähän työhön metodiksi valittiin vikapuuanalyysi sovellettuna, koska se on nopea toteuttaa. Nopea toteutus edellyttää, että analyysi tehdään yksinkertaistettuna. Tieto kriittisistä komponenteista auttaa siinä, että tiedetään mitä kannattaa valvoa sekä järjestelmän vikasietoisuuden parantamisessa. Vikasietoisuutta voidaan parantaa mm. vaihtamalla komponentteja laadukkaampiin tai kahdentamalla kriittisiä komponentteja.

3 VALVONTAPROSESSIT

Valvontaan liittyviä IT-palvelutuotannon ITIL:n mukaisia prosesseja ovat tapahtumahallinta, poikkeamahallinta ja ongelmahallinta (Optanix 2020). Tässä opinnäytetyössä etsitään parhaita ratkaisuja näihin prosesseihin liittyen organisaation käyttöön. Nämä prosessit ovat toisaalta myös erittäin tärkeitä ylipäätään palveluiden toiminnan kannalta.

Suunniteltavia asioita ovat myös tapahtumien ja poikkeamien luonti ja keräys, luokittelu, viestintä ja eskalointi, mitä tietoa tapahtumakortille ja poikkeamakortille asetetaan ja mihin kaikki tallennetaan. On suunniteltava järjestelmä järjestelmältä ja palvelu palvelulta, mitä tapahtumia tarvitsee kerätä, mitä tapahtumadataa ne tuottavat automaattisesti ja mitä pitää erikseen kysellä. Näitä toimenpiteitä hyvä valvontajärjestelmä tukee työkalujensa avulla auttaen myös iteratiivisessa kehittämisessä. Näitä toimenpiteitä ei tässä työssä pystytä tekemään, vaan ne jäävät jatkokehitystä odottamaan.

Valvonnasta on liittymä myös palvelunhallintaan. Steinberg (2011, 123), esittelee valvontahallintasyklin, missä verrataan prosessien lopputuotteita ns. normaaliin tuotteeseen tai ennalta määritettyyn normiin. Kuvio 1 havainnollistaa tätä. Mikäli jossakin kohtaa tuote muuttuu liikaa normiin nähden, luodaan järjestelmään poikkeamatapahtuma.



Kuvio 1. Valvonta-hallintasykli (Steinberg 2011)

Valvonta-hallintasyklissä on kyse siitä, että havaitaan ei-toivotut muutokset tuotteiden tai palveluiden tulosteissa. Sykli alkaa syötteestä (Input), mille tehdään prosessissa joku aktiviteetti (Activity). Tuotetta tai vastaavaa tarkastellaan aktiviteetin jälkeen (Monitor) ja verrataan (Compare) normituotteeseen (Norm). Tarvittaessa sille tehdään hallintatoimia (Control), minkä jälkeen se menee uudelleen prosessiin. Normituote asettaa rajat minkälainen tuote saa olla, että huomataan mahdolliset virheet tuotannossa. (Steinberg 2011, 123.)

3.1 Tapahtumahallinta

Valvonnan kannalta tärkein prosessi on tapahtumahallinta. Tapahtuma (event) on kuvattu ITIL:ssä näin: tilamuutos, jolla on merkitystä IT-palvelun tai muun komponentin hallintaan. Termiä voidaan käyttää myös IT-palvelun, komponentin tai valvontajärjestelmän luomien hälytysten ja huomautusten yhteydessä. Tapahtuma usein vaatii IT-palveluhenkilöstön toimenpiteitä johtaen poikkeamailmoituksen luontiin. (Axelos 2011.)

ITIL-käytäntökokoelmissa tapahtumat jaetaan tapahtumien merkityksellisyyttä kuvaaviin tapahtumatyyppeihin. ITIL:ssä käytettyjä tapahtumatyyppejä ovat tietotapahtumat (informational events), varoitustapahtumat (warning events) ja virhetapahtumat (exception events). (Santoshi 2019.)

Tapahtumahallinta käsittää siis kaikki tapahtumat mitä ihmiset, järjestelmät, verkot ja komponentit tuottavat järjestelmiin ja niiden perusteella käynnistetään mm. poikkeamahallinnan, ongelmahallinnan ja pääsyhallinnan prosesseja.

Hyvän tapahtumahallinnan mahdollistaa valvontajärjestelmä, joka pohjautuu kahdentyyppisiin työkaluihin: aktiivisiin valvontatyökaluihin mitkä pollaavat avainkomponentteja ja passiivisiin valvontatyökaluihin mitkä havaitsevat ja korreloivat komponenttien viestintää ja hälytyksiä (Steinberg 2011, 58). Taulukkoon 1 on koottu aktiivisen ja passiivisen sekä reaktiivisen ja proaktiivisen valvonnan tunnusmerkkejä.

Taulukko 1. Aktiivinen ja passiivinen ja reaktiivinen ja proaktiivinen valvonta (Steinberg 2011)

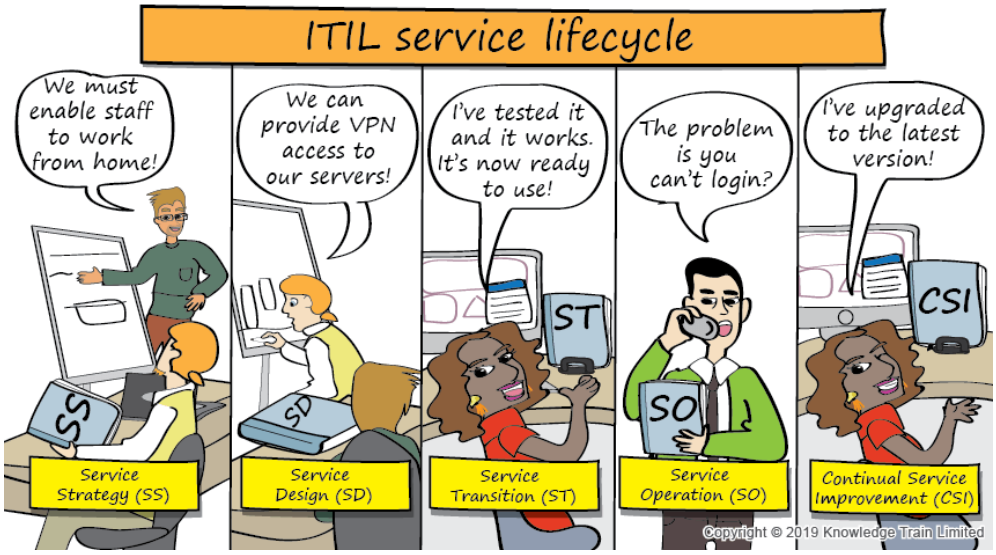
	Active	**Passive**
Reactive	Used to diagnose which device is causing the failure and under what conditions (e.g. 'ping' a device, or run and track a sample transaction through a series of devices) Requires knowledge of the infrastructure topography and the mapping of services to CIs Requires capability to simulate service workloads and demand volumes	Detects and correlates event records to determine the meaning of the events and the appropriate action (e.g. a user logs in three times with the incorrect password, which represents a security exception and is escalated through information security management procedures) Requires detailed knowledge of the normal operation of the infrastructure and services
Proactive	Used to determine the real-time status of a device, system or service – usually for critical components or following the recovery of a failed device to ensure that it is fully recovered (i.e. is not going to cause further incidents)	Event records are correlated over time to build trends for proactive problem management Patterns of events are defined and programmed into correlation tools for future recognition

Aktiivis-reaktiivisessa valvonnassa pyritään diagnosoimaan mikä laite aiheuttaa vikaa ja minkälaisessa tilanteessa. Passiivis-reaktiivinen havainnoi ja korreloi tapahtumia etsien syitä tapahtumille tarvittaessa eskaloiden asian asianmukaiseen prosessiin. Aktiivis-proaktiivinen pyrkii ottamaan selvää laitteen, järjestelmän tai palvelun reaaliaikaisesta tilasta etenkin kriittisten komponenttien osalta, tai aiemmin vikaantuneen, toimintaan palautetun laitteen osalta, ettei se vikaantuisi uudelleen. Passiivis-proaktiivisessa valvonnassa tapahtumia korreloidaan ajan kuluessa etsien trendejä proaktiivisen ongelmahallinnan käyttöön.

Steinberg (2011, 59) vertaa valvontaa ja tapahtumahallintaa siten, että tapahtumahallinta luo ja havaitsee huomioita IT-infrastruktuurissa ja palveluissa, ja valvonta taas on laajempi kokonaisuus, sisältäen tapahtumahallinnan syötteiden lisäksi myös tarkempaa esim. suoraan laitteelta erikseen kyseltyä tilatietoa.

Varoitusten ja poikkeamien osalta tarvitaan poikkeamahallinnan ja mahdollisesti ongelmahallinnan prosesseja, eli ne tulee eskaloida eteenpäin. Tietotapahtumien osalta voidaan tehdä säännöstöjä, esim. siten että mikäli joku odotettu tapahtuma ei toistu, voidaan päätellä palvelussa olevan vikaa ja tällöin eskaloida se poikkeamahallintaan. Joistakin tapahtumista tulee myös lähettää tiedonantoja eteenpäin, tyypillisesti sähköpostitse tiedonantoja varten luodulle sähköpostijakelulle. Tapahtumia pitää kyetä myös suodattamaan. IT-infrastruktuurissa voi tulla muuten aivan liikaa tapahtumia, että sieltä kyettäisiin analysoimaan poikkeamia, tai että valvontajärjestelmän kapasiteetti riittää niitä säilyttämään.

Kuviot 2 ja 3 avaavat valvonnan suhdetta IT-palvelun elinkaareen. Valvonta on jatkuvaa ja päivittäistä toimintaa (service operation), mutta valvonnan kautta saadaan tietoa, millä voi olla vaikutusta myös palvelustrategiaan (service strategy), uusien palveluiden suunnitteluun (service design) ja palvelumuutoksiin (service transition). Tämä motivoi tekemään valvontaosion laadukkaasti. Kuviossa 2 IT-tukihenkilö saa tiedon kirjautumisongelmasta puhelimitse. Kuviossa 3 saadaan vihiä strategian epäonnistumisesta ITIL:n palvelutoimintatasolta.



Kuvio 2. ITIL-palvelutoiminnan (valvonnan) suhde palvelun elinkaareen (Buehring 2020)

Kuvio 3. ITIL-palvelutoiminnan (valvonnan) suhde strategiaan (Buehring 2020)

3.2 Poikkeamahallinta

ITIL kuvaa poikkeamaksi keskeytykset ja laadun heikkenemisen IT-palvelutuotannossa. Poikkeamahallinnalla pyritään korjaamaan tapahtumahallinnan kautta havaittuja vikoja minimoiden häiriöt organisaation toiminnassa. (Axelos 2011.)

Poikkeamia voivat olla vaikkapa komponentin hajoaminen, suorituskyky-, saatavuus-, kapasiteetti- tai verkkoyhteysongelmat. Poikkeamahallinta on siis riippuvainen tapahtumahallinnasta, missä poikkeamat havaitaan.

Poikkeamien osalta on suunniteltava, käytetäänkö Steinbergin (2011, 75) käyttämiä poikkeamatasoja eli poikkeama ja vakava poikkeama vai tarvitaanko enemmän poikkeamatasoja. Tätäkin täytyy organisaatiossa jatkokehityksen lomassa miettiä. Mikäli organisaation käytössä on toiminnanohjausjärjestelmä, johon nämä ovat jo määritetyt, nämä voidaan kopioida suoraan sieltä.

3.3 Ongelmahallinta

Ongelma (problem) on ITIL:n mukaisesti yhden tai useamman tapahtuman syy. Ongelmahallinnalla pyritään proaktiivisesti estämään poikkeamien tapahtuminen ja vähentämään vaikutuksia niiden poikkeamien osalta, joita ei kyetä estämään. (Axelos 2011.) Valvontaan ongelmahallinta liittyy siten, että ongelmat tulee tunnistaa ja eskaloida ongelmahallintaan.

Usein ongelmaksi kirjataan myös vika, jota ei saada korjattua kohtuullisella työmäärällä, vaan vian korjaus vaatii isomman urakan tai esimerkiksi muutoksen ongelmalliseen järjestelmään.

4 VALVONTA ORGANISAATIOSSA

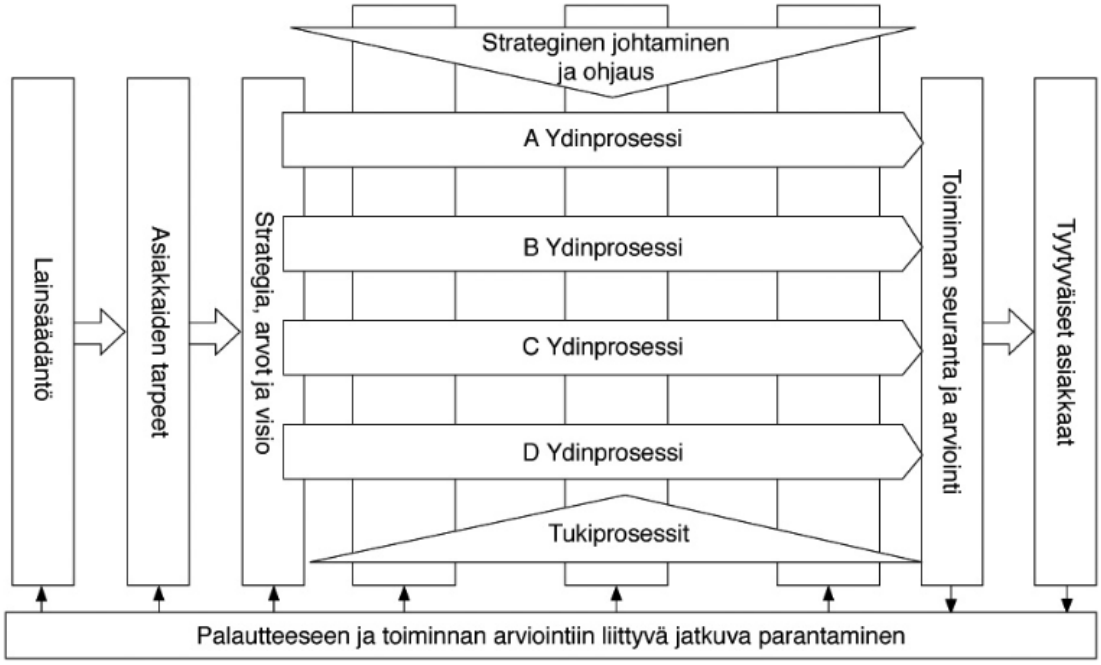
Kappaleessa käydään läpi valvonnan tila, kehitystarpeet, roolit organisaatiossa sekä valvontajärjestelmälle asetetut vaatimukset. Kappaleessa mietitään myös mittareita, valvonnan suhdetta hallintaan ja sääntökokoelmien käyttöä.

4.1 Valvonnan nykytila ja kehitystarpeet organisaatiossa

Lähivuosilta on olemassa esimerkkitapauksia, joissa olisi ollut tarkemmasta valvonnasta hyötyä joko estämään vikatilanne täysin, tai nopeuttamaan korjausta. Yhdessä tapauksessa eräs palvelukomponentti ei lähtenyt käyntiin rekisteriasetusten muututtua, ja tässä kului ensin aikaa, että vika paikallistettiin kyseiseen komponenttiin ja lisää aikaa, että havaittiin rekisterimuutokset. Molempia on mahdollista valvoa ja valvominen on järkevää noin kriittisten komponenttien osalta. Tässä tapauksessa lähes kaikkien käyttäjien kirjautuminen toimialueelle oli estynyt. Toinen tapaus oli siinä mielessä samantyyppinen, että siinäkin oli kyse palvelukomponentista minkä uudelleenkäynnistys auttoi vikaan. Tapaus oli senkaltainen, että valvontajärjestelmä voisi komponentin tilan havaitessaan jopa automaattisesti käynnistää uudelleen komponentin, jolloin vika korjaantuu. Nämä toimenpiteet pitää tietenkin kirjata lokiin tarkasti. Kolmas tyypillinen tilanne on, että käyttäjämäärien lisääntyessä työpäivän vilkkaimpaan aikaan alkaa kehittyä kapasiteettiongelma, ja järjestelmä toimii hitaasti, tai ei toimi ollenkaan. Kyseessä on tyypillisesti palvelimen massamuisti-, keskusmuisti- tai suoritinresurssin riittämättömyys tai tietoliikenteen pullonkaula. Molemmat voidaan havaita jo ennen ongelmia, ja lisätä resurssia tai poistaa pullonkauloja tarpeen mukaan. Kapasiteettiin liittyen valvontaa voidaan käyttää myös siten, että jos jollekin palvelulle on allokoitu liikaa resurssia, voidaan sitä sieltä vapauttaa tarpeeseen.

4.2 Organisaation toiminta

Organisaation toimintaan vaikuttaa kokonaisuutena usea asia. Kuvio 4, JHS:n prosessikarttaesimerkki, havainnollistaa tätä: organisaatiossa on 4 ydinprosessia (A, B, C, D). Kuviossa ylhäältä niiden toimintaan vaikuttaa strateginen johtaminen ja ohjaus, vasemmalta lainsäädäntö, asiakkaiden tarpeet, strategia, arvot ja visio, alhaalta palautteeseen ja toiminnan arviointiin liittyvä jatkuva parantaminen. Ydinprosessien tuotantoa seurataan toiminnan seurannalla ja arvioinnilla ja lopputuloksena ovat tyytyväiset asiakkaat. Toiminnan seurannasta ja arvioinnista sekä asiakkailta tulevaa palautetta käytetään hyväksi toiminnan jatkuvassa parantamisessa.



Kuvio 4. Prosessikarttaesimerkki (JHS 2020)

Tähän opinnäytetyöhön liittyen oleellista on, että tuetaan erilaisia ydinprosesseja, joiden päämäärää tukemassa on erilaisia järjestelmiä. Ydinprosesseja tukevia järjestelmiä kehitetään kehitysprojekteissa ja ylläpidetään ylläpitoprojekteissa. Kyseisten ydinprosessien tärkeys organisaation tehtävän kannalta (ja sitä kautta priorisointi) saattaa muuttua ja tätä tarkastellaankin vuosittain. Vuosittain voidaan asiakkaiden kanssa yhdessä tarkentaa myös palvelutasosopimusta, kun edellä on priorisointeja mietitty. Palvelutasosopimus auttaa valvottavien palveluiden ja

komponenttien kriittisyyden arvioinnissa. Sellaisiakin järjestelmiä, jotka eivät suoraan liity ydinprosesseihin, ja joita ei välttämättä kirjata palvelutasosopimukseen täytyy valvoa, koska kyseiset järjestelmät voivat kuitenkin olla kriittisiä ydinprosessien tukemisessa, eli toimivat ydinprosesseja tukevien järjestelmien pohjana.

Liiketoimintavaikutusanalyysi voisi auttaa valvonnan kohdentamisessa kriittisimpiin komponentteihin palvelutasojen lisäksi. Sen tarkoituksena on hahmottaa katastrofin vaikutuksia liiketoimintaan. (Hunnebeck 2011, 283.) Hunnebeck (2011) jakaa liiketoimintavaikutusanalyysin kahteen osa-alueeseen, liiketoiminnan hallinta, mikä tutkii vaikutusta liiketoimintaprosessin tai -toiminnon menetyksessä tai osittaisessa menetyksessä ja palvelunhallinta, missä palvelun menetyksen vaikutukset avataan liiketoiminnalle. Käytännössä kumpikin osapuoli siis analysoi asiaa omalta kantiltaan ja kommunikoi toiselle osapuolelle.

Valvonta-arkkitehtuurin ylläpitotoimet käynnistetään vuosittain. Kuvio 5 havainnollistaa kokonaisarkkitehtuurin ylläpitomallia, mutta soveltuu hyvin myös valvonta-arkkitehtuurin ylläpitoon. Valvonta-arkkitehtuuri on tietenkin myös riippuvainen kokonaisarkkitehtuurista, eli muutokset kokonaisarkkitehtuurissa aiheuttavat muutoksia myös valvonta-arkkitehtuuriin. Kun vaikkapa strategia muuttuu, täytyy tarkastella valvonta-arkkitehtuuria ainakin muutosten osalta. Kuvion vasemmasta ympyrästä tulee siis esimerkiksi strategiamuutoksia, mitkä täytyy huomioida valvonta-arkkitehtuurissa. Valvonta-arkkitehtuurin ylläpito voidaan nähdä tässä toistuvana projektina, missä käydään muuttuneet palvelutasosopimukset läpi ja tehdään sen mukaiset muutokset valvontaan. (Business Technology Standard 2019). Kuviosta poiketen kevyempi malli tähän voisi olla, että asiantuntijatiimi käy mahdolliset muutokset läpi, käsittelee palvelutasot asiakkaiden kanssa ja ohjaa palvelutasojen avulla valvontajärjestelmän ylläpitoa.

Kuvio 5. Enterprise Architecture Governance (Business Technology Standard 2019)

Kuviossa 5 vasemmalla on kuvattuna kokonaisarkkitehtuurin hallintosykli (Enterprise Architecture Governance Cycle). Sykli kulkee strategiaprosessista (1 Strategy Process) kokonaisarkkitehtuurin tilaan ja tiekarttaan (2 EA Target State and Roadmap), kehitysprojekteihin (3 Development projects) ja uuteen tilaan ja liiketoimintavaikutukseen (New Current State and Business Impact), minkä jälkeen sykli alkaa uudelleen. Oikealla on kokonaisarkkitehtuurin tuki projekteille (EA Support to Projects), mikä saa ohjausta kokonaisarkkitehtuurin hallintosyklin kohdasta kehitysprojektit. Syklissä päivitetään ensin projektien päämäärät tai liiketoimintatapaukset (3.1 Project Goals / Business Case), sitten tehdään kokonaisarkkitehtuuripäivitykset, sitten arkkitehtuurin mukaiset implementaatiot ja lopuksi tarkastellaan vaikutuksia liiketoimintaan.

4.3 Valvontaan liittyvät roolit

Valvontaan liittyvät roolit tehtävineen täytyy käydä läpi, että valvontatehtäville on tekijänsä. Tässä työssä on kuvattuna esimerkkiroolitus mikä voisi toimia useassakin organisaatiossa, ainakin tekemällä pieniä muutoksia riippuen organisaation koosta ja rakenteesta. Roolit käydään tasoittain läpi, 1. taso on lähimpänä loppukäyttäjää ja 3. taso kauimpana.

1. tason tukena toimii palvelupiste. Käytetään ns. yhden luukun periaatetta, eli

palvelupiste vastaanottaa sekä palvelupyynnöt että häiriöilmoitukset. Palvelupisteen tehtäviä ovat:

1. Tikettien seuranta.
2. Tikettien priorisointi, luokittelu ja kategorisointi.
3. Tikettien ohjaus eteenpäin.
4. Oman vastuualueen tikettien ratkaisu. Toistaiseksi palvelupisteen tehtäviä tekevillä on myös muita tehtäviä ja vastuita.
5. Yleinen palvelupistetoiminta: oheislaitteiden ja kannettavien yms. lainaaminen, pienet asennustehtävät, neuvonta, ym. soveltuvat tehtävät.
6. Toiminnan jatkuva kehittäminen. Mahdollisiin epäkohtiin puuttuminen ja kehitystyöhön osallistuminen.

Verkonvalvomo valvoo verkkoa, teknistä alustaa ja palveluiden tilaa toimien 2. tason tukena. Verkonvalvomon tehtäviä ovat:

1. Verkon, teknisen alustan ja palveluiden valvonta.
2. Häiriöiden hallinnan koordinointi (poikkeamahallinta).
3. Häiriö- ja vikatilanteiden analysointi ja rajaus tai ratkaisu itsenäisesti, jos mahdollista.
4. Osoitus 3. tason tuelle.
5. Tilannetietoisuuden ylläpito.
6. Häiriöt.
7. Vikatilanteet.
8. Tiedossa olevat muutostyöt.
9. Palveluiden saatavuus.
10. Tiedottaminen – häiriöt ja muutostyöt (toimiala asiakkaineen, kumppanit).
11. Järjestelmätilannekuvan ylläpito.
12. Omat järjestelmät.
13. Runkoverkko.
14. Johdon raportoinnin tuki.
15. Palvelutasosopimusraportointi (edellyttää sovitut ja mitattavat mittarit).
16. Menneen aikajakson häiriöt ja tapahtumat.
17. Toiminnan jatkuva kehittäminen.

3. tason tuessa toimivat järjestelmien asiantuntijat ja kumppanit. 3. tason tuen tehtävänä on toimia yhteistyössä muiden 3. tason asiantuntijoiden ja palvelupiste- sekä verkonvalvomohenkilöstön kanssa pyrkien ratkaisemaan tiketit.

Asiakas voi luoda palvelupyyntöjä ja häiriöilmoituksia itsepalveluportaalissa, puhelimitse tai palvelupisteellä sekä tiedottaa luotujen tikettien osalta mahdollisista muutoksista tukihenkilöstöä.

4.4 Valvonnasta hallintaan

Kappaleen 4.3 roolikuvauksista voidaan päätellä, että missä valvonta ja hallinta roolillisesti kohtaavat. Verkonvalvomo tekee valvontatyötä, mutta myös ratkaisee ne tiketit mitkä ovat verkonvalvomon ratkaistavissa. Erikoistapaukset, mitkä eivät ole verkonvalvomon ratkaistavissa, se osoittaa 3.tason tukeen. Valvontaan käytettävillä työkaluilla voidaan tehdä pienessä mittakaavassa myös hallintatehtäviä, mutta hallinta on kuitenkin oma osa-alueensa, ja sitä hoitavat omien osa-alueidensa asiantuntijat.

4.5 Vaatimukset uudelle valvontajärjestelmäkokonaisuudelle

Vaatimukset kohdistuvat sekä organisaatioon että käytettäville työkaluille. Työkaluilta vaaditaan tiettyjä ominaisuuksia ja organisaatiolta tietotaitoa työkalujen käytössä, että kyetään tekemään oikeanlaisia mittareita, käytäntöjä ja sääntöjä.

Yleisesti järjestelmän tulee olla toimintavarma, kustannustehokas, helposti käyttöönotettavissa sekä helppokäyttöinen. Järjestelmän osalta myös turvallisuus on huomioitava erityisen tarkasti, koska valvontajärjestelmän pitää päästä valvomaan avainkomponentteja ja mahdollisesti sensitiivistäkin tietoa sisältäviä järjestelmiä. Huomiota täytyy kiinnittää siihen, että tuotteet ovat tunnettuja ja hyvämaineisia ja käyttöönotto tehdään hallitusti sovittujen menetelmien mukaisesti sekä ylläpito, päivittäminen ja konfigurointi tehdään asianmukaisesti. Järjestelmä tulee olla mahdollista integroida muihin järjestelmiin yleisimmin käytettyjen rajapintojen

kautta. Näitä ovat esimerkiksi SNMP (Simple Network Management Protocol), XML (extensive markup language ja JSON (JavaScript Object Notation). Tapahtumia ja poikkeamia pitää pystyä muokkaamaan luomisen jälkeen ohjelmallisesti (turvallisuus huomioiden) ja niitä pitää pystyä poissulkemaan ennakoitujen huoltokatkojen ajaksi. Järjestelmän tulee omata myös hyvät raportointiominaisuudet.

4.5.1 Teknologiset vaatimukset

Valvontajärjestelmän tulee kyetä valvomaan teknistä alustaa, palveluita ja komponentteja. Järjestelmä voi koostua joko useasta sovelluksesta mitkä erikoistuvat omaan osa-alueeseensa tai sitten järjestelmä voi toimia näkymänä, mikä kerää tilatietoa eri lähteistä. Valvontajärjestelmän tulee kyetä seuraamaan ainakin seuraavia asioita:

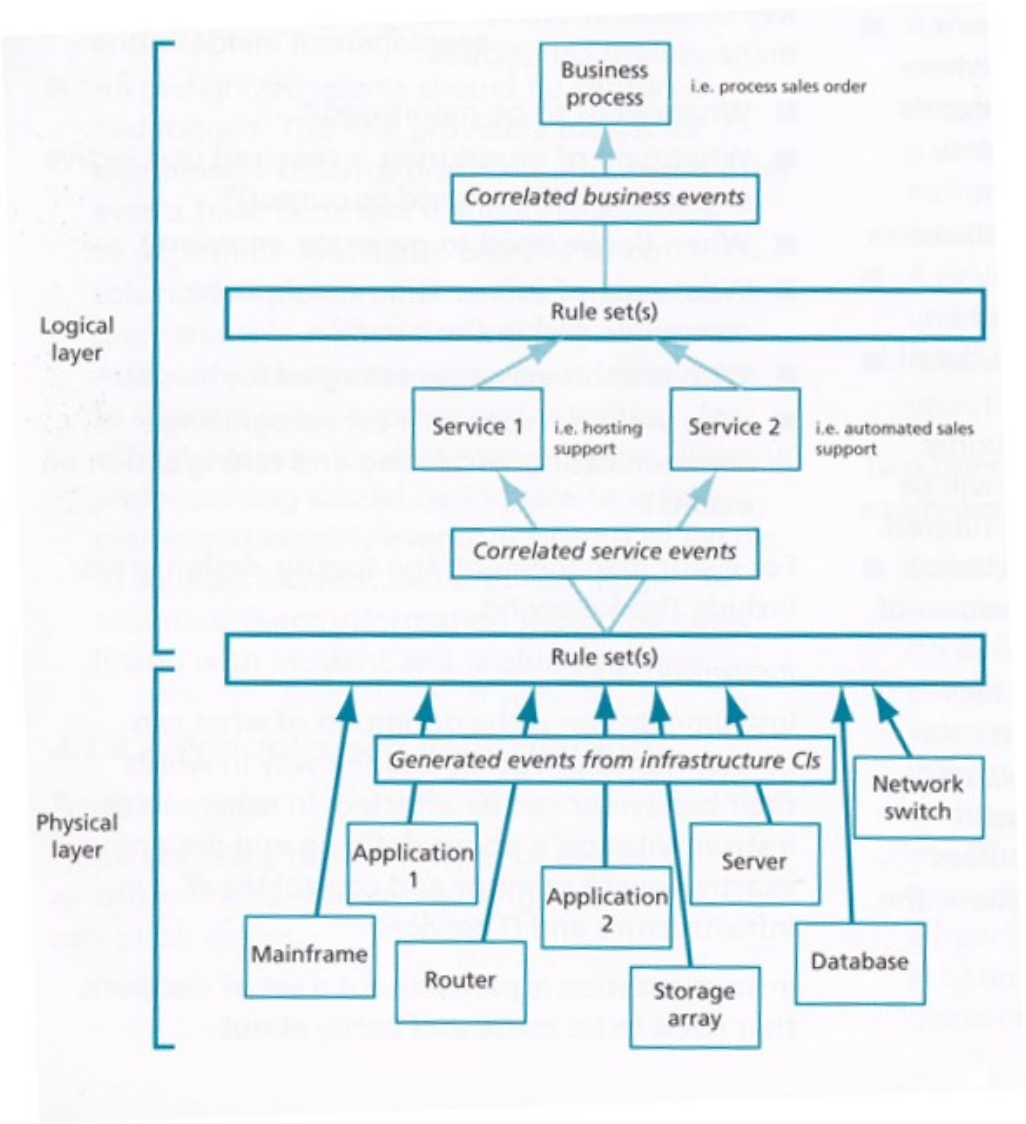
1. Windows-käyttöjärjestelmän palvelut
2. Linux-käyttöjärjestelmän palvelut ja prosessit
3. Windows-käyttöjärjestelmät
4. Linux-käyttöjärjestelmät
5. Virtuaalialustat
6. Verkkokomponentit (kytkimet, reitittimet, palomuurit)
7. Tulostimet ja skannerit
8. Levyjärjestelmät
9. Konttiteknologia.

Tarve ohjaa valvontajärjestelmätoimittajia siinä, että yleisimmin käytettyjä komponentteja kyetään valvomaan. Tästä syystä yllä mainittujen yleisesti käytettyjen komponenttien valvonta onkin valvontajärjestelmissä usein kattavasti toteutettu.

4.5.2 Sääntökokoelmat

Sääntökokoelmien avulla voidaan tehdä palvelukohtaisia arvioita järjestelmän kyvykkyydestä. Palvelukohtainen sääntökokoelma voi sisältää palveluiden osien tilan ja laskea sen perusteella palvelun saatavuustason. Palvelukohtainen sääntökokoelma voi sisältää myös palveluun liittyvät komponentit, joista kukin arvotetaan kriittisyyden perusteella. Yksittäisen komponentin rikkoontuminen ei välttämättä vaikuta ollenkaan palvelukohtaiseen saatavuuteen tai sitten se voi lamaannuttaa koko palvelun tai se voi heikentää palvelun saatavuutta osittain. (Steinberg 2011, 63.)

Sääntökokoelmien käyttöä fyysisellä ja loogisella tasolla havainnollistaa kuvio 6. Kuviossa 6 kuljetaan fyysiseltä tasolta (Physical layer) loogiselle (Logical layer). Fyysisen ja loogisen tason rajapinnassa käytetään sääntökokoelmia (Rule sets), jotka perustuvat fyysisen tason komponentteihin ja niiden muodostamiin tapahtumiin (Generated events from infrastructure CIs). Sääntökokoelmien perusteella tapahtumat korreloidaan palveluihin (Correlated service events). Loogisella tasolla on omat sääntökokoelmat, jotka huomioivat palveluihin liittyvät tapahtumat. Nämä tapahtumat korreloituvat liiketoimintatapahtumiksi (Correlated business events), jolloin tiedetään, mikä on palveluiden tilanne liiketoiminnallisesta näkökulmasta. Kriittisen komponentin rikkoutuessa vaikutukset voivat näkyä liiketoiminnassa asti heti, kuten kuvion esimerkissä tilausprosessissa (Business process, i.e. process sales order). Tällä tavalla tiedetään myös mihin palveluun komponentin vikatilanne vaikuttaa.



Kuvio 6. Fyysisen infrastruktuurin tapahtumien, palveluiden ja prosessien välinen suhde (Hunnebeck 2011)

4.5.3 Mittaaminen

Mittaamalla voidaan varmistaa, että valvontajärjestelmä ja valvottavat järjestelmät toimivat, seurata organisaation tuottavuutta ja tuotteiden laatua, ennakoida tulevaa ja tuottaa raportteja päätöksenteon tueksi.

Valvontajärjestelmällä tulisi olla mahdollista mitata seuraavia asioita:

1. Saatavuus. Saatavuutta tulisi kyetä mittaamaan ketjun alusta loppuun. Palvelun saatavuus on yhtä kuin ketjun heikoin lenkki, eli sitä voidaan parantaa paljon eliminoimalla heikkoja tai epäluotettavia komponentteja ja yksittäisiä vikaantumispisteitä. (Hunnebeck 2011, 127.)

   Palvelutasojen mukaista saatavuutta voidaan mitata valvontajärjestelmän avulla ja saatavuutta tulee myös verrata sovittuun tasoon. Jos tavoite ei täyty, tulee käynnistää tarvittavat prosessit asian korjaamiseksi. Valvontajärjestelmästä saatavaa hyötyä voidaan mitata myös mittaamalla saatavuutta järjestelmän käyttöönoton yhteydessä ja vertaamalla sitä tulevaisuuden saatavuuteen.

   Saatavuudenhallintaprosessin tulee pystyä valvomaan kaikkia IT-palveluiden ja -komponenttien saatavuuden, luotettavuuden ja ylläpidettävyyden aspekteja käyttäen soveltuvia tapahtumia, hälytyksiä ja toimenpiteitä sekä automaattisia palautumisskriptejä (Hunnebeck 2011, 126). Suunniteltava valvontajärjestelmä tarvitsee tietenkin aikaa, että kyetään tekemään automaattisia palautumisskriptejä. Saatavuutta on seurattava, että saadaan riittävästi dataa tietääksemme mihin saatavuusongelmiin kannattaa tarttua sekä tehdä mahdollisesti niihin liittyviä palautumisskriptejä.

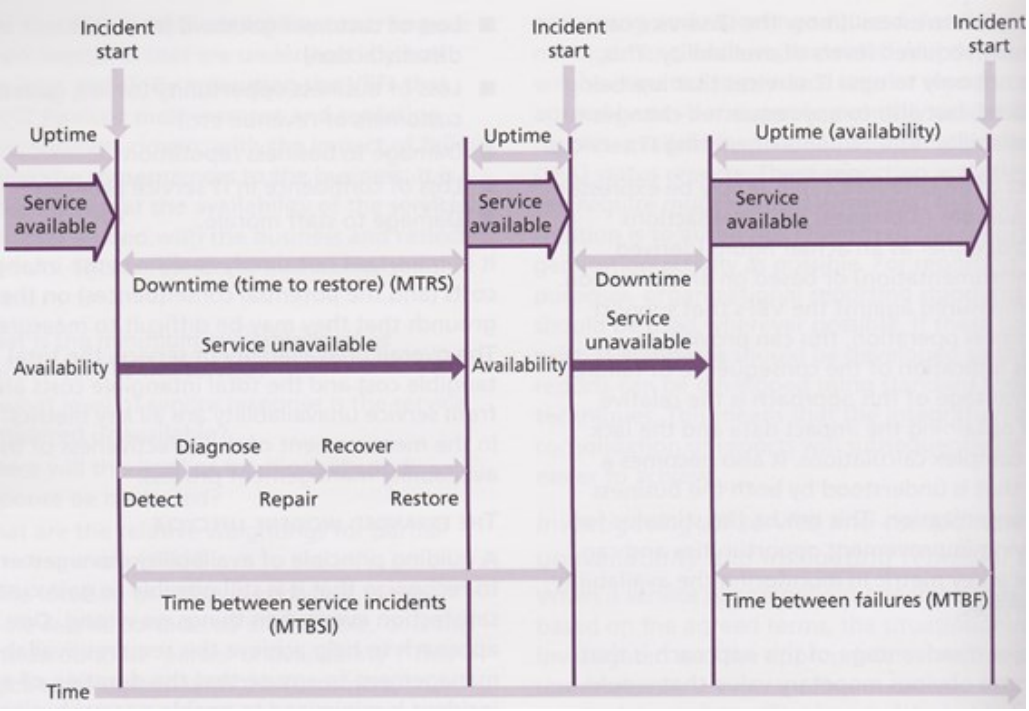
2. Kapasiteetti. Esimerkkejä mittareista ovat massamuistin käyttöaste, kelluvien lisenssien käyttöaste, käyttäjämäärä verrattuna muihin mittareihin tietyllä ajanhetkellä. Esimerkiksi riittävätkö kelluvat lisenssit kaikkina ajan hetkinä vai täyttyykö lisenssimäärä kesken työpäivän?

   Olennaista kapasiteettimittareissa on myös se, että kuinka hyvin voidaan ennustaa tulevaa kapasiteetintarvetta, eli analysointiin saadaan valvonnan kautta hyvää dataa.

3. Suorituskyky. Esimerkkejä mittareista ovat suoritinteho, keskusmuistin käyttö, kaistanleveys, siirtonopeus, vasteaika. Voidaan myös mitata, kuinka järjestelmä selviää toimistotyöaikaan tulevista kuormituspiikeistä. Valvontajärjestelmän avulla saatava tieto auttaa skaalaamaan resursseja

tarpeen mukaan paremmin. Voisiko virtuaalijärjestelmissä siirtää resurssia yöaikaan tietyille palvelimille, jos niillä ajetaan esimerkiksi indeksointeja tai muuta resursseja vaativaa tehtävää yöllä, ja aamulla takaisin toimistotyöaikaan tarvittaville resursseille? Tämäkin voisi olla tapa lisätä asiakastyytyväisyyttä ja resurssien tehokasta käyttöä.

4. Ylläpidettävyys. Ylläpidettävyyttä voidaan mitata MTTR (Mean time to repair) -mittarilla sekä MTRS (mean time to restore service) -mittarilla (Hunnebeck 2011, 128). Tätä selventää kuvio 7: laajennettu poikkeaman elinkaari. Ylläpidettävyyden mittaaminen vaatii käytännössä seuranta-aikaa, että saadaan poikkeamia talteen ja sitä kautta mitattua ylläpidettävyyttä.



Kuvio 7. Laajennettu poikkeaman elinkaari (Hunnebeck 2011)

Laajennetun poikkeaman elinkaaren ideana on purkaa poikkeaman aiheuttama katko osiin. Aikaa kuluu poikkeaman havaitsemiseen (Detect), diagnosointiin (Diagnose), korjaukseen (Repair), palautumiseen (Recover) ja ennallistamiseen (Restore). Kuvio havainnollistaa myös poikkeamien välistä aikaa (Time between service incidents), häiriöaikaa (Downtime), saatavuusaikaa (Uptime (availability)) sekä häiriöiden välistä

aikaa (Time between failures). Kun poikkeama on purettuna osiin, voidaan keskittää parannustoimenpiteet osiin, joissa eniten on parannettavaa.

5. Luotettavuus. Luotettavuuden mittana pidetään palvelun tai komponentin keskeytyksetöntä suoritusta ilman laatuongelmia. Luotettavuuden mittaamisessa voidaan käyttää MTBSI (mean time between service incidents) ja MTBF (mean time between failures) -mittareita. (Hunnebeck 2011, 128.)

   Tätä avaa kuvio 7: laajennettu poikkeaman elinkaari. Vaatii käytännössä seuranta-aikaa, että saadaan poikkeamia talteen ja sitä kautta mitattua luotettavuutta.

6. Valvontajärjestelmän toiminta. Järjestelmän toimintaa voidaan mitata käyttämällä CSF (critical success factor) - ja KPI (key performance indicator) -mittareita. CSF-tekijät tulee suunnitella alkuvaiheessa siten, että saadaan kaikki olennainen irti valvontajärjestelmästä. Esimerkiksi että saadaanko kaikki halutut tapahtumat järjestelmästä vai jääkö jotain tietoa saamatta ja eskaloidaanko tietyt tapahtumat eteenpäin jne. KPI:lla muutetaan tuo CSF-tekijä numeroiksi vertailun helpottamiseksi.

5 VALVONTAJÄRJESTELMÄT

Kappaleessa kuvataan valvontajärjestelmien keskeisiä teknisiä ominaisuuksia sekä arvioidaan niiden soveltuvuutta eri valvontatarkoituksiin. Kappaleessa ennakoidaan myös suunnittelun ja valmistelun jatkokehitystä sekä käyttöönottoa.

5.1 Valvontajärjestelmien soveltuvuuden arviointi

Seuraavassa esitellään vertailuun kaavailtuja ohjelmistoja. Osaa valvontajärjestelmistä vertaillaan syvällisemmin kappaleessa 5.1, taulukossa 1. Osa valvontajärjestelmistä jätettiin syvällisemmästä vertailusta pois, koska ne eivät sovellu valvontakäyttöön riittävän hyvin.

1. Microsoft Endpoint Configuration Manager (ConfigMgr)

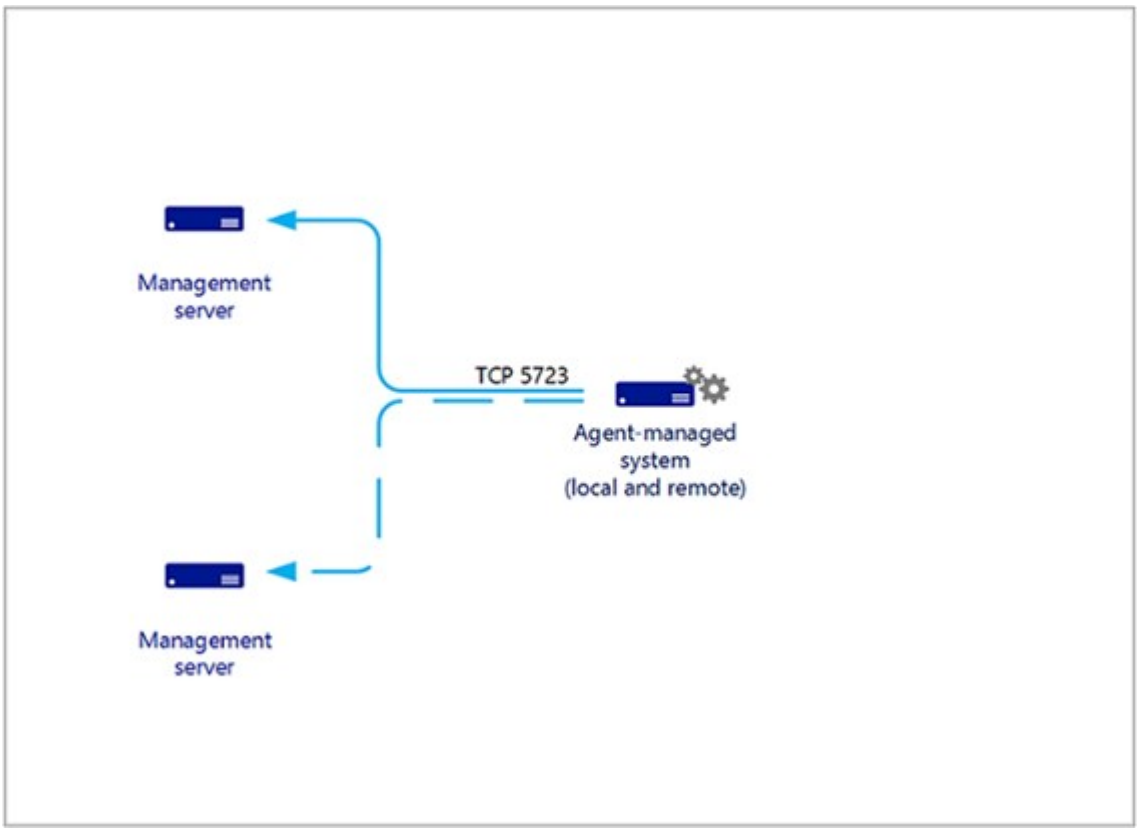
Microsoft Endpoint Configuration Manager tunnettiin aiemmin nimellä Microsoft System Center Configuration Manager. ConfigMgr:lla voidaan valvoa päätelaitteiden ja Windows-käyttöjärjestelmien tilaa. Edellyttää käytännössä ConfigMgr Client -sovelluksen asennuksen kyseiseen instanssiin. ConfigMgr hyödyntää Windows Management Instrumentation (WMI) -rajapintaa, minkä kautta se saa yksityiskohtaista tietoa kyseisestä käyttöjärjestelmästä ja laitteesta (myös virtuaalisesta), mihin se on asennettu. ConfigMgr:ssa on mm. Client Health Dashboard, mistä voi tarkastella client-asennusten tilatietoja ja ConfigMgr:sta pystyy tarkastelemaan myös kyseisen instanssin sovellus- ja laiteluetteloita. (Microsoft 2020c.)

Pääasiassa ConfigMgr on kuitenkin hallintakäyttöön (kuten ohjelmisto- ja käyttöjärjestelmäasennukset ja päivitykset) suunniteltu, joten valvontakäyttöön se ei ole optimaalinen tuote. ConfigMgr on maksullinen tuote.

2. Microsoft System Center Operations Manager (SCOM)

Microsoft System Center Operations Manager on ConfigMgr:n yhteyteen asennettava maksullinen lisäosa. SCOM on nimenomaan tarkoitettu infrastruktuurin monitorointikäyttöön. Windows-käyttöjärjestelmän osalta se kykenee valvomaan tapahtumia ja suorituskykyä. Valvonnan lisäksi kykenee suorittamaan tehtäviä ja työnkulkuja hallintapaketin mukaisesti. Windowsiin asennetaan agentti, joka lähettää valvontatietoa SCOM hallintapalvelimelle. Agentti sisältää valvottavan instanssin ”terveyttä” seuraavan palvelun. Windowsissa voidaan agentin asennus käynnistää automaattisesti koneen ilmaantuessa aktiivihakemiston (Active Directory) luetteloon.

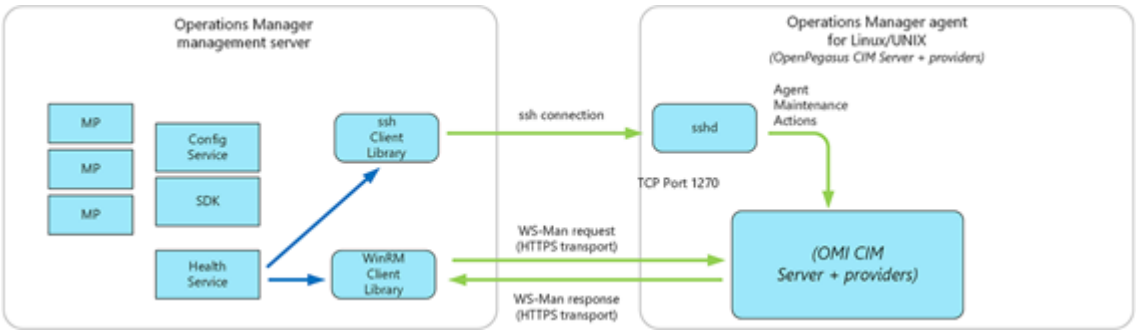
Kommunikointi hallintapalvelimien suuntaan on loogisessa mielessä yksinkertaista, kuten kuviosta 8 selviää. SCOM:issa voi asettaa sekä staattisia että itsestään skaalautuvia suorituskykymittareita, mitkä pohjautuvat Windowsin suorituskykylaskuriin. Skaalautuvista on hyötyä etenkin pitkässä juoksussa, kun suorituskykyä on ehditty seurata jonkun aikaa. Seuranta-ajan voi itse määritellä, jolloin järjestelmä kykenee esimerkiksi oppimaan toimistoajan kovimmat kuormituspiikit. SCOM:in hallintapaketteja voi ottaa käyttöön myös Powershell-skriptien avulla, joten uusien järjestelmien valvontaa voidaan nopeuttaa tekemällä valmiita skriptejä. Tähän työhön liittyen mielenkiintoinen ominaisuus on myös tilatiedon vieminen suoraan Sharepoint-sivustolle. (Microsoft 2021b).



Kuvio 8. Kommunikointi hallintapalvelimen ja Windows-agentin välillä (Microsoft 2021b)

Kuviossa 8 Agentilla hallittu järjestelmä (Agent-manager system) lähettää hallintapalvelimille (Management server(s)) tilatietojaan.

Linuxin ja Unixin osalta pystytään valvomaan massamuistia, suoritintehoa, keskusmuistia, verkkosovittimia, käyttöjärjestelmää, prosesseja ja lokitiedostoja. Linux- ja UNIX-instansseille asennetaan agentti kuten Windows-instansseille, mutta toiminta eroaa siten, että agentissa ei ole omaa Health Service -palvelua vaan tietoja lähetetään hallintapalvelimelle ”terveyden” arviointia varten. Kuviossa 9 on esitelty kommunikointi hallintapalvelimen (Operations Manager management server) ja Linux/UNIX-agentin (Operations Manager agent for Linux/UNIX) välillä.



Kuvio 9. Kommunikointi hallintapalvelimen ja Linux/UNIX-agentin välillä (Microsoft 2021b)

Kuviossa 9 hallintapalvelin (Operations Manager management server) ottaa ssh (secure shell client) -yhteyden Linux/UNIX-agenttiin (Operations Manager agent for Linux/UNIX) tehdäkseen agentin huoltotoimenpiteitä (Agent Maintenance Actions). Muu valvontakommunikointi tapahtuu HTTPS-yhteydellä WinRM-asiakaskirjaston ja OMI CIM (Open Management Infrastructure Common Information Model) -palvelun välillä.

Hajautettujen sovellusten valvontaa SCOM:illa voidaan tehdä luomalla kustomoituja hallintapaketteja (Management Pack). Hallintapakettiin konfiguroidaan kaikki komponentit valvontasääntöineen. Voidaan käyttää myös valmiiksi tehtyjä hallintapaketteja, joita löytyy paljon Internetistä etenkin Microsoftin tuotteille. (Microsoft 2021b.)

3. Progress WhatsUp Gold (WUG)

WUG on verkonvalvontasovellus, jolla voidaan valvoa verkkotopologiaa, verkon ja sovellusten suorituskykyä, pilvipohjaisia resursseja sekä hallita lokeja ja konfiguraatioita. WUG:iin saa nykyään lisäosana myös REST API:n, mikä tarjoaa mahdollisuuden luoda integraatioita muihin järjestelmiin ja automatisoida valvontatehtäviä. (Progress 2021a.) Käytännössä WUG:illa pääsee valvonnassa jo pitkälle etenkin käytettäessä suurien laitevalmistajien valmistamia päätelaitteita ja verkkolaitteita sekä yleisesti käytettyjä käyttöjärjestelmiä. G2-organisaatio arvioi WUG:in johtavaksi tuotteeksi useiden tekijöiden perusteella. Tekijöitä olivat mm. toiminnot ja toiminnallisuus sekä asiakastyytyväisyys (Progress 2021b.) G2 on käyttäjien arviointeja keräävä organisaatio (G2, 2021).

4. Nmap

Nmap on lyhennys sanoista Network Mapper. Se on avoimen lähdekoodin sovellus verkon skannaukseen ja turvallisuusauditointiin. Sillä voi mm. valvoa, mitä laitteita verkosta löytyy ja kuinka kauan palvelu tai laite on ollut toiminnassa. Nmap on konsolipohjainen sovellus, mutta siihen on saatavilla helppokäyttöisempi käyttöliittymä. (Nmap 2021.)

5. Paessler PRTG Network Monitor

PRTG Network Monitorin mainostetaan kykenemään monitoroimaan kaikkia IT-infrastruktuurin järjestelmiä, laitteita, tietoliikennettä ja sovelluksia. Sivustojen listaus PRTG Network Monitorin kyvyistä on varsin vakuuttava, se kykenee valvomaan lokitiedostoja, sharepointia, SQL-palvelinsovelluksia, Exchange-palvelinsovelluksia, varmistuksia, sähköpostia, Hyper-V:tä ja VMWarea, IIS:iä, tiedostoja jne. Paessler on useiden johtavien IT-alan yritysten kumppani. Näitä ovat mm. Fujitsu Alliance, Dell Technologies, Cisco, AXIS Communications ja VMWare Technology Alliance. (Paessler 2021t.)

6. Park Place Technologies Entuity Network Analytics (ENA)

ENA keskittyy verkon hallintaan, skannaukseen, topologiaan, tapahtumien ja liikenteen seurantaan lähde- ja kohdeportin välillä sekä sovelluksien polun seuraamiseen verkon läpi (Park Place Technologies 2021a).

Taulukkoon 1 koottiin valikoitujen järjestelmien valvontakykyvertailu valiten mm. joitakin yleisesti käytössä olevia käyttöjärjestelmiä, ohjelmistoja ja tietokantamoottoreita mukaan. Taulukosta jätettiin valvontakäyttöön huonommin soveltuvat Microsoft Configuration Manager ja Network Mapper pois. Network Mapperia käytetään pääasiassa tietoturva-auditointiin ja Microsoft Configuration Manageria laitteiden hallintaan. Mukaan valikoitui Progress WhatsUp Gold (WUG), Microsoft System Center Operations Manager (SCOM), Paessler PRTG Network Monitor (PRTG) ja Park Place Technologies Entuity Network Analytics (ENA).

Taulukon avulla nopeasti huomataan, että valvontaa pystytään varsin kattavasti suorittamaan tuotteilla WUG, SCOM ja PRTG. ENA taas on selvästi profiloitunut verkonvalvontaan. WUG on varsin kykenevä valvontaan sellaisenaan. Heikkouksia löytyy ainoastaan Windowsin ajastettujen tehtävien ja PostgreSQL:n osalta. Molemmat onnistuvat, mutta valvonnan mahdollistaminen teettää lisätyötä. SCOM taas on tarkoitettu Configuration Managerilla hallittuihin laitteisiin liittyviin operaatioihin. Se pystyy kuitenkin havaitsemaan ja ainakin osittain valvomaan laitteita, joiden IP-osoite on skannaukseen asetetulla IP-osoitealueella. VMWaren osalta SCOM vaatii hallintapaketin (Management Pack) ja toimivasta, laadukkaasta hallintapaketista voi joutua maksamaan. Myös Tomcatin ja Oraclen valvonnassa on puutteita SCOM:ssa. PRTG:llä voidaan myös kaikki vertailuun nostetut asiat toteuttaa, joten PRTG on varteenotettava vaihtoehto, mutta lisätyötä PRTG:n osalta teettävät Windowsin ajastetut tehtävät, Linux-palvelut ja Tomcat. Myös kombinaatiot WUG ja SCOM, PRTG ja SCOM voisivat olla toimiva ratkaisu, mikäli SCOM:lla valvottaisiin palvelupuolta ja WUG:illa tai PRTG:llä verkkoa. Sekä WUG:ista että PRTG:stä yhdessä ei kannata maksaa. Jatkokehityksen yhteydessä päätetään, että mitä järjestelmiä organisaatiossa valvontaan käytetään.

Taulukko 1. Valvontajärjestelmävertailu (Dell 2021; Github 2019; Hewlett Packard Enterprise 2019; Liam Matthews IT 2014; Microsoft 2017, 2019, 2020a, 2020b, 2020d, 2020e, 2020f, 2020g, 2020h, 2021a, 2021c; NZ DBA 2016; Paessler 2011, 2021a, 2021b, 2021c, 2021d, 2021e, 2021f, 2021g, 2021h, 2021i, 2021j, 2021k, 2021l, 2021m, 2021n, 2021o, 2021p, 2021q, 2021r, 2021s; Park Place Technologies 2021a; 2021b, 2021c; Progress Community 2017a; 2017b, 2017c, 2020; Burri 2019; System Center Management Pack Catalog n.d.a, System Center Management Pack Catalog n.d.b).

	Onnistuu	Osittain onnistuu tai tarvitsee toimenpiteitä	Ei tuettu	
	WUG	**SCOM**	**PRTG**	**ENA**
Laitteiden havaitseminen / skannaus				
* Virtuaalisten ympäristöjen havaitseminen				
* Tallennusjärjestelmien havaitseminen				
* Karttavisualisaatio				
Windows-palvelut				
Windows-ajastetut tehtävät				
Windows-palvelimet (ping, latenssi ja saatavuus, levyn, suorittimen ja keskusmuistin käyttöaste)				
Windows-työasemat				
Palvelimet (Esim. HPE Proliant, DELL…)				
Linux-palvelut (prosessit)				
Linux-palvelimet				
Hyper-V				
VMWare				
Verkkokomponentit				
Tietoliikenteen analysointi				
Tulostimet				
Levyjärjestelmät				
SQL Server				
PostGreSQL				
IIS				
Apache				
Tomcat				
Lokien hallinta				
Sertifikaatit				
Hälytysten eskalointi				
Toimenpiteiden eskalointi (esim. palvelimen uudelleenkäynnistykset yms.)				
Oracle				

5.2 Muita sovelluksia valvontakäyttöön

Zabbix on avoimen lähdekoodin reaaliaikainen valvontaohjelmisto. Sitä voidaan käyttää Windows-, Linux- ja UNIX-käyttöjärjestelmissä. Zabbixin valvontakyvyt näyttävät olevan varsin hyvät, erilaisia ratkaisuja löytyy vakuuttavan paljon. Sama agentti toimii useissa käyttöjärjestelmissä (Windows, Linux, Unix), ja sillä voi tehdä sekä aktiivista että reaktiivista valvontaa. Agentti kykenee valvomaan mm. tärkeimpiä resursseja (keskusmuisti, massamuisti, prosessori), palveluita (palvelu- ja prosessitilatieto, muistinkäyttö, TCP-yhteystila ja vasteaika), tiedostoja (koko, olemassaolo, tarkistussumma ja hash-summa), verkkoa (siirretyt paketit/bitit, virheet/pudotetut paketit ja törmäykset) ja lokeja (tekstiloki, Windowsin tapahtumaloki). (Zabbix 2021.)

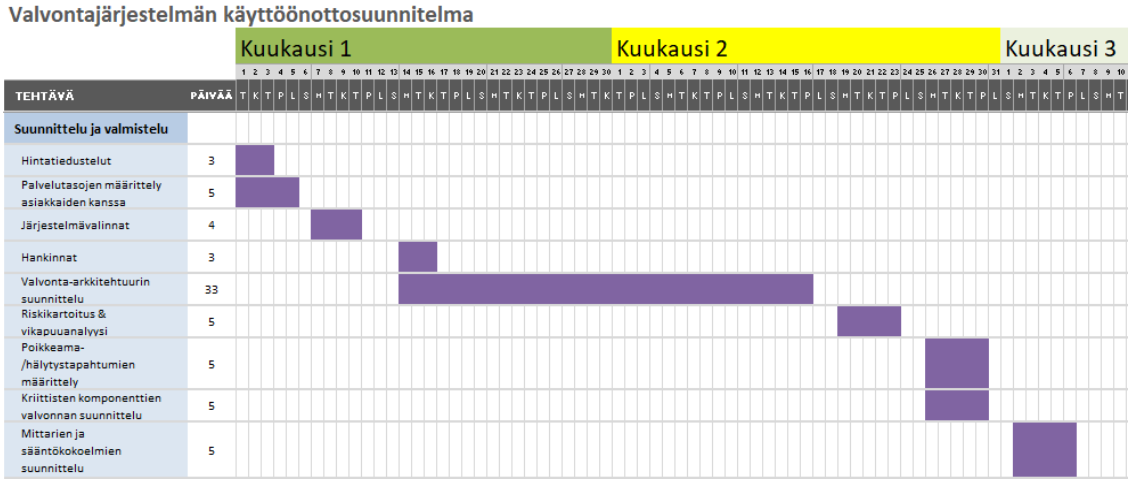
Zabbix ei ehtinyt edellisen kappaleen vertailuun mukaan mutta sitä kannattaa tarkastella ennen valvontajärjestelmähankintoja ilmaisuutensa vuoksi. Yksi tapa toimia voisi olla, että Zabbix asennetaan joka tapauksessa testimielessä ja tutkitaan ja testataan sen soveltuvuutta organisaation valvontakäyttöön.

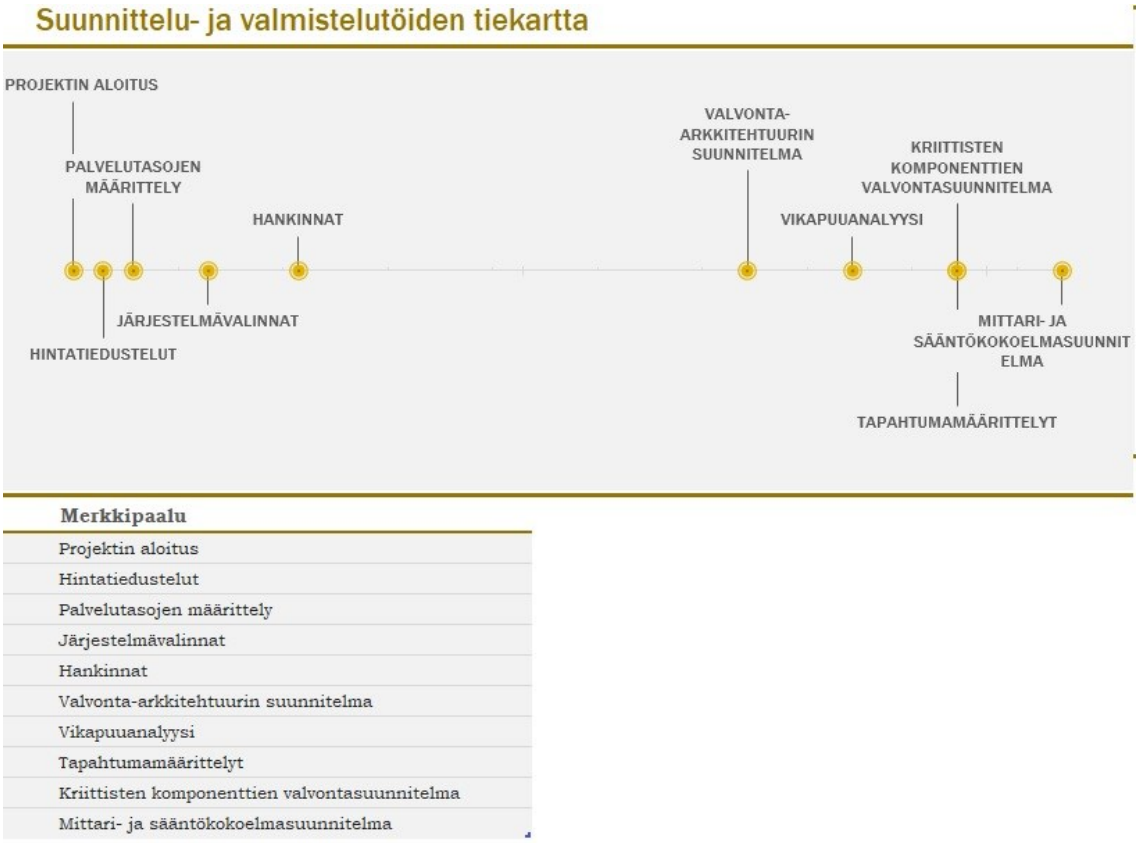
Grafana on kehittynyt maailman suosituimmaksi teknologiaksi, millä havainnollistetaan valvontatietoa. Se on skaalautuva, yksinkertainen, turvallinen ja tuettu (GrafanaLabs 2021). Käytännössä Grafana on enimmäkseen erilaisten mittarien seuraamiseen ja mitattavien asioiden visualisointiin luotu ohjelmisto, joten sen kyvyt eivät ole valvontamielessä niin hyvät. Grafanaan saakin esimerkiksi Zabbix-lisäosan, millä voi tuoda Zabbixistakin dataa Grafanaan (GrafanaLabs 2021). Grafana voisi olla käytössä Zabbixin tai vastaavan ohjelmiston rinnalla ollessaan vahva etenkin visualisoinnissa.

5.3 Jatkokehitys

Opinnäytetyössä tehdyn suunnittelun jälkeen työ jatkuu valvontajärjestelmän suunnittelu- ja valmistelutehtävillä. Tarkempi suunnitelma suunnittelu- ja valmistelutöistä on kuvattuna taulukossa 2 ja suunnittelu- ja valmistelutöiden tiekartta kuviossa 10.

Taulukko 2. Valvontajärjestelmän käyttöönottosuunnitelma: suunnittelu- ja valmistelu





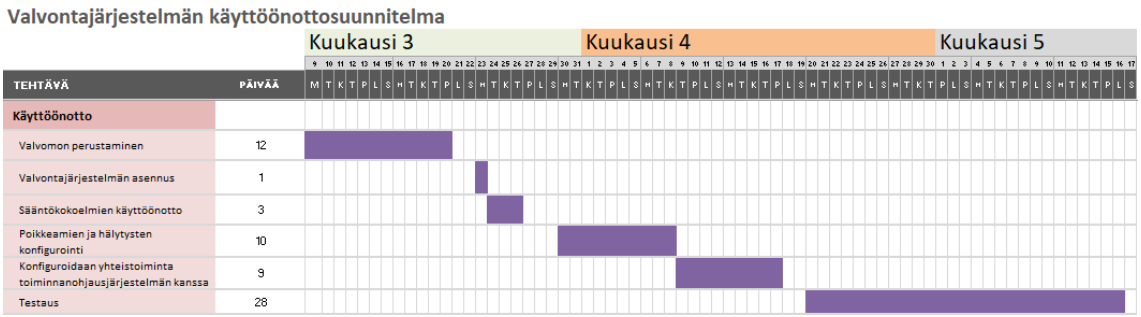
Kuvio 10. Suunnittelu- ja valmistelutehtävien tiekartta

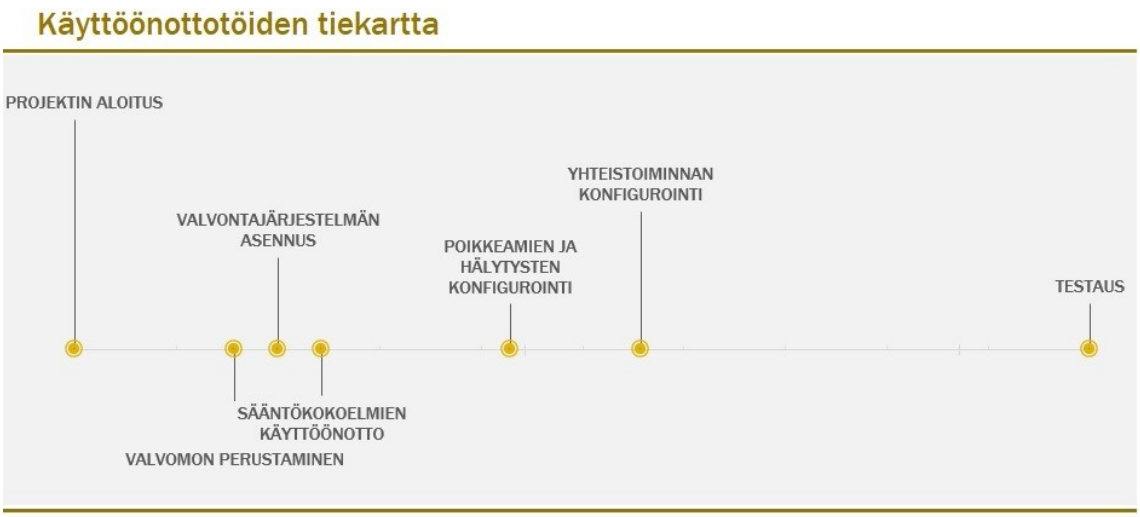
Suunnittelu- ja valmistelutehtävien jälkeen jatketaan käyttöönottotehtäviin, joiden tarkempi suunnitelma on kuvattuna taulukossa 3 ja tiekartta kuviossa 11.

Taulukko 3. Valvontajärjestelmän käyttöönottosuunnitelma: käyttöönotto

Valvontajärjestelmän käyttöönottosuunnitelma

TEHTÄVÄ	PÄIVÄÄ
Käyttöönotto	
Valvomon perustaminen	12
Valvontajärjestelmän asennus	1
Sääntökokoelmien käyttöönotto	3
Poikkeamien ja hälytysten konfigurointi	10
Konfiguroidaan yhteistoiminta toiminnanohjausjärjestelmän kanssa	9
Testaus	28





Projektin merkkipaalut

Merkkipaalu
Projektin aloitus
Valvomon perustaminen
Valvontajärjestelmän asennus
Sääntökokoelmien käyttöönotto
Poikkeamien ja hälytysten konfigurointi
Yhteistoiminnan konfigurointi
Testaus

Kuvio 11. Valvontajärjestelmän käyttöönottosuunnitelma: käyttöönottotehtävien tiekartta

Jatkokehitykseen käytetään usean eri osa-alueen asiantuntijan panosta, eri järjestelmien järjestelmäasiantuntijoista tietoliikenneasiantuntijoihin. Tämä tarkentuu mm. palvelutasomääritysten perusteella. Alkuvaiheen hankinta- ja järjestelmävalintatehtäviin riittää pienemmät henkilöresurssit.

Suunnittelutehtävien toteutuksessa tulee varmasti paljon eteen pohdittavaa, joten niihin on hyvä kohdentaa riittävästi resursseja. Mitä on järkevää valvoa? Kannattaako elinkaaren loppupuolella olevat järjestelmät jättää suosiolla pois, vai onko

niissä suurimmat riskit vanhenevien komponenttien vuoksi? Ylimääräisen työn välttämiseksi kannattaa lähitulevaisuudessa poistuvat järjestelmät jättää pois, etenkin jos niille on jo korvaava järjestelmä käytettävissä. Järjestelmävalintoja tehdessä tulee miettiä kustannuksia pitemmällä aikajanalla. Halvin, käytännössä ilmainen, valvontajärjestelmä voi tulla pitkässä juoksussa kalliimmaksi, mikäli sen toiminta vaatii enemmän henkilö- ja laiteresursseja. Toisaalta jos ilmainen ajaa saman asian samoilla resursseilla niin se on järkevä valinta.

Käyttäjien koulutus aloitetaan järjestelmän ollessa testikäytössä. Käyttöönottotöiden valmistuttua valvontajärjestelmän käyttäjien koulutusta tehostetaan ja käyttämisen voi kukin aloittaa heti koulutuksen saatuaan. Koulutuksen järjestelyt jätetään tässä vaiheessa tarkemmin suunnittelematta, koska koulutukselliset tarpeet riippuvat järjestelmävalinnoista.

6 POHDINTA

Valvontajärjestelmän hyödyntämisestä tuli työtä tehdessä ajatuksia, mitä ei sinänsä tähän työhön sisällytetä. Yhtenä ajatuksena tuli koneoppimiseen ja automatiikan käyttöön liittyen: kyseisiä tekniikoita voisi hyödyntää vikojen ennakoinnissa ja automaattisessa ratkaisussa. Koneoppimisen keinoin voitaisiin löytää vikaantumiskaavoja ja automatiikka voisi puolestaan tiettyjen oireiden ilmaantuessa tehdä palveluille korjaavia toimenpiteitä. Näihin liittyviä ajatuksia tulee todennäköisesti lisää, kun varsinaisia poikkeaman ja hälytyksen aiheuttavia tapahtumia määritetään.

Opinnäytetyössä käytiin läpi tärkeimmät valvontajärjestelmän käyttöönoton suunnitteluun liittyvät asiat. Työssä käytiin läpi valvontaan liittyvät prosessit, koska valvontajärjestelmän käyttöönotto edellyttää todennäköisesti muutoksia organisaation prosesseihin. Työssä pyrittiin löytämään olennaisimmat prosesseihin liittyvät seikat, mitkä käyttöönotossa on huomioitava. Organisaation toimintaa oli hyvä avata seuraavaksi: mihin rooleihin tarvitaan henkilöresursseja, minkälaisia vikatilanteita valvontajärjestelmän avulla voitaisiin ratkaista ja minkälaisia vaatimuksia organisaatiolla on valvontajärjestelmäkokonaisuudelle. Roolit, vaatimukset ja järjestelmästä oletettavasti saatavat hyödyt onnistuttiin listaamaan hyvin. Tämän jälkeen jatkettiin arvioimalla muutamien valvontajärjestelmien soveltuvuutta ja tekemällä jatkokehityssuunnitelmaa. Vertailu jäi tosin liian suppeaksi - valvontajärjestelmiä olisi voitu ottaa vertailuun useampia. Vertailtujen järjestelmien joukosta löytyy tosin hyviä vaihtoehtoja valvontakäyttöön. Jatkokehityssuunnitelma antaa hyvin osviittaa, että kauanko käyttöönotossa valmistelu- ja suunnittelutöineen voisi mennä, mutta aikataulu riippuu paljon organisaation ja sen tietojärjestelmien koosta, valvonnan tasosta, ja töihin saatavien resurssien määrästä ja laadusta.

Opinnäytetyön tavoitteena oli, että luotava suunnitelma auttaa läpi organisaation arvoa tuottavan valvontajärjestelmän käyttöönotossa. Työssä on pyritty huomioimaan tärkeimmät asiat, mitkä käyttöönotossa tulee huomioida, missä onkin onnistuttu. Suunnitelma antaa mahdollisuuden onnistua käyttöönotossa, mutta arvon tuottaminen läpi organisaation riippuu siitä, että kuinka laajasti järjestelmiä

valvotaan. Mikäli päätetään valvoa vain kriittisiä komponentteja tai muilla kriteereillä valittuja komponentteja, ei järjestelmä välttämättä tuota arvoa kuin valvontaan valittuihin komponentteihin liittyvien palveluiden käyttäjille.

Opinnäytetyön tarkoituksena oli, että luodaan suunnitelma niin hyvin, että tilannetietoisuutta ja tulevaisuuden ennakointia kehittävä valvontajärjestelmä on toteutettavissa mahdollisimman sujuvasti. Tarkoituksen täyttäminenkin selviää käytännössä vasta valvontajärjestelmän ollessa käytössä. Mikäli esim. havaitaan vikoja mitkä olisivat olleet valvontajärjestelmän kautta havaittavissa, on ainakin osittain epäonnistuttu. Työssä mainittujen mittarien avulla voidaan myös tarkastella valvontajärjestelmän toimivuutta määrätyn seuranta-ajan kuluttua, esim. poikkeamien välisen ajan piteneminen kertoo kehityksestä. Työssä on onnistuttu, koska luotu suunnitelma mahdollistaa tarkoituksen täyttämisen.

Valvontajärjestelmän toiminnan keskiössä on jatkuva iteratiivinen kehittäminen. Mikäli iteratiivista kehittämistä ei tehdä, tulee arvon tuottaminen pikkuhiljaa hiipumaan. Järjestelmiä, komponentteja ja sovelluksia uusitaan jatkuvalla syötöllä ja toisaalta niitä myös poistuu käytöstä. Voisikin sanoa, että valvontajärjestelmä on naimisissa muutoksenhallintaprosessin kanssa. Olennaista on myös, että valvontajärjestelmän hyöty saadaan realisoitua – käyttäjät täytyy kouluttaa valvontajärjestelmän käyttöön ja tarvittavia hallintapaketteja ja tapoja valvoa tulee etsiä ja kehittää jatkuvasti. Valvontajärjestelmän käyttöönotto edellyttää, että suunnittelu-, valmistelu- ja käyttöönottovaiheisiin saadaan riittävät resurssit, joten myös tietohallinnon ja johdon tuki on erittäin tärkeää. Tuen saamiseksi valvontajärjestelmästä saatavat hyödyt tulee tuoda ilmi päättäville tahoille. Lopullisesti valvontajärjestelmäsuunnitelman onnistuminen tai epäonnistuminen tulee kuitenkin ilmi vasta käyttöönoton yhteydessä. Tuolloin on syytä katsoa hieman taaksepäin ja ottaa tarvittaessa opiksi seuraavia suunnitelmia katsoen.

Organisaatiossa voidaan suunnitelman perusteella aloittaa jatkokehitys. Ensiksi tulee selvittää, että paljonko työhön saadaan henkilöresursseja ja tarvitaanko laitehankintoja. Valvontajärjestelmä tarvitsee vähintään yhden palvelimen, mihin ohjelmisto asennetaan. Laitehankinta voidaan tehdä samassa yhteydessä, kun

ohjelmistohankintaa tehdään. Henkilöresurssien määrän ja ammattitaidon perusteella voidaan päivittää käyttöönottosuunnitelmia ja aikatauluja. Tämän jälkeen voidaan aloittaa työt seuraamalla suunnitelmaa vaihe vaiheelta.

Suunnitelma auttaa myös siinä, että voidaan tarkentaa valvontajärjestelmän käyttöönottoon meneviä kuluja, koska tiedossa on mitä käyttöönotto vaatii. Toisaalta se auttaa tarvittaessa tekemään käyttöönoton mahdollisimman pienillä resurssitarpeilla, mikäli on tiedossa, että halutaan valvoa esimerkiksi vain tiettyjä, kriittisimpiä komponentteja.

Vertailun ja siinä tehdyn ominaisuuskartoituksen yhteydessä löydettiin paljon valmiita hallintapaketteja, joita voidaan hyödyntää käyttöönoton yhteydessä. Käyttöönoton mahdollisesti venyessä tulee kuitenkin tarkistaa, etteivät löydetyt hallintapaketit ole vanhentuneet. Valvontajärjestelmän käyttöönottotoimenpiteet kannattaakin aloittaa mahdollisimman pian.

LÄHTEET

Axelos. 2011. ITIL® Glossary of Terms English v.1.0. Luettu 8.5.2021. https://www.axelos.com/corporate/media/files/glossaries/itil_2011_glossary_gb-v1-0.pdf

Axelos. 2020. Building IT and digital excellence with ITIL 4 White Paper. Luettu 7.5.2021. https://www.axelos.com/case-studies-and-white-papers/building-it-digital-excellence-with-itil-4

Axelos. 2021. What is ITIL®? Luettu 24.4.2021. https://www.axelos.com/best-practice-solutions/itil/what-is-itil

Buehring, S. 2020. What is ITIL®: Free ebook. Luettu 8.5.2021. https://www.knowledgetrain.co.uk/it/itil/what-is-itil

Business Technology Standard. 2019. 2.2 Enterprise Architecture. Luettu 27.2.2021. https://www.managebt.org/book/demand/enterprise-architecture/

Cannon, D. 2011. ITIL Service Strategy: 2011 edition. Lontoo, The Stationery Office ltd.

Dell. 2021. Dell Server Management Pack Suite. Hallintapaketti. Luettu 31.3.2021. https://www.dell.com/support/kbdoc/fi-fi/000178001/dell-server-management-pack-suite

Ellingwood, J. 2017. An Introduction to Metrics, Monitoring, and Alerting. Luettu 7.5.2021. https://www.digitalocean.com/community/tutorials/an-introduction-to-metrics-monitoring-and-alerting

G2. 2021. Where you go to buy software. Luettu 6.5.2021. https://www.g2.com/

Github. 2019. SCOM-PKICertificateMP. Hallintapaketti. Luettu 31.3.2021. https://github.com/rafabu/SCOM-PKICertificateMP

GrafanaLabs. 2021. The analytics platform for all your metrics. Luettu 6.5.2021. https://grafana.com/grafana/

Hewlett Packard Enterprise. 2019. HPE ProLiant Management Pack for System Center Operations Manager. Hallintapaketti. Luettu 5.4.2021. https://myenterpriselicense.hpe.com/cwp-ui/free-software/HPSCOMMP-P

Hunnebeck, L. 2011. ITIL Service Design: 2011 edition. Lontoo, The Stationery Office ltd.

Julkisen hallinnon tietohallinnon neuvottelukunta. 2020. JHS 152 Prosessien kuvaaminen. Luettu 1.3.2021. https://www.suomidigi.fi/sites/default/files/2020-06/JHS152_0.doc

LIAM MATTHEWS IT. 2014. SCOM 2012 R2 – Monitor a Windows Service. Luettu 31.3.2021. https://liammatthewsit.com/2014/01/14/scom-2012-r2-monitor-a-windows-service/

Microsoft. 2017. Monitoring networks by using Operations Manager. Luettu 31.3.2021. https://docs.microsoft.com/en-us/system-center/scom/manage-monitor-networkdevice-overview?view=sc-om-2019

Microsoft. 2019. UNIX or Linux process. Luettu 31.3.2021. https://docs.microsoft.com/en-us/system-center/scom/unix-linux-process?view=sc-om-2019

Microsoft. 2020a. Dashboards in Operations Manager. Luettu 31.3.2021. https://docs.microsoft.com/en-us/system-center/scom/manage-dashboards-overview?view=sc-om-2019

Microsoft. 2020b. How to enable recovery and diagnostic tasks. Luettu 31.3.2021. https://docs.microsoft.com/en-us/system-center/scom/manage-enable-recovery-and-diagnostic-tasks?view=sc-om-2019

Microsoft. 2020c. How to monitor clients in Configuration Manager. Luettu 8.5.2021. https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/monitor-clients

Microsoft. 2020d. Integrate VMM with Operations Manager for monitoring and reporting. Luettu 31.3.2021. https://docs.microsoft.com/en-us/system-center/vmm/monitors-ops-manager?view=sc-vmm-2019

Microsoft. 2020e. Microsoft System Center 2019 Management Pack for Hyper-V. Hallintapaketti. Luettu 31.3.2021. https://www.microsoft.com/en-us/download/details.aspx?id=101312

Microsoft. 2020f. Microsoft System Center Management Pack for Internet Information Service 2016 and 1709 Plus. Hallintapaketti. Luettu 31.3.2021. https://www.microsoft.com/en-us/download/details.aspx?id=54445

Microsoft. 2020g. Microsoft System Center Management Pack for SQL Server. Hallintapaketti. Luettu 5.4.2021. https://www.microsoft.com/en-us/download/details.aspx?id=56203

Microsoft. 2020h. Microsoft System Center Management Pack for Windows Print Server 2016 and 1709 plus. Hallintapaketti. Luettu 31.3.2021. https://www.microsoft.com/en-us/download/details.aspx?id=54588

Microsoft. 2021a. Microsoft System Center Management Pack for Windows Server Operating System 2016 and above. Hallintapaketti. Luettu 31.3.2021. https://www.microsoft.com/en-us/download/details.aspx?id=54303

Microsoft. 2021b. Operations Manager agents. Luettu 3.3.2021. https://docs.microsoft.com/en-us/system-center/scom/plan-planning-agent-deployment?view=sc-om-2019

Microsoft. 2021c. System Center Management Packs for Open Source Software. Hallintapaketti. Luettu 31.3.2021. https://www.microsoft.com/en-us/download/details.aspx?id=46924

Nmap. 2021. Introduction. Luettu 4.3.2021. https://nmap.org/

NZ DBA. 2016. Monitoring Oracle Databases with SCOM. Luettu 31.3.2021. https://nzdba.wordpress.com/2016/02/21/monitoring-oracle-databases-with-scom/

Optanix. 2020. What's the Difference Between ITIL Event, Incident and Problem Management, and How Are They Related? Luettu 8.5.2021. https://www.optanix.com/events-incidents-and-problems-how-are-they-related/

Overby, Greiner & Gibbons Paul. 2017. What is an SLA? Best practices for service-level agreements. Luettu 7.5.2021. https://www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html

Paessler. 2011. Monitoring processes in Linux. Luettu 5.4.2021. https://kb.paessler.com/en/topic/29403-monitoring-processes-in-linux

Paessler. 2021a. Computer monitoring with PRTG. Hallintapaketti. Luettu 5.4.2021. https://www.paessler.com/computer_monitoring

Paessler. 2021b. Dell monitoring: Premium monitoring for hardware, hard disks, and servers. Luettu 5.4.2021. https://www.paessler.com/dell-monitoring

Paessler. 2021c. Features to help you monitor anything. Luettu 5.4.2021. https://www.paessler.com/prtg/features

Paessler. 2021d. Fix database errors with PRTG Oracle monitoring. Luettu 5.4.2021. https://www.paessler.com/oracle_monitoring

Paessler. 2021e. Monitor PostgreSQL databases with PRTG. Luettu 5.4.2021. https://www.paessler.com/postgresql-monitoring

Paessler. 2021f. Professional host and server monitoring software. Luettu 5.4.2021. https://www.paessler.com/server_monitoring_software

Paessler. 2021g. PRTG as a network analyzer: Powerful and user-friendly. Luettu 5.4.2021. https://www.paessler.com/network-analyzer

Paessler. 2021h. PRTG Manual: HTTP Apache ModStatus PerfStats Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/http_apache_modstatus_perfstats_sensor

Paessler. 2021i. PRTG Manual: Hyper-V Host Server Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/hyper_v_host_server_sensor

Paessler. 2021j. PRTG Manual: Logs. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/logs

Paessler. 2021k. PRTG Manual: Microsoft SQL v2 Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/microsoft_sql_v2_sensor

Paessler. 2021l. PRTG Manual: SNMP HPE ProLiant System Health Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/snmp_hp_proliant_system_health_sensor

Paessler. 2021m. PRTG Manual: SNMP Linux Load Average Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/snmp_linux_load_average_sensor

Paessler. 2021n. PRTG Manual: SNMP Printer Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/snmp_printer_sensor

Paessler. 2021o. PRTG Manual: SSL Certificate Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/ssl_certificate_sensor

Paessler. 2021p. PRTG Manual: VMware Host Hardware (WBEM) Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/vmware_host_hardware_wbem_sensor

Paessler. 2021q. PRTG Manual: VMware Virtual Machine (SOAP) Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/vmware_virtual_machine_soap_sensor

Paessler. 2021r. PRTG Manual: Windows IIS Application Sensor. Käyttöohje. Luettu 5.4.2021. https://www.paessler.com/manuals/prtg/wmi_iis_application_sensor

Paessler. 2021s. Storage monitoring with PRTG. Luettu 5.4.2021. https://www.paessler.com/storage-monitoring

Paessler. 2021t. The monitoring solution for all areas of IT. Luettu 1.4.2021. https://www.paessler.com/monitoring

Park Place Technologies. 2021a. Key Features. Luettu 4.3.2021. https://www.parkplacetechnologies.com/entuity-network-analytics/

Park Place Technologies. 2021b. Network Discovery™. Luettu 5.4.2021. https://www.parkplacetechnologies.com/entuity-network-analytics/network-discovery/

Park Place Technologies. 2021c. Network Topology Mapping. Luettu 5.4.2021. https://www.parkplacetechnologies.com/entuity-network-analytics/network-topology-mapping/

Prescient. 2016. Monitoring Lets You Be Reactive and Proactive, and You Need to be Both. Luettu 7.5.2021. https://www.prescientsolutions.com/blog/monitoring-lets-reactive-proactive-need/

Progress Community. 2017a. APM Profile - Apache Web Server. Sovelluksen suorituskyvyn valvontaprofiili. Luettu 20.3.2021. https://community.progress.com/s/question/0D54Q00007oKeC6SAK/apm-profile-apache-web-server

Progress Community. 2017b. APM Profile - Dell Server Health Monitor (OM v6.5). Sovelluksen suorituskyvyn valvontaprofiili. Luettu 20.3.2021. https://community.progress.com/s/question/0D54Q00007oKeBiSAK/apm-profile-dell-server-health-monitor-om-v65

Progress Community. 2017c. APM Profile - IIS. Sovelluksen suorituskyvyn valvontaprofiili. Luettu 20.3.2021. https://community.progress.com/s/question/0D54Q00007oKeBRSA0/apm-profile-iis

Progress Community. 2020. Monitoring performance on Unix and Linux. Luettu 20.3.2021. https://community.progress.com/s/article/Monitoring-performance-on-Unix-and-Linux-1307717739619

Progress. 2021a. WhatsUp Gold. Luettu 4.3.2021. https://www.whatsupgold.com/

Progress. 2021b. WhatsUp Gold Named a Leader in Report for Network Management. Luettu 6.5.2021. https://www.whatsupgold.com/resources/analyst-reports/whatsup-gold-named-a-leader-in-report-for-network-management

Raphael Burri. 2019. Open Source – Scheduled Task and PS Scheduled Job Management Pack for SCOM 2012 / 2016 / 2019. Hallintapaketti. Luettu 5.4.2021. https://rburri.wordpress.com/2019/10/30/open-source-scheduled-task-and-ps-scheduled-job-management-pack-for-scom-2012-2016-2019/

Salo, A. 2007. Luento 4 Vikapuuanalyysit. Luentomateriaali. Luettu 8.5.2021. http://salserver.org.aalto.fi/vanhat_sivut/Opinnot/Mat-2.3117/luennot/luento04.pdf

Santoshi. 2019. ITIL Event Management. Luettu 8.5.2021. https://www.itil-docs.com/itil-event-management/

Steinberg, R. 2011. ITIL Service Operation: 2011 edition. Lontoo, The Stationery Office ltd.

System Center Management Pack Catalog. n.d.a Community.VMware 1.0.2.0 (Management Pack). Hallintapaketti. Luettu 31.3.2021. https://systemcenter.wiki/?Get-ManagementPack=Community.VMware&Version=1.0.2.0

System Center Management Pack Catalog. n.d.b Microsoft System Center Management Pack for Windows 10. Hallintapaketti. Luettu 31.3.2021. https://systemcenter.wiki/?Get-ManagementPack=Microsoft.Windows.Client.Win10&Version=10.0.0.0

Zabbix. 2021. Solutions. Luettu 30.4.2021. https://www.zabbix.com/solutions