Joni Nevalainen

Valvontadatan keräys ja visualisointi

Sähkötekniikan korkeakoulu

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 30.5.2011.

Työn valvoja:

Prof. Jukka Manner

Työn ohjaaja:

FM Tero Tuononen

Aalto-yliopisto
Sähkötekniikan korkeakoulu

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Joni Nevalainen

Työn nimi: Valvontadatan keräys ja visualisointi

Päivämäärä: 30.5.2011 Kieli: Suomi Sivumäärä:7+47

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotekniikka Koodi: S-38

Valvoja: Prof. Jukka Manner

Ohjaaja: FM Tero Tuononen

Työ on ollut case-tutkimus valvontadatapalvelimen suunnittelusta ja pystyttämisestä. Palvelin sijoitettiin julkisesti saataville, ja se ottaa ajastetusti vastaan muualla mitattua julkistamiskelpoista dataa.
Tämän tutkimuksen päämääränä on selvittää keskitetyn valvontadatan visualisointijärjestelmän vaihtoehtoja, jotka tuottaisivat graafeja sekä asiakkaille järjestelmien kuormitus- ja käyttöasteesta, että johdolle ja ylläpidolle komponenttien tilasta, vikatiheydestä ja käyttöpolitiikan noudattamisesta. Tavoitteena on myös aloittaa järjestelmän pystyttäminen ja todentaa sen toimivuus ja jatkokehitysmahdollisuudet. Palvelimella hyödynnetään ilmaisia ja avoimia ohjelmistoja, jotta ratkaisu voitaisiin toistaa tarvittaessa muissa ympäristöissä pienin kustannuksin. Palvelimen ensimmäiseksi datalähteeksi valittiin konesalien tehomittaukset. Järjestelmän tietoturvasta pyritään pitämään huolta automaattisilla päivityksillä sekä tiedonkeräystapojen valinnalla.
Tutkimuksessa painotetaan valvontajärjestelmän toteutuksen suunnittelua sekä toteutuksen käyttöönoton edistämistä organisaatiossa. Dokumentin on tarkoitus olla apuna muille ylläpitäjille sekä organisaatioille vastaavien projektien harkinnassa sekä toteuttamisessa. Tutkimusmenetelminä käytettiin kirjallisuustutkimusta sekä käytännön toteutuksen myötä oppimista.
Olennaiset tulokset työstä ovat että tehonkäytön hyötysuhde (PUE)-mittari kaipaa kehittämistä tai suhteuttamista muihin konesalin tunnuslukuihin edistääkseen parhaiten ympäristötavoitteita. Samoin datan tallentaminen useassa muodossa mahdollistaa jatkokehityksen kuten datan avaamisen julkiseksi tai uusien visualisointityökalujen käyttöönoton.

Avainsanat: valvonta, PUE, konesali, SNMP, visualisointi, Cacti

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Joni Nevalainen

Title: Gathering and visualization of monitoring data

Date: 30.5.2011 Language: Finnish Number of pages:7+47

Department of Communications and Networking

Professorship: Networking technology Code: S-38

Supervisor: Prof. Jukka Manner

Instructor: M.A. Tero Tuononen

This work is a case study in design and implementation of a system monitoring service. The service was made available to everyone, and the server receives scheduled transfers of measurements done elsewhere that are cleared for publishing.
The aim of this research is to research alternatives for a centralized visualization system for operations monitoring, with the main function to produce informative graphs of both system load and usage for the end-users and system status, error frequencies and compliance with usage guidelines for the system administrators and managers. Part of that aim is to set up an intial system and verify it's functions and development potential. As a principle, free and open source software are prioritized, so that the solution would be re-usable in other environments with minimal costs. The first dataset was chosen to be machine hall power usage measurements. System security is designed to be upheld by automatic applying of updates and design of information flows.
The research puts focus on the planning phase and the deployment of the platform inside the organization. This work is intended to help other administrators and organizations in planning and implementing similar projects. Research methods used include literature research and learning through implementation.
Relevant results of this work are that the use of Power Usage Efficiency (PUE) as the defining factor of machine halls environmental effectiveness requires more investigation, or at least comparisons to other factors of machine halls to better reflect its environmental goals. Also, the storage of data in multiple formats allows further development, like wider publication of data and deployment of improved visualization tools.

Keywords: monitoring, PUE, co-location, SNMP, visualization, Cacti

Esipuhe

Haluan kiittää valvojaani, professori Jukka Manneria sekä ohjaajaani Tero Tuonosta tarjoamistaan mahdollisuuksista työn aikaansaamiseksi. Erityiskiitokset suon ystävälleni, DI Risto Järviselle sinnikkäästä kannustamisestaan ja käytännönläheisestä otteestaan pitkän prosessin kaikissa vaiheissa. Aliarvioimatta voin todeta että ilman Ristoa työn valmistuminen olisi pitkittynyt merkittävästi.

Kiitän myös entisen TKK:n, nykyisen Aalto-yliopiston sähkötekniikan korkeakoulun sekä muiden Aallon teknisten korkeakoulujen opettajia, joiden opetuksesta olen päässyt osalliseksi vuosien varrella. Kunkin alansa huiput ovat olleet asioista hyvin perillä sekä kertoneet välillä yllättäviäkin totuuksia elämän osa-alueilta. Suomen valtiota ja kaikkia sen tunnollisia veronmaksajia kiitän koulutuspuitteiden järjestämisestä, pyrin olemaan investointinne arvoinen. Kiitän myös sähköosaston henkilökuntaa, joista erityisesti Mika Nupposta, Seppo Saastamoista sekä Viktor Nässiä. He ovat osoittaneet esimerkillistä käytännöntajua sekä opiskelijaystävällisyyttä toimissaan, ja suurelta osin varmistavat sen että opiskelijoilla on myös realistiset valmiudet kestää vaatimusten puristuksessa ja valmistua niin käytännön järjestelyiden kuin henkisen eheydenkin osalta. Kiitän CSC:tä työjoustojen tarjoamisesta opintojeni loppuunsaattamiseksi, sekä lukuisia kollegoitani joiden pitkäaikainen panos on saanut aikaan monia toimivia ratkaisuja sekä mielekkään työympäristön.

Kirjoitusprosessin varrelta haluan myös kiittää vanhempiani sekä sisaruksiani tuesta sekä ymmärryksestä kirjoitusprosessin aikana. Kiitän myös läheisiä ihmisiäni, ystäviä ja tuttavia jotka ovat tasapainottaneet elämää näinä luomisen aikoina.

Antoisia lukuhetkiä valvontadatan parissa, tavataan työelämässä.

Otaniemi, 30.5.2011

Joni A. Nevalainen

Sisältö

Lyhenteet

AD	Active Directory, LDAPin sukulaishakemistoprotokolla
BITS	Background Intelligent Transfer Service, Microsoftin tiedonsiirtoprotokolla
CPU	Central Processing Unit, tietokoneen suoritin
CSC	Center of Scientific Computing, CSC - Tieteen tietotekniikan keskus Oy on Opetusministeriön alainen valtion tietotekniikka-yritys
DHCP	Dynamic Host Configuration Protocol, verkkoasetusten jakoprotokolla
DOS	Disk Operating System, varhainen käyttöjärjestelmä
DRAC	Dell Remote Access Controller, IPMIn yksi valmistajatoteutus
FAT	File Allocation Table, tiedostojärjestelmä
FUNET	Finnish University and Research Network, suomalainen runkoverkko
GSM	Global System for Mobile communications, matkapuhelinjärjestelmä
HF	High Frequency, sähkömagneettisen säteilyn aallonpituudet 3 - 30 MHz
HTTP	HyperText Transfer Protocol, WWW:n ydinprotokolla
IETF	Internet Engineering Task Force, Internet-standardointiorganisaatio
IIS	Internet Information Services, Microsoftin WWW-palvelin
IP	Internet Protocol, tietoliikenneprotokolla
IPMI	Intelligent Platform Management Interface, hallintarajapinta
IT	Information Technology, sähköiset palvelut ja kaikki niiden tuottamiseen liittyvä
ITIL	Information Technology Infrastructure Library, prosessikirjasarja
JSON	Javascript Object Notation, tiedon esitystapa
LAMP	Linux, Apache, MySQL, PHP, yleinen ohjelmistokokonaisuus
LDAP	Lightweight Directory Access Protocol, hakemistoprotokolla
MMS	Multimedia Messaging Service, viestistandardi
MOM	Microsoft Operations Manager, palvelimien hallintapalvelin
NAS	Network Attached Storage, tiedostopalvelin
NFS	Network File System, tiedontallennustapa jossa verkkoliikenne hoidetaan tiedostotasolla
NTFS	New Technology File System, tiedostojärjestelmä
NTP	Network Time Protocol, aikapalveluprotokolla
PERL	Practical Extraction and Report Language, ohjelmointikieli
PHP	PHP: Hypertext Preprocessor, verkkosivujen ohjelmointikieli
PUE	Power Usage Effectiveness, ekologisuusmittari
RAID	Redundant Array of Inexpensive Disks, tiedontallennustapa

RFC	Request For Comments, IETF:n julkaisema Internet-standardi
RMON	Remote Monitoring, verkonvalvontastandardi
RPM	RPM Package Manager, ohjelmistojen paketointijärjestelmä
RRD	Round Robin Database, tiedonvarastointitapa
SAN	Storage Area Network, tiedontallennustapa jossa verkkoliikenne hoidetaan laitelohkotasolla
SCCM	System Center Configuration Manager, Microsoftin SMS:n uudempi versio
SIP	Session Initiation Protocol, Internet-puheluprotokolla
SLA	Service Level Agreement, sopimus palveluntarjoajan ja -saajan välillä
SMART	Self-Monitoring Analysis and Reporting Technology, kovalevyjen diagnostiikkatyökalu
SMS	Systems Management Server, Microsoftin ohjelmistojenjakopalvelin
SNMP	Simple Network Management Protocol, hallintaprotokolla
SQL	Structured Query Language, tietokantarajapinta
SSH	Secure SHell, suojattu verkkoliikennöintiprotokolla
SWOT	Strenths-Weaknessess-Opportunities-Threats, analyysimalli
UPS	Uninterruptible Power Supply, varmistettu virransyöttöjärjestelmä
USB	Universal Serial Bus, lisälaitteiden liitäntäväylä
VOIP	Voice Over IP, Internet-puhelupalvelu
VPN	Virtual Private Network, verkonsiirtoprotokolla
WLAN	Wireless Local Area Network, langaton verkko
WMI	Windows Management Instrumentation, Microsoftin järjestelmärajapinta
WWW	World Wide Web, hyperdokumenttipalvelu
XML	Extensible Markup Language, rakenteistettu tiedonesitystapa
ZFS	Zettabyte File System, monipuolinen tiedostojärjestelmä

1 Johdanto

Tietokoneilla voidaan nopeuttaa monia laskentaa vaativia tehtäviä, viestiä ympäri maailmaa ja käsitellä mediaa eri muodoissaan. Nämä ja muut toiminnot ovat mahdollisia jos koneet toimivat odotetusti ja niiden käyttöedellytykset ovat kunnossa — sähköä on saatavilla oikealla jännitteellä ja vakaasti, jäähdytys toimii jotta osat eivät ylikuumene, kuluvien osien kuten kovalevyjen käyttöikää on vielä jäljellä, kaapelit ovat kunnossa eivätkä hiirenjyrsimiä, käyttöjärjestelmät ja ohjelmistot eivät kohtaa odottamattomia virhetilanteita eikä verkkoyhteyksissä ole tukkoisuutta.

Laitteiden elinkaari on rajallinen, ja niiden uusiminen maksaa. Yksi hyvä käyttöiän mittari on takuun tai huoltosopimuksen pituus, eli miten pitkään koneille on saatavissa varaosia ilman lisäkustannuksia. Osien takuuvaihdon yhteydessä tosin aiheutuu palvelukatko jonka kesto riippuu ongelman laadusta. Jos katko tehdään vasta vian ilmettyä, palveluiden saatavuus ei ole suoraan ennakoitavissa ilman varajärjestelmiä. Tämä on perinteinen reaktiivinen ongelmanratkaisutapa, jossa viat korjataan sitä mukaa kun ne havaitaan.

Entä jos laitteiden toimintatilasta ja kestävyydestä olisi saatavissa ennusmerkkejä? Riittääkö kapasiteetti kasvavalle asiakasmäärälle vai pitääkö tehdä lisäinvestointeja? Mikä on palvelun kuormitusaste? Mitä lämpötilapiikki saakaan konesalissa aikaan ja miten tärkeää on ehkäistä lämpötilamuutokset jatkossa? Kuinka paljon sähköä eri laitteistot kuluttavat ja missä olisi säästövaraa? Dataa voidaan kerätä nykyään jo varsin monesta paikasta, mutta datamassan jatkojalostaminen käyttökelpoiseksi tiedoksi on vielä yksittäisten ohjelmistojen ominaisuuksien varassa. Eri näkymiä katsomaan tarvitaan mahdollisesti useita päivystäjiä ja toisistaan riippuvien ongelmavyyhtien havaitseminen on sattumanvaraista.

1.1 Tutkimuksen tavoitteet

Tämän tutkimuksen päämääränä on selvittää keskitetyn valvontadatan visualisointijärjestelmän vaihtoehtoja, jotka tuottaisivat graafeja sekä asiakkaille järjestelmien kuormitus- ja käyttöasteesta, että johdolle ja ylläpidolle komponenttien tilasta, vikatiheydestä ja käyttöpolitiikan noudattamisesta. Tavoitteena on myös aloittaa järjestelmän pystyttäminen ja todentaa sen toimivuus ja jatkokehitysmahdollisuudet. Palvelimella hyödynnetään ilmaisia ja avoimia ohjelmistoja, jotta ratkaisu voitaisiin toistaa tarvittaessa muissa ympäristöissä pienin kustannuksin. Palvelimen ensimmäiseksi datalähteeksi valittiin konesalien tehomittaukset. Järjestelmän tietoturvasta pyritään pitämään huolta automaattisilla päivityksillä sekä tiedonkeräystapojen

valinnalla.

Tutkimuksessa painotetaan valvontajärjestelmän toteutuksen suunnittelua sekä toteutuksen käyttöönoton edistämistä organisaatiossa. Dokumentin on tarkoitus olla apuna muille ylläpitäjille sekä organisaatioille vastaavien projektien harkinnassa sekä toteuttamisessa. Tutkimusmenetelminä käytettiin kirjallisuustutkimusta sekä käytännön toteutuksen myötä oppimista.

Olennaiset tulokset työstä ovat että tehonkäytön hyötysuhde (PUE)-mittari kaipaa kehittämistä tai suhteuttamista muihin konesalin tunnuslukuihin edistääkseen parhaiten ympäristötavoitteita. Tutkimuksessa ehdotetaan korvaajaksi System Power Efficiency (SPE) lukua. Samoin datan tallentaminen useassa muodossa mahdollistaa jatkokehityksen kuten datan avaamisen julkiseksi tai uusien visualisointityökalujen käyttöönoton.

1.2 Työn rakenne

Työssä käydään aluksi läpi olemassa olevien järjestelmien ja tekniikoiden tärkeimmät yksityiskohdat tämän työn kannalta luvussa 2. Näiden taustatietojen voimin edetään luvussa 3 nykytila-analyysiin sekä selitetään toimintaympäristö että olemassa olevat valvontajärjestelmät. Luvussa käydään myös läpi mahdollisia kehityspolkuja valvonnan parantamiseksi.

Ratkaisumalli esitetään luvussa 4, painottuen tekniseen toteutukseen sekä käytännön toimiin organisaation prosessien hyödyntämiseksi uuden järjestelmän pystyttämisessä. Luvun lopussa käydään läpi tyypilliset valvontajärjestelmän käyttötavat sekä sen kytkökset muihin organisaation osiin sekä asiakkaisiin.

Luvussa 5 suoritetaan jatkopohdinnat tulevista kehityskohteista joita ei toteutettu tämän työn puitteissa. Järjestelmä on toimiessaan jatkuvan kehityksen alainen prosessi, jota tullaan eittämättä hyödyntämään uusillakin osa-alueilla kun perusteet on luotu.

2 Järjestelmävalvonnan osa-alueet

Tietotekniikan kehitys perustuu onneksemme menneille saavutuksille, uudelleenkäytettäville ohjelmistokomponenteille, kirjastoille sekä rajapinnoille. Ongelmia ratkoessa voi säästää paljonkin aikaa löytämällä valmiin ratkaisun jollekin osa-alueelle, kuten tiedon varastointiin, sen hakemiseen, verkossa siirtämiseen tai palautteen käsittelyyn. Tämä luku käsittelee valvontadatan keruun ja visualisoinnin kannalta olennaisia olemassa olevia tekniikoita, sekä erinäisiä tietotekniikan osa-alueita joiden valvomisesta on hyötyä.

2.1 Tallennusmediat

Käytössä oleva tietotekniikka kaipaa huoltoa ja korjausta ajan myötä, ja toisaalta komponentit jotka on todella suunniteltu kestämään (kuten avaruustekniikassa) ovat huomattavan kalliita. Kuluttajille valmistettavien laitteistojen hinnat ovat hyvin kilpailukykyisiä suurien valmistusmäärien ansiosta, joten osa Internetin palvelimista on toteutettu kuluttajatason laitteilla. Mekaanisesti pyörivät magneettikovalevyt ovat tällä hetkellä kustannustehokkain tapa varastoida satoja gigatavuja tietoa. Käsittelemme seuraavaksi niihin liittyviä ominaisuuksia sekä muita toimivan tietojärjestelmän edellytyksiä.

Googlen tekemässä tutkimuksessa ei havaittu yhteyttä kovalevyjen virheentymistiheyden ja niiden käyttölämpötilan tai käyttökuorman välillä. Levyjen SMART (Self-Monitoring Analysis and Reporting Technology) tietueisiin kirjattujen virheiden määrä täsmäsi vikaantumistodennäköisyyden kanssa, mutta näistä saatiin huonosti ennakkovaroituksia (56% levyistä ei osoittanut vikaantumisen merkkejä SMART-tiedoissaan ennen hajoamistaan) joten SMART-tiedot eivät sovellu vikaantumisen ennusmerkiksi. [1]

Tyypillinen tapa suojautua datahävikiltä levyvirheiden sattuessa on käyttää RAID-teknologiaa (Redundant Array of Inexpensive Disks) [2]. Perusidea on datan tallentaminen useampaan kertaan erillisille fyysisille levyille, jotta yhden vikaantuessa dataa ei vielä menetetä. Käyttötavasta riippuen RAID-pakka voidaan määrittää käyttämään RAID-tasoa 0, 1, 5, 1+0 tai 6.

RAID 0 nopeuttaa datan siirtoa käyttämällä yhtä aikaa useampaa levyä datan tallentamiseen lomittain levyille – virhetodennäköisyys tällöin tosin kasvaa koska datan eheys riippuu molempien levyjen kunnosta. RAID 1 parantaa datan luotettavuutta kirjoittamalla saman datan kahdelle levylle yhtä aikaa. RAID 5 kirjoittaa vähintään kolmelle levylle datan sekä tarkistussumman datasta, jolloin yhden le-

vyn puute voidaan paikata laskemalla puuttuva data tarkistussummasta. RAID 6 kirjoittaa vähintään neljälle levylle datan ja kaksi eri tarkistussummaa, jotta järjestelmä sietää kahden levyn rikkoutumisen datan katoamatta. RAID 1+0 tarvitsee vähintään neljä levyä kirjoittaakseen saman datan kahdelle levylle ja lomittamalla sen kahdelle muulle.

Suosittu RAID-levyjen käyttötapa on RAID 5, joka tarjoaa esimerkiksi neljän samankokoisen levyn järjestelmässä $\frac{3}{4}$ levyjen yhteenlasketusta kapasiteetista käyttöön. RAID 5:lla saavutettavan kapasiteetin laskentakaava on seuraava:

$$\text{kapasiteetti} = \text{pienin levykoko} \times (\text{levyjen määrä} - 1) \tag{1}$$

Toteutustapoja on sekä laitteisto- että ohjelmistopohjaisia. Laitteistopohjalla tarkistussummien laskeminen ei kuormita muuta järjestelmää, kun taas ohjelmistopohjaisella toteutuksella ei tarvitse huolehtia RAID-laitteiston vikaantumisesta ja identtisen laskentapiirin hankkimisesta.

RAID-järjestelmän haitta on pystytetyn järjestelmän joustamattomuus: tallennuskapasiteetin kasvattaminen uusia levyjä lisäämällä vaatii datan siirtoa muualle tai toisen RAID-levyn luomista. Tätä voidaan kiertää Linuxin LVM:n (Logical Volume Management) avulla joka niputtaa sille lisätyn kapasiteetin yhdeksi joustavaksi virtuaalilevyksi [3]. Toinen haitta on valvonnan tarve: yhden levyn hajotessa järjestelmä voi toimia vielä normaalisti, mutta vikaantuminen pitää huomata ja korjata ennenkuin toinenkin levy hajoaa ja dataa katoaa. Valvontatyökalut vaihtelevat toteutuksesta riippuen, erityisesti rautapohjaisille RAID-järjestelyille vaaditaan omat ajurit ja ohjelmistot niiden tilan seuraamiseksi, sekä prosessi mittavankin palvelinmäärän virheilmoitusten seuraamiseksi.

RAID-levyjärjestelmä voi olla neljässä tilassa: Active, Degraded, Rebuilding, Failed. Active-tilassa levyt toimivat kuten pitää, Degraded-tilassa tieto siirtyy vielä ongelmitta mutta ainakin yhdellä levyllä on havaittu virhe (hetkellinen kuten koneen kaatuminen tai pysyvä kuten lukukelvoton lohko). Failed-tilassa tieto ei enää siirry ja virheitä on tullut liikaa korjattavaksi. Rebuilding-tilassa järjestelmää koitetaan kirjoittaa takaisin virheettömäksi. Degraded-tilasta olisi syytä saada tieto järjestelmän ylläpitäjälle koska kone vaikuttaa muuten vielä toimivan normaalisti. Riippuen RAIDin toteutustavasta tieto voidaan saada käyttöjärjestelmän tai laitteiston puolelta soveltuvin komennoin.

Nykyisistä yli 100 GB magneettikiekkoperustaisista levyistä löytyy kalliimpia RAID-käyttöön suunniteltuja levyjä. Ero perustuu levyn reagointiaikoihin virhetilanteissa: kuluttajalevyt voivat koittaa paikata virheitään sisäisellä virheenkorjauk-

sellaan niin kauan että RAID-toiminnassa levyn vasteaika ylittää 10-20 sekuntia ja RAID-ohjain tulkitsee levyn virheelliseksi, siirtyen Degraded-tilaan [4]. RAID-versioissa levy ei yritä sisäistä toipumista niin pitkään, jolloin RAID-logiikka tulkitsee vain yksittäisen levyn sektorin virheelliseksi ja monistaa tarvitun tiedon muilta RAID-pakan levyiltä.

Storage Area Network (SAN) on tapa jakaa osioituja kovalevylohkoja erillisverkkoa pitkin palvelimille [5]. Osiot voivat olla tehtyjä esimerkiksi RAID-levyjärjestelmän päälle. Verkon nopeus ja luotettavuus on SAN-levyä käytettäessä avainasemassa, toisaalta koska data siirretään levylohkoina niin tiedostorajoitukset tulevat kunkin asiakaskoneen tiedostojärjestelmien puolelta. SAN-verkko toteutetaan tyypillisesti Fibre Channel -valokuituverkolla, jolloin jokainen siihen kytkeytyvä palvelin varustetaan erillisellä verkkokortilla joka on omistettu vain SAN-käyttöön. Fibre Channel -verkko ei sinällään rajoita teknologiaa käytettäväksi pelkästään valokuitulinkeillä, vaan kuparikaapeleillekin on olemassa määritykset.

Kun kovalevyjen osioinnit ja käyttötavat on saatu tehtyä, on aika valita käytettävä tiedostojärjestelmä. Tiedostojärjestelmä on sovittu tapa tallentaa tietoa kovalevylle ja luoda tallennetulle tiedolle hakurakenne. Seuraavassa aliluvussa tarkastellaan neljän järjestelmän etuja ja haittoja: FAT32, NTFS, Ext3 sekä ZFS. Tiedostojärjestelmiä on näiden lisäksi olemassa kymmenittäin lisää [6].

2.2 Tiedostojärjestelmät

FAT32 on viimeisin versio File Allocation Table tiedostojärjestelmien perheestä, jota on käytetty Disk Operating System (DOS) ajoista saakka. Tuki järjestelmälle on hyvin yleistä niin että kaikki käyttöjärjestelmät osavat lukea ja kirjoittaa FAT32-tiedostojärjestelmän levyjä. FAT32 on erityisen suosittu järjestelmä siirrettävissä medioissa, kuten kameroiden muistikorteissa, USB-tikuissa sekä siirtokovalevyissä. Diagnostiikkaa ja ylläpitoa varten tehdyt mediat pidetään myös usein FAT-formatoituina koska tietokoneen Basic Input/Output System (BIOS) osaa lukea niitä. FAT32:n rajoituksina ovat maksimissaan 4 GB tiedostokoko ja 8 TB osiokoko, joskin Windows rajoittaa luotaessa FAT32-osion kooksi max 32 GB tehokkuussyistä. Tämä rajoitus ei estä muilla työkaluilla tehtyjen suurempien FAT32-levyjen käyttämistä. FAT32:n tiedostojärjestelmän korjaustyökalut voidaan ajaa tiedostojärjestelmän ollessa käytössä. Korjaukseen sisältyy tiedostojärjestelmän tietorakenteiden eheyden tarkistus, yksityiskohdat vaihtelevat käyttöjärjestelmäkohtaisesti.

New Technology File System (NTFS) on Microsoftin jatkokehittämä tiedostojärjestelmä 90-luvulta. Nykyisin NTFS-tuen saa lisättyä Linux- ja Macintosh-

käyttöjärjestelmiin NTFS-3G ajurin avulla. NTFS:n toimintavarmuutta on lisätty FATiin verrattuna mm. kirjaavalla tiedostojärjestelmällä (journaling filesystem) joka säilyttää tiedostojen ja tiedostojärjestelmän eheyden paremmin keskeytysten sattuessa (esimerkiksi virtakatko, käyttöjärjestelmän kaatuminen). NTFS:n yksittäisen tiedoston maksimikoko on 16 TB ja partition maksimikoko 256 TB. NTFS:n eheystarkistus voidaan suorittaa osittain tiedostojärjestelmän ollessa käytössä, vakavampien virheiden korjaamiseksi tiedostojärjestelmä pitää poistaa käytöstä ja tarkistaa järjestelmän käynnistyksen yhteydessä.

Third Extended Filesystem (Ext3) on Linux-käyttöjärjestelmässä yleisesti käytetty tiedostojärjestelmä. Sen kehitys on tehty 2000-luvulla ja pohjautuu Ext2:een, lisäyksenä muutosten kirjaus (journaling). Tavanomaisella PC-tietokoneella tehtynä tiedoston maksimikoko on 2 TB ja partition maksimikoko 16 TB. Tuki Ext2-tiedostojärjestelmään voidaan lisätä Windows- ja Macintosh- käyttöjärjestelmiin useilla toteutuksilla, mm. Ext2 Filesystem Driverin avulla (Ext2FSD). Ext3-tiedostojärjestelmän eheystarkistukset voidaan tehdä vain kun tiedostojärjestelmä ei ole käytössä, esimerkiksi järjestelmän käynnistyksen yhteydessä tai erillisillä diagnostiikkatyökaluilla, kuten CD:ltä, USB-tikulta tai korpulta bootattavalla Linuxilla.

Zettabyte File System (ZFS) on Sun Microsystemsin kehittämä tiedostojärjestelmä Solaris-käyttöjärjestelmälleen, joka julkaistiin vuonna 2004. ZFS tukee useiden fyysisten levyjen yhdistämistä yhdeksi osioitavaksi virtuaalilevyksi, tiedon eheyden säilyttämistä RAID-tyylisesti tarkistussummin sekä tiedostojen pakkausta lennossa. Suurin osio- ja tiedostokoko ovat 16 EB. ZFS-tiedostojärjestelmäajureita on tehty FreeBSD:lle, MacOSX:lle ja Linuxille – joskin nämä ovat vielä jatkokehitysvaiheessa. ZFS:n eheystarkistukset tehdään tiedostojärjestelmän ollessa käytössä zpool scrub -komennolla. Oraclen ostettua Sunin, ZFS on siirtynyt Oraclen palvelutarjonnan joukkoon [7]. Tässä vertailtujen tiedostojärjestelmien erot on koottu taulukkoon 1.

Taulukko 1: Tiedostojärjestelmien vertailu

Tiedostojärjestelmä	**FAT32**	**NTFS**	**Ext3**	**ZFS**
Windows tukee	Kyllä	Kyllä	Ajurilla	Ei
Linux tukee	Kyllä	Ajurilla	Kyllä	Ajurilla
Mac tukee	Kyllä	Ajurilla	Ajurilla	Ajurilla
Solaris tukee	Kyllä	Ei	Ajurilla	Kyllä
Tiedostoraja	4 GB	16 TB	2 TB	16 EB
Partitioraja	8 TB	256 TB	16 TB	16 EB
Korjaus käytettäessä	Kyllä	Osittain	Ei	Kyllä
Virheentarkistustyökalu	chkdsk, fsck	chkdsk	fsck	zpool scrub

Network File System (NFS) on Sun Microsystemsin vuonna 1984 kehittämä ja RFC-standardoitu tapa jakaa tiedostojärjestelmiä verkon yli. Operaatiot ovat tasolla "luo tiedosto nimeltä xx", "lukitse tiedosto xx kirjoitettavaksi". [8, 9] Protokollan viimeisin versio 4.1 sai RFC-numeron tammikuussa 2010 [10]. Tiedostorajat ovat NFSv2:ssa 2 GB, NFSv3:sta eteenpäin 16 EB tai niin paljon kuin palvelimen tiedostojärjestelmä antaa myöten. Tiedostojen lukitseminen lukua tai kirjoitusta varten voi aiheuttaa ongelmia jos verkkoyhteys katkeilee tai koneet ovat muun virheen vuoksi tavoittamattomissa [11].

2.3 Verkonvalvonta

Tiedonsiirtoverkko on laitteiden keskinäisen viestinnän mahdollistava infrastruktuuri. Viestinnässä käytetään sovittuja protokollia ja käytäntöjä. Kiinteän verkon rakennuspalasia ovat valokuitu- sekä kuparikaapelit, radioliikenteessä sovitut taajuuskaistat ja -protokollat, suurien etäisyyksien siirroissa myös satelliitit sekä HF-radiot.

Liikenteen määrän valvominen kussakin linkissä auttaa mitoittamaan laitteiston kapasiteetiltaan sopivaksi ja mahdollisesti rakentamaan uusia linkkejä tiheästi liikennöivien osapuolien välille. Vikaantuessaan verkko on rakenteensa takia usean muuttujan ongelma. Koko tiedonsiirtopolun laitteiden täytyy toimia, jotta viesti välittyisi onnistuneesti. Siirtovirheiden suuri määrä voi johtua mm. viallisesta laitteistosta, vaurioituneesta verkkojohdosta, viallisesta liitoksesta (esimerkiksi pölyä valokuidun päässä) tai ympäristöstä (esimerkiksi toinen WLAN-tukiasema samalla taajuudella).

Jos verkossa on käytössä palomuureja, niistä on mahdollista saada pakettien luokittelun sivutuotteena liikennöintimääriä eri Internet-osoitteisiin. Maakohtainen erittely voi paljastaa palveluiden käyttäjäjakaumaa sekä haavoittuvuuksien etsijöitä ja mahdollisesti oman verkon saastuneita koneita (esimerkiksi runsasta sähköpostien lähetystä maihin joissa yrityksellä ei ole toimintaa). Tällaisia yhteenniputettuja tunnistetietoja voidaan vielä koota automaattisesti ja tarkastella ilman eri ilmoituksia. Tutkittaessa yksittäisten koneiden liikennöintiä ja paketteja tarvitaan lisälaitteiston lisäksi lain vaatimat ilmoitukset tietosuojavaltuutetulle sekä henkilöstölle (Sähköisen viestinnän tietosuojalaki HE 48/2008) [12].

Verkon valvontaan käytetään usein samaa valvottavaa verkkoa, joka on nurinkurista ongelmatilanteissa. Ratkaisuna tähän on rinnakkaisen verkon pystyttäminen josta on pääsy samoihin kriittisiin verkkolaitteisiin joita tuotantoverkko käyttää. Näin virhetilanteiden kestoja saadaan pienennettyä kun diagnoosi ja korjaus voidaan tehdä käymättä fyysisesti yhteyden jokaista verkkolaitetta läpi. Muita perus-

riippuvuuksia ovat sähkönsyöttö, toimintalämpötila ja -ympäristö (esimerkiksi liiallinen kosteus tai pöly). Nämä riippuvuudet pätevät myös muulle tietotekniikalle. Verkon valvontamenetelmiä käsitellään tarkemmin seuraavassa luvussa, jossa pohditaan kehitysvaihtoehtoja.

Jotta tyypillisessä toimistoverkossa olevat palvelut olisivat saavutettavissa, täytyy verkon peruspalveluiden olla toiminnassa. Näitä ovat mm. Domain Name System (DNS), Domain-tunnistautuminen (esimerkiksi Lightweight Directory Access Protocol – LDAP tai Active Directory – AD) sekä Dynamic Host Configuration Protocol (DHCP) [13, 14, 15, 16]. Verkko voi toimia ilmankin näitä pelkillä IP-osoitteilla, mutta silloin jokaiselle verkkolaitteelle pitää olla määritettynä käsin kiinteä osoite sekä tapa selvittää laitteiden IP:t joiden kanssa se liikennöi. DHCP tarjoaa automaattisesti määritetyt IP-osoitteet ja sen myötä sujuvammat siirtymät verkosta toiseen. DHCP-palvelimelta on saatavissa tiedoksi mm. vapaiden IP-osoitteiden määrä, jota kannattaa seurata jotta kaikille verkkoon kytkeytyville laitteille riittää osoitteita. Internet Protocol version 6 (IPv6):n käyttöönoton myötä osoitepula poistuu.

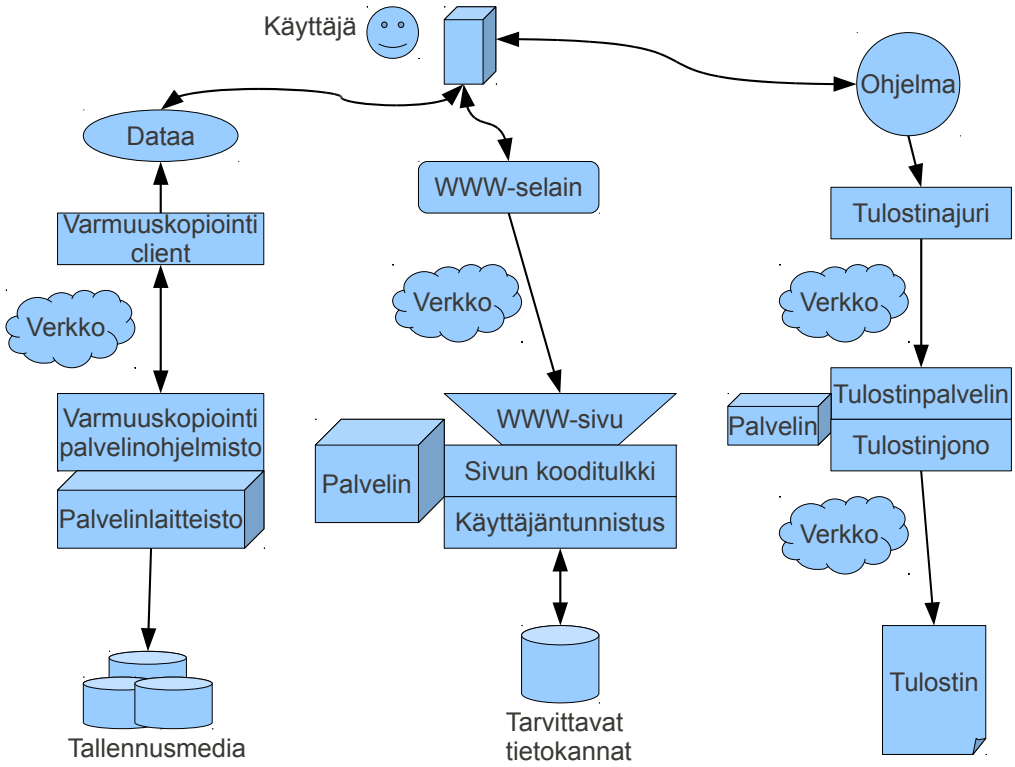
DNS-järjestelmä tarjoaa nimipalvelut ihmisille helpommin muistettavien nimien muuntamiseksi IP-osoitteiksi, esimerkiksi ”www.csc.fi”. Moni käytössä oleva järjestelmä luottaa DNS-nimiin joten DNS-palvelinten toiminta on yksi edellytys verkon toiminnalle. DNS-palvelimilta saadaan valvontadataa mm. tehtyjen DNS-kyselyiden määrästä ja DNS-tietojen voimassaoloajasta. Tunnistautumista hyödyntävissä palveluissa tunnistustiedon tarjoaja on tärkeässä asemassa järjestelmän toimimiseksi, joskin tarvetta voidaan lieventää paikallisella tunnistetietojen välimuistilla johon turvaudutaan yhteydenpuutteessa. Tunnistautumista tarjoavista LDAP- ja AD-palveluista saadaan valvontatietoa tunnistautuneista käyttäjistä sekä epäonnistuneista tunnistautumisyrityksistä.

2.4 Palvelut

Palvelut ovat resursseja joita käyttäjät hyödyntävät, kuten ohjelmistoja, rajapintoja, NAS- tai SAN- levyjä ja neuvontaa. Palveluiden toimivuus riippuu tyypillisesti palvelualustan kunnosta, mutta alustan virheetön toiminta ei ole tae palvelun moitteettomasta toimimisesta. Palvelun toiminnan tarkistamiseksi yksi parhaista tavoista on suorittaa testikäyttäjän oikeuksilla jokin tyypillinen toimenpide ja varmistaa sen onnistuminen, esimerkiksi sähköpostin osalta viestin perilletulo. Toiminnan tarkistajilla tulisi joko olla valtuudet ja keinot mahdollisten ongelmien korjaamiseksi, tai suora yhteys korjaajakykyiseen henkilöön. Päivystyksen kattavuus voi olla kolmitasoinen: järjestelmä toimii kokonaisuudessaan, järjestelmän osakomponentit

toimivat tai osakomponenttien toimintahistoria lähiajalta vastaa odotettua.

Kuvassa 1 on esitetty joidenkin organisaation sisäisesti tarjottavien palveluiden riippuvuuksia. Esimerkkeinä palveluista ovat varmuuskopiointi, tulostaminen ja WWW-pohjaiset palvelut. Ongelmatilanne missä tahansa ketjun osassa aiheuttaa palvelun toimimattomuuden. Seuraavaksi käydään läpi näiden palveluiden erikoispiirteitä.



Kuva 1: Tyypillisiä sisäisesti tarjottavia palveluita riippuvuuksineen

Varmuuskopiointi on varsin usein tarpeellinen palvelu, vaikka tiedonsäilytys olisikin kahdennettu. Palvelun tarkoitus on tarjota päivittäin tallennettuja arkistokopioita käytettäväksi jos alkuperäinen tietoväline hajoaa tai toimimisestaan huolimatta korruptoituu. Esimerkiksi kahdennettu levyjärjestelmä voi toimia täysin oikein siitä huolimatta että ohjelmistovirhe tyhjentää käyttäjän kotihakemiston. Tällöin varmuuskopioinnin toimivuus tulee viimeistään tarkistettua. Varmuuskopioinnista vastaavan henkilön tulee olla varmistanut jo ennen tiedonhävikkiä että varmuuskopiointi toimii, data on relevanttia ja palauttamismekanismi on kunnossa. Näitä asioita voidaan valvoa esimerkiksi varmistettujen datamäärien visualisoinneilla. Var-

muuskopiointi voi riippua esimerkiksi varmuuskopiointiohjelmiston ajantasaisuudesta, kopioiden tallennusjärjestelmän toimivuustilasta ja verkon saatavuudesta. Varmuuskopiointi on useimmiten organisaation sisäinen palvelu, vaikka on myös olemassa verkkopohjaisia varmuuskopiointipalveluita. Näissä tulee huolehtia erityisesti luottamuksellisen tiedon turvaamisesta joko sopimuksin tai salausalgoritmien avulla.

Tulostaminen on yksi harvoista palveluista joka tuottaa käsintuntuvia tuloksia. Samaisesta syystä, koska tulostamiseen liittyy mekaanista liikettä paperia käsitellessä, tulostimien vikaantumistiheys on suurempi kuin tietokoneiden. Tavanomainen ratkaisu tälle on ostaa muutama laadukkaampi tulostin ja jakaa ne palvelimen avulla kaikkien käyttäjien hyödynnettäväksi. Tulostimien käyttämisestä tällä tavoin muodostuu kohtuullisen pitkä riippuvuusketju, alkaen tulostavan ohjelman asetuksista, kulkien tulostinajureiden ja tulostinpalvelimen tekemien muotoilujen kautta tulostinjonoon ja käsiteltäväksi paperimuotoon. Edistyneemmät toiminnot kuten salasanalla vapauttavat tulosteet eivät ole vielä vakiintuneita. Tulostimia valitessa kannattaa myös huomioida tuleva käyttöympäristö: Applen työasemilta sekä Linux-koneilta tulostaminen onnistuu parhaiten postscript-komentokieltä tukeville tulostimille.

WWW-pohjaisten palveluiden käyttäminen on edullista siinä mielessä että käyttäjän koneelta ei vaadita muuta kuin toimiva WWW-selain ja verkkoyhteys. Näin palvelu on helpompi päivittää ajan tasalle ja tarjota saataville joustavammin erilaisille laitteistoille, muun muassa käyttöjärjestelmästä riippumatta. Riippumattomuuden varmistus tosin vaatii standardeissa pitäytymistä, mutta aihe on niin laaja ettei sitä tässä tarkemmin käsitellä. Palvelun saatavuus riippuu verkon toiminnan lisäksi muun muassa sivuston generoivan sovelluksen ajantasaisuudesta sekä kuormasta. Jos sivusto vaatii käyttäjiltä tunnistautumista, tunnistautumisjärjestelmän saatavuus on myös palvelun toiminnan edellytys.

2.5 Ylläpitoprosessi

Jotta ylläpito toimintana olisi hallittava ja arvioitava, sen yksittäiset toimet on eriteltävissä prosesseiksi. Ylläpidon tapauksessa prosessit tarkoittavat yleensä joukkoa vaiheita joita tietyn ongelman ratkaiseminen tarvitsee. Esimerkiksi viallisen osan vaihtamiseksi on suoritettava seuraavat vaiheet:

1. sammuta tietokone
2. irroita virransyöttö
3. avaa kotelo
4. irroita viallinen osa

5. asenna varaosa
6. sulje kotelo
7. palauta virransyöttö
8. käynnistä tietokone
9. testaa että varaosa toimii

Ylläpitoprosessien esittäminen vaiheittain eriteltynä mahdollistaa työtehtävien analysoinnin ja suoriutumisen paremman arvioinnin. Jokainen tehtävän suorittava työntekijä suorittaa työn samanlailla, jolloin suoritukset ovat vertailukelpoisia. Tiukasta vaiheistamisesta on eniten hyötyä uuden prosessin opetteluvaiheessa. Jatkuva jokaisesta vaiheesta raportointi voi kuitenkin syödä ylläpitäjän motivaatiota merkittävästi ”turhan byrokratian” pyörittäjänä, joten tehtävän raportoinnin määrä tulee pitää kohtuullisena. Raportoinnin puute ei estä yksityiskohtaisten tehtävämuistilistojen tekoa.

Information Technology Infrastructure Library (ITIL) on Iso-Britannian 1980-luvulta asti kehittämä prosessikehys tietoteknisten palvelujen tuotantoon. ITIL koostuu kirjoista, joihin on koottu aihepiireittäin parhaita käytäntöjä tietoteknisten palvelujen tarjoamisen vaiheista alkaen pystyttämisestä aina tukemiseen asti [17]. ITIL-aineisto on ryhmitelty kirjoiksi kolme kertaa vuosina 1989, 2000 ja 2007. ITIL on toiminut pohjana muille vastaaville standardeille. Tämän työn valvontaohjelmisto liittyy ITILv2:n osaan Service Support ja sen lukuun Problem Management, eli ongelmien ennaltaehkäisy. Nopeasti käyttöönotettavat parannukset tällä saralla ovat mittaustulosten keruu sekä jakaminen ja useimmiten toistuvien virheiden trendianalyysi. Ongelmanhallinnan tavoitteena on löytää virhetilanteiden perimmäiset syyt jotta niihin voidaan puuttua, erotuksena vikatilanteesta toipumiseen jossa tavoitteena on saada järjestelmä takaisin toimintaan mahdollisimman nopeasti.

ITIL käsittelee asioita prosessien näkökulmasta. Se pohjautuu ihmisen toiminnasta tehtyihin psykologisiin tutkimuksiin, joissa on selvitetty millaisia valintakriteereiden olisi oltava, jotta ne saisivat aikaan muutoksen käyttäytymisessä. Tilannekohtaiset suositukset sisältävät tarkistuslistoja näkökulmista jotka tulee ottaa huomioon prosessia toteuttaessa. Esimerkiksi ITILv3:n vastaus kysymykseen “Miten varmistaa että johtoportaan strategiat realisoituvat työntekijöiden toiminnaksi” tarjoaa huomioon otettaviksi näkökulmiksi proaktiivisen toiminnan, tulevien muutosten hyödyllisyydestä kertomisen ja kaikkien osapuolten mukaan ottaminen kehitystyöhön. [18]

2.6 Visualisointi

Informaatioteknologia mahdollistaa massiivisten datajoukkojen käsittelyn, minkä seurauksena on yhä hankalampi käsittää datan merkitystä tai edes erottaa datajoukosta olennainen osa. Käytännöllisin ratkaisu monimutkaisen datan käsittelyssä on esittää se graafisesti ihmiselle ymmärrettävässä muodossa, eli visualisoida se. Käytettävät menetelmät perustuvat ihmisen näköaistin ominaisuuksiin ja rajoituksiin, joten nämä tulee tiedostaa visualisointeja suunnitellessa.

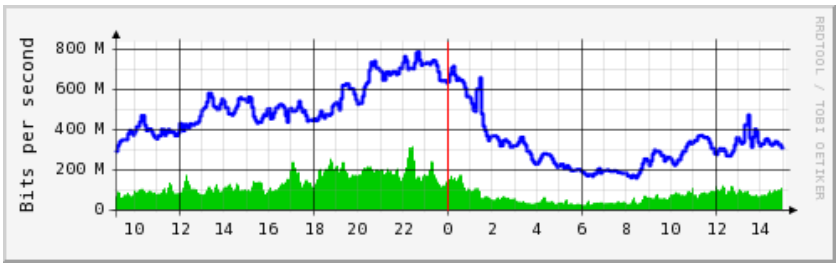
Edward Tufte esitti että graafisen esityksen tulisi muun muassa:[19]

- ensisijaisesti esittää tietoa,
- välttää tiedon vääristämistä,
- tehdä isoista tietomääristä koherentteja,
- kannustaa silmää vertailemaan eri osia tiedosta.
- paljastaa useita kerroksia tiedosta; yleisnäkymästä yksityiskohtiin.

Näiden päämäärien tarkasteluun Tufte kehitti apuvälineitä, kuten tietomuste-suhde, joka lasketaan visualisoinnissa datan esittämiseen käytetyn ”musteen” suhteesta muuhun visualisoinnissa käytettyyn musteeseen, ja valehtelukerroin, joka lasketaan suureiden esittämiseen käytettyjen visuaalisten elementtien koon suhteesta suureiden arvoihin.

Yleisimmät visualisointimenetelmät jotka soveltuvat automatisoituihin järjestelmiin ovat aikasarjat, tietokartat ja suhdegraafit. Aikasarjat ovat näistä ehdottomasti yleisimpiä. Aikasarjalla tarkoitetaan mitä tahansa kuvaajaa, jossa esitetään ajallisesti peräkkäisiä arvoja. Esimerkkinä aikasarjoista on kuvassa 2 esitetty Otaniemen teekkarikylän (Trinet) ulkoyhteyden kuormitus vuorokauden aikana. Vaaka-akselina on siis viimeisen vuorokauden kellonajat ja pystyakselilla on hetkittäiset mitatut liikennemäärät, vihreällä saapuva liikenne ja sinisellä lähtevä liikenne. Tietokartat esittävät arvoja sijoitettuna kartalle, eli kaksiulotteiselle pinnalle. Pinta voi olla sovitettu karttapohjalle tai vain sommiteltu esittämään halutun tiedon suhteet mittakaavasta piittaamatta. Suhdegraafit esittävät yleisesti kahden suureen suhdetta toisiinsa. Aikasarja on siis suhdegraafien alijoukko, jossa toinen suure on aika.[19]

Suuruusluokkien visuaalisessa hahmottamisessa kannattaa harkita datan lineaarisuutta - data joka on suoraan lineaarisessa suhteessa keskenään on luontaisesti esitettävissä pylväsdiagrammeilla. Toisessa potenssissa kasvavat datasuhteet voivat hyötyä ympyröiden vertailusta, koska ympyröiden pinta-ala kasvaa myös toisessa



Kuva 2: Trinet FUNET/Espoo yhteyden graafi.[20]

potenssissa, esimerkiksi verkostoituneiden ihmisten kontaktien määrät. Kolmannen potenssin suhteille luontainen vastine ovat puolestaan tilavuudeltaan samassa suhteessa kasvavat pallot tai kolmiulotteiset suorakulmiot.

2.6.1 Värien käyttö

Yksi erinomainen visualisointityöväline on värien käyttö. Värit perustuvat näkyvän valon spektrin tehojakaumaan. Ihmisen näköaisti on kehittynyt hyvin tarkaksi erottamaan tiettyjä ominaisuuksia väreistä. Visualisoinnin kannalta olennaisinta on käytännölliset tavat käyttää värejä erottamaan asioita toisistaan tai esittää arvoskaaloja siten että ne voi nähdä yhdellä silmäyksellä.[21]

Värien käyttöä erotteluun, eli eri asioiden merkitsemiseen, rajoittaa erilliseksi tunnistettavien värien määrä. Tunnistettavuuden lisäksi käytettävissä olevien värien määrää rajoittavat kuvan kontrasti eli kuvan kirkkauserot, mahdollinen katsojan värisokeus ja yleiset käytännöt värien käytössä (esimerkiksi vihreä on normaalitila, punainen vikatila). Colin Ware suosittelee työssään[21] kahden kuuden värin ryhmän käyttöä datan merkitsemisessä. Värit on esitelty kuvassa 3. Näistä kuusi vasemmanpuoleista on ns. päävärejä ja kuusi oikeanpuolimmaista ns. välivärejä. Visualisointeja tehdessä tulisi ensisijaisesti käyttää päävärejä, ja tukeutua väliväreihin vasta kun päävärit on käytetty. Edellä mainittua suurempaa värimäärää ei suositella käytettäväksi, koska silmän kyky erottaa värit toisistaan vaarantuu. Tällöin vaarana on että visualisoinnin ymmärrettävyys heikkenee.

Toinen havainnollinen tapa värien käyttöön on käyttää väriskaaloja tietokarttojen esittämiseen. Tietokartan avulla voidaan esittää joko diskreettejä tai jatkuvia arvoja sijoitettuna kartalle. Tällöin visualisoinnista voidaan erottaa yhtäaikaisesti sekä sijainti että arvo. Yleisimmät tavat arvojen esittämiseen on nimetä tietyille väreille tietty arvo, esimerkiksi punainen tarkoittaa vikaa, vihreä ehjää, tai käyttää väriliukua, joko kirkkauden tai värisävyn yli, suoran numeerisen arvovälin esittämiseen. Kirkkauden käyttö on yksinkertaisin, mutta myös huonoin tapa, sillä ihmisen

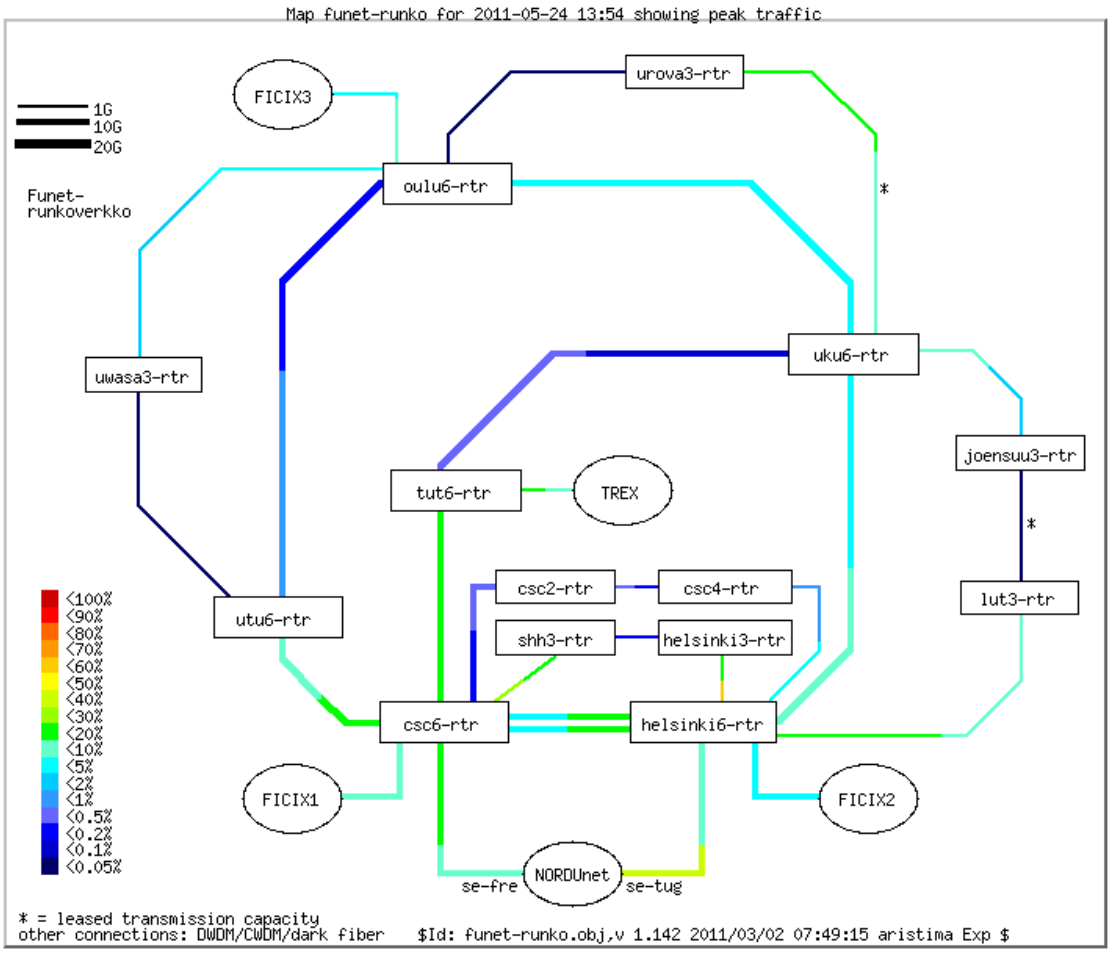
Kuva 3: Kaksitoista merkintöihin soveltuvaa väriä.[21]

näköaisti on hyvin kontrastiriippuvainen ja kirkkausarvojen tulkinta siis riippuu tarkasteltavan alueen vieressä olevista alueista. Esimerkkinä tällaisesta visualisoinnista tietoliikenneympäristössä on kuvassa 4 niin sanottu ”verkkosääkartta” (engl. network weather map). Kuvassa nähdään FUNET-runkoverkon yhteydet, niiden kapasiteetit viivanleveydellä ja niiden kuormitusasteet väreillä esitettynä.[21]

2.6.2 Visuaalinen huomio

Ihmisaivot käsittelevät silmän välittämää informaatiota purskeina. Prosessi on rinnakkainen ja koostuu visuaalisten ominaisuuksien poiminnasta ja kokoamisesta. Visuaalisen raakadatan määrä on aisteista suurin, kuulon tullessa seuraavana. Aivoilla kumminkin on rajoituksia ja esimerkiksi liian suuri määrä ominaisuuksia yhdellä näkemällä aiheuttaa ns. tunnelinäön tiedolle; aivot eivät pysty prosessoimaan kaikkea, joten effektiivisesti aistitaan vain hyvin pieni osa kokonaiskuvasta. Tätä prosessia auttamassa on aivojen ominaisuus jota kutsutaan esihuomiolliseksi käsittelyksi (engl. preattentive processing), jossa tietyt visuaaliset ominaisuudet ”hyppäävät esiin” kuvasta, ennen kuin kuva on kokonaan käsitelty. Tämä on hyödyllistä koska sopivalla suunnittelulla on mahdollista kiinnittää katsojan huomio välittömästi tärkeään kohtaan kuvassa, tarvitsematta peittää muuta dataa.[21]

Ominaisuudet jotka havaitaan esihuomiollisessa käsittelyssä voidaan jakaa neljään ryhmään: muoto, väri, liike ja sijainti. Ominaisuuksia on esitelty kuvassa 5. Muodossa tunnistettavia ominaisuuksia ovat muun muassa asento, koko, kaarevuus, ryhmittely ja terävyys. Värissä tunnistettavia ominaisuuksia ovat sävy ja kirkkaus. Liikkeessä tunnistettavia ovat vilkkuminen ja liikkeen suunta. Sijainnissa tunnistettavia ominaisuuksia ovat 2D-sijainti, stereoskooppinen syvyys ja varjostuksen antama muoto.

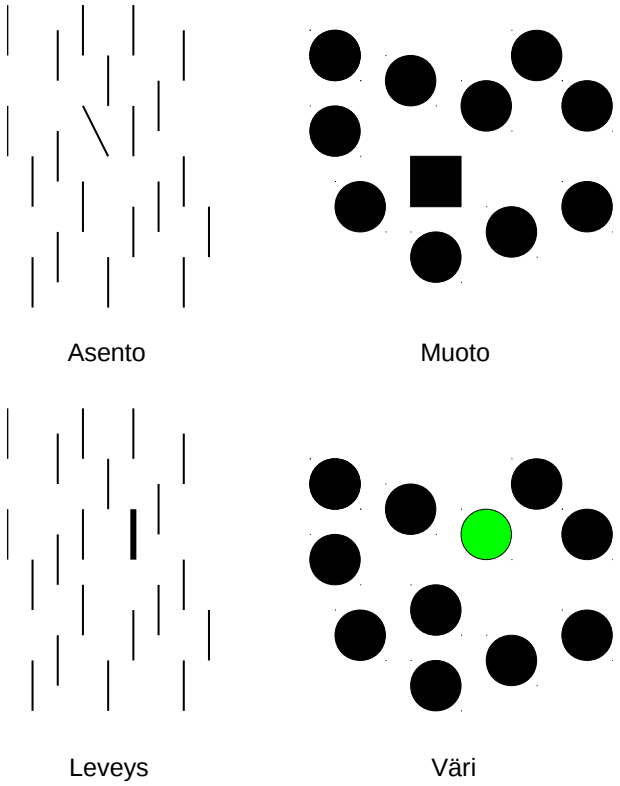


Kuva 4: FUNET-runkoverkon verkkosääkartta.[22]

Tiedon visualisoinnissa tulee siis harkita tarkasti miten suureet esittää. Visualisointien tulee olla korrekteja ja havainnollisia. Korrektius on ehdottoman tärkeä, jotta visualisointia voi pitää luotettavana, siten käyttökelpoisena. Havainnollisuuden takaamiseen on monia keinoja, jotka perustuvat pääosin esitettävän tiedon valikointiin ja esitystavan valintaan. Esitystavalla voidaan korostaa tiettyjä osia tiedosta jotka koetaan tärkeämmiksi, esimerkiksi kriittisen raja-arvon ylittävät hälytystilanteet.

2.7 Yhteenveto

Tietotekniset palvelut ovat yleisesti ottaen kokonaisuuksia, jotka rakentuvat monista komponenteista, lähtien fyysisistä osista, jatkaen loogisiin toimintakäytäntöihin ja päätyen ylläpitoprosesseihin. Ihmispsykologiakin astuu prosessien myötä kuvaan mukaan. Olemme tässä luvussa osoittaneet mitä hyötyä on eri osaratkaisujen val-



Kuva 5: Esihuomiollisia visuaalisia ominaisuuksia

vonnasta, ennen kaikkea jotta ongelmiin voidaan puuttua ennaltaehkäisevästi.

Ratkaisujen paremmuutta arvioidessa voidaan painottaa eri tekijöitä riippuen mitä ratkaisulla halutaan optimoida. Vastuunjakoa ratkaisun toimivuudesta saa aikaan jos tekniikalle on saatavissa kaupallista tukea, joka pätee niin suljetuille kuin avoimille ohjelmistoille. Jos ratkaisu on tarkoitus ottaa käyttöön useassa kohteessa, avoimia ohjelmistoja suosimalla säästää lisenssimaksuissa. Samoin jos ratkaisu vaatii muokkausta omiin tarpeisiin, avoimien ohjelmistojen osalta tarvitaan oma tai ulkoinen koodaaja joka osaa käytetyn ohjelmointikielen ja perehtyy ohjelmistoon. Kaupallisten ohjelmistojen osalta muutospyynnöt tehdään ohjelman tuottajalle, ja muutosten laajuus sekä hinta ovat neuvottelukysymyksiä.

Kaikkien uusien tekniikoiden käyttöönottoon liittyy koulutusta, jonka voi tehdä työntekijöiden itseopiskeluna, sisäisen koulutuksen avulla, maksullisilla kursseilla tai rekrytoimalla uuden asiaan perehtyneen työntekijän. Jos tekniikan on tarkoitus integroitua muiden järjestelmien kanssa yhteistoimintaan, standardoidut rajapinnat ovat tärkeyslistan kärkipäässä. Yleisemmin käytössä olevat tekniikat ovat massatuotantokustannuksiltaan edullisempia, tarjoajia voi kilpailuttaa ja yhden tarjoajan poistuminen ei lopeta tekniikan tukea.

3 Nykytila-analyysi ja kehitysvaihtoehdot

Informaatiotulvassa tulee entistä tarkemmin valittua mihin asioihin perehtyy, ts. mistä minulle voisi olla hyötyä. Opettelu on kuitenkin työtä ja ylimääräistä työtä koitetaan välttää jos tarjolla on tutumpia vaihtoehtoja. Tietääkseen tämän ratkaisun soveltuvuudesta omaan käyttöönsä, on hyödyllistä perehtyä alkutilanteeseen. Mikä on ongelma jota ratkaistaan, ja millä reunaehdoilla toteutusta lähdetään hakemaan? Esimerkkinä tästä voisi olla kännyköiden Internet-puheluominaisuus. Lähteekö keskiverto puhelimen ostaja perehtymään satunnaisen kirjainlyhenteen toimintaan, tarvittaviin asetuksiin ja käyttötapamuutoksiin pelkän otsikon perusteella? Vai vasta sitten kun hän saa tietää joltakulta minkä ongelman ominaisuus ratkaisee hänen tapauksessaan (joka siis on matalahintaisemmat puhelut tietoverkkojen kautta, erityisesti ulkomaille *jos* vastapuoli käyttää myös samanlaista päätettä). Onko oikea vaihtoehto SIP, MMS, VoIP, VPN vai joku muu kirjainlyhenne jonka merkitystä ei selitetä suoraan esiintymisen asiayhteydessä?

Tässä luvussa käsitellään aikasemmin olemassa olleita toteutuksia valvontaan ja visualisointiin liittyen ja arvioidaan mahdollisia kehityspolkuja. Nykyisten ratkaisujen määrittämät reunaehdot käsitellään, jotta seuraavassa luvussa esitettävä ratkaisumalli saadaan perusteltua.

3.1 Tieteen tietotekniikan keskus CSC

CSC - Tieteen tietotekniikan keskus Oy on Suomen valtion pääosin rahoittama, opetus- ja kulttuuriministeriön hallinnoima IT-keskus. CSC on voittoa tavoittelematon osakeyhtiö jonka tehtävänä on tuottaa palveluita Suomen korkeakoulujen, tutkimuslaitosten ja yritysten tueksi. Näitä palveluita ovat muun muassa mallinnus-, laskenta-, verkko- ja tietopalvelut. [23]

CSC ylläpitää Suomen korkeakoulut ja ammattikorkeakoulut laajasti kattavaa FUNET (Finnish University and Research Network) tietoliikenneverkkoa, sekä tarjoaa lukuisia teknisiä sekä käytännönläheisiä palveluita. Palveluista esimerkkeinä mainittakoon ftp.funet.fi ftp-tiedostopalvelin jonka kautta Linux aikanaan levisi maailmalle [24], runsasliikenteinen Usenet news-juuripalvelin sekä kansallinen digitaalinen radio- ja TV-arkisto. Palveluita ovat myös Linnea-kirjastojen varausjärjestelmä sekä tutkijan käyttöliittymä, joka on WWW-pohjainen valikko laskentapalveluiden hyödyntämiseen tutkimuksen osana.

Tämän työn järjestelmä on tehty CSC:n toimeksiannosta case-tapauksena valvontadatajärjestelmän pystyttämisestä sekä käyttöönotosta. Lopputuloksena saatu

valvonnan visualisointikone jää yrityksen käyttöön ja jatkokehitettäväksi muita visualisointitarpeita silmälläpitäen.

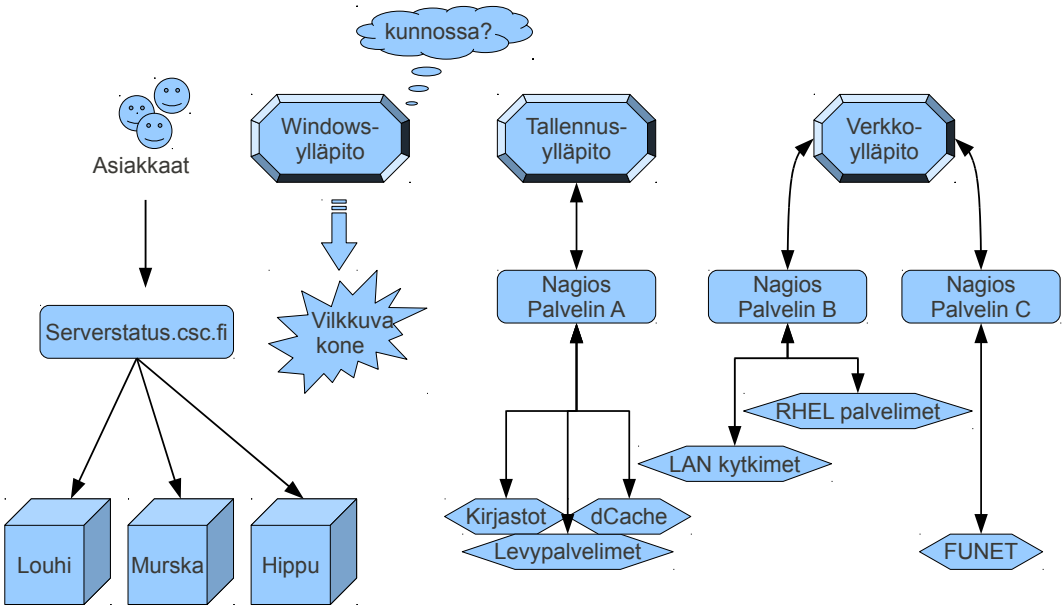
CSC:n tapauksessa valvottavia koneita ja palveluita on useissa verkoissa, joiden välillä on palomuureja tai ei laisinkaan suoraan muodostettavissa olevaa yhteyttä. Valvontatyökaluja on käytössä useita erilaisia – valmistajien tarjoamia mittaustyökaluja, itse koodattuja komentorivisarjoja ja ennakkovaroituksia tarjoavia mittausohjelmistoja kuten Nagios. Dataa kerätään tai pyydettäessä näytetään eri palvelimilta jotka sijaitsevat omissa verkoissaan CSC:llä. Hälytyksistä lähetetään mahdollisuuksien mukaan sähköpostia vastuulliselle ylläpitotunnukselle tai henkilölle. Talotekniikan hälytyksistä lähtee lisäksi tekstiviestejä oman GSM-antennin, GSM-modeemin, liittymän ja hälytyksiä hoitavan tietokoneen kautta.

Valvonta hoidetaan osittain proaktiivisesti, osittain reaktiivisesti. Päivystäviä ryhmiä on CSC:llä useita ja valvonnan käytännöt vaihtelevat ryhmien välillä. Osa ryhmistä reagoi ongelmiin sitä mukaa kun asiakkaat niistä ilmoittavat, priorisoiden työtä eniten haittaavien ongelmien korjauksen ensimmäiseksi. Osalle ryhmistä on kasattu verkkosivunäkymiä valvottavista kohteista, joita päivystäjäksi nimetty ryhmäläinen tutkii esimerkiksi tunnin välein päivittäin. Iltaisin ja viikonloppuisin päivystys on ulkoistettu yhteistyöyritykselle, joka käy tutkimassa sovitut näkymät kolmen tunnin välein ja hälyttää poikkeamien sattuessa CSC:n asiantuntijan korjaamaan ongelmaa.

Kuvassa 6 on esitetty valvontatyökalut jotka olivat käytössä työtä aloittaessa. Kuvassa alimpana ovat valvottavat resurssit: vasemmassa laidassa superlaskentakoneiden kuorma, keskellä tiedonvarastointiin liittyvät palvelut, oikealla verkon toimivuuteen liittyvät palvelut. Keskimmäisellä tasolla ovat valvontadatan esitysmuodot ja datan kerääjät, ylimpänä ovat datan vastaanottajat ja niihin reagoijat.

CSC:llä on palveluvelvoitteita tarjoamilleen palveluille, josta johtuen tiukempien velvoitteiden palveluita valvotaan tarkemmin ja komponenteille järjestetään redundanssia kahdennuksen ja varmuuskopioinnin muodossa. Service Level Agreement (SLA) on velvoitteiden määrittelyssä yleisesti käytettävä sopimustyyppi, jota voidaan käyttää sekä organisaation sisäisten ryhmien välillä että organisaatioiden välillä. Sovittaviin asioihin kuuluvat tyypillisesti vasteajat ilmeneviin vikoihin, kommunikointikanavat ja palvelun tavoitettavuustaso vuodessa (kuten 99,9%).

Olemassa olevien tiedonkeruujärjestelmien ohjelmistot päivittyvät eri tahtiin. Lähinnä windows-alustalla toimiva sähkönkulutusmittausjärjestelmä ei ole päivittynyt julkaisemisensa jälkeen, joten suurella todennäköisyydellä sen protokollapinoissa on paikkaamattomia ohjelmistoreikiä. Jos tätä haluttaisiin valvoa tilakysely-



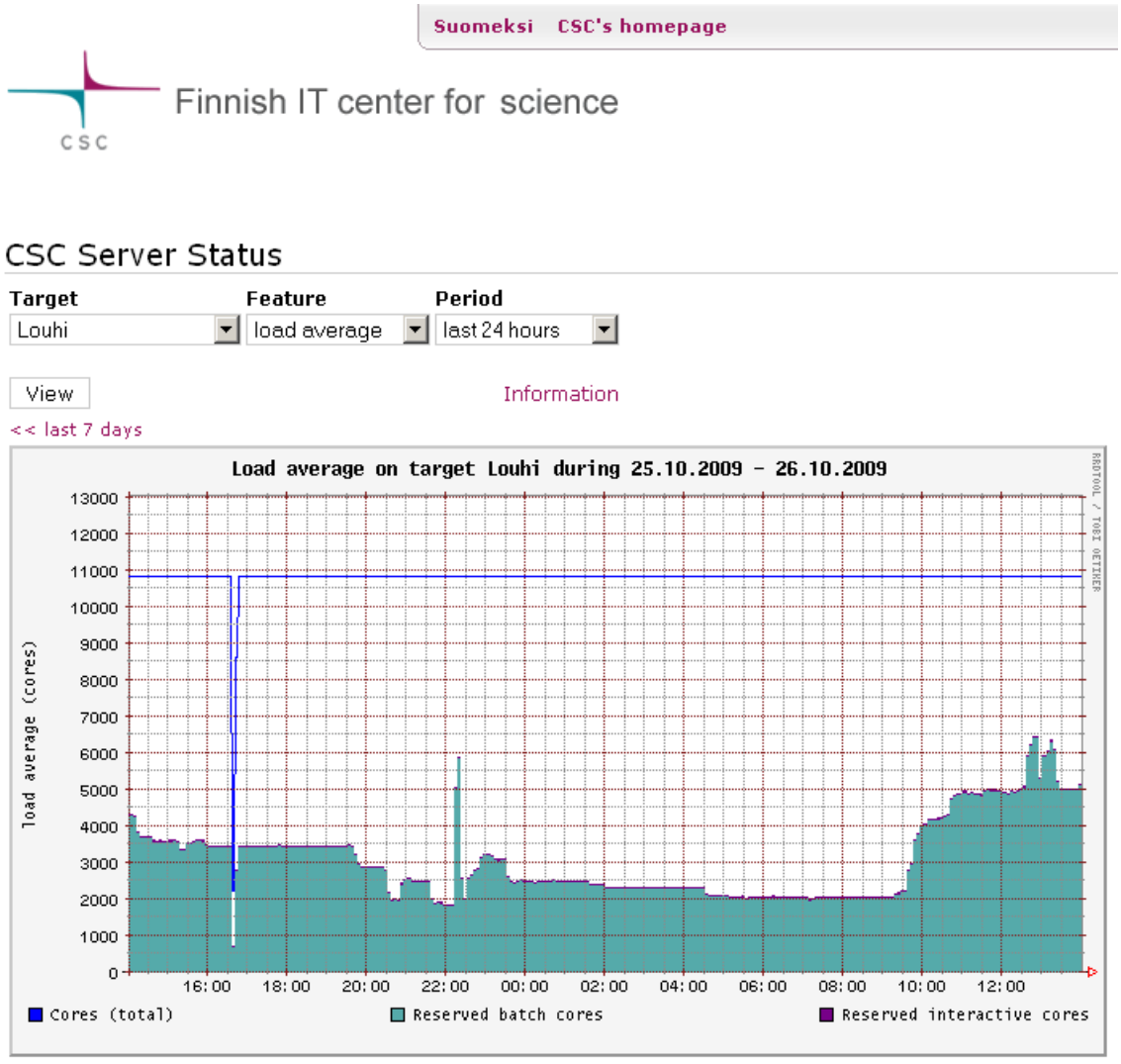
Kuva 6: Alkutilanne

jä tekevällä järjestelmällä, pitäisi palomuureista avata portteja jotka voisivat altistaa haavoittuvia palveluita verkkohyökkäyksille. Toinen vaihtoehto on ajastaa sähkönkulutusmittauksia tekevästä koneesta datansiirtoja ulkoiseen järjestelmään jolloin yhteyksiä otettaisiin ainoastaan suojatusta verkosta ulospäin.

Nykyisellään CSC:llä on käytössä serverstatus.csc.fi palvelu, josta asiakkaat voivat tarkistaa superkoneiden kuormitustason päivä- viikko- kuukausi- ja vuositasolla. Palvelussa näkyvät CSC:n kolme superkonetta: louhi, murska ja hippu (CPU-ytimien määrät vastaavasti 10864, 2176 ja 64). Graafiin piirretään mitatut kuormat halutulta ajanjaksolta, ja graafiin lisätään trendiviiva osoittamaan koneessa olevien CPU-ytimien määrää. Palvelu on CSC:llä koodattu ja käyttää hyväkseen PERL-skriptejä, SSH-tiedonsiirtoa sekä PHP-ohjelmointikieltä nettisivun luomiseksi.

Mittaustietokannat tallennetaan RRD-tiedostoihin jotka pysyvät saman kokoisina pitkillä ajanjaksoilla sekä karkeistavat mittapisteitä tiedon ollessa yli kuukauden tai vuoden vanhaa. Serverstatus.csc.fi -palvelu on julkisesti Internetissä saatavilla ilman kirjautumista. Kuva 7 esittää serverstatus-palvelun tilaa projektin alkupuolella. Kuvasta on rajattu pois alempana oleva teksti graafin tulkitsemisesta, jossa kerrotaan mistä tunnusluvut on kerätty (esimerkiksi load average tai varattujen ytimien määrä). Samoin selitetään trendiviivan merkitys koneen fyysisten ytimien määrä-

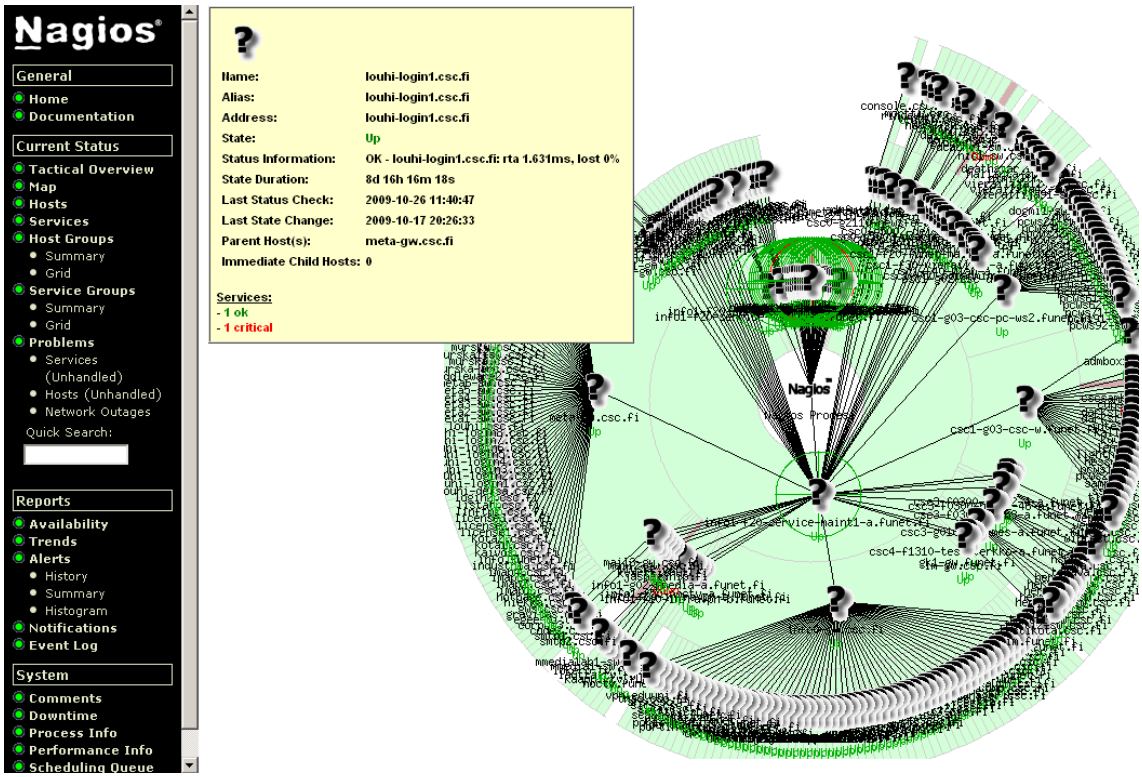
nä. Serverstatus-palvelu on tarkoitus siirtää sellaisenaan uudelle valvontadatan keruupalvelimelle toimimaan, jotta sama palveluosoite toimii jatkossakin ja edellinen palvelin saadaan kierrätettyä muuhun käyttöön.



Kuva 7: Serverstatus.csc.fi palvelu näyttää laskentaytimien kuormitushistorian

Käytössä on myös useita Nagios-palvelimia, jotka hakevat tai vastaanottavat verkon välityksellä tietoja valvomistaan koneista. Koska mittausajankohtien väli on pieni (<5min) ja kohteiden määrä suuri (>400), on valvontatehtäviä hajautettu myös kuormasyistä useammalle palvelimelle. Valvontapalvelimet ovat myös eri verkoissa valvomassa omia kohteitaan, koska esimerkiksi Backup-verkkoon ei ole palomuureista sallittu ulkopuolisia yhteydenottoja. Kuvassa 8 on näkymä yhden Nagios-palvelimen valvomien laitteiden määrästä.

Valvonnan piirissä on lähinnä Linux- ja Unix-palvelimia. Windows-palvelimet ei-



Kuva 8: Verkonvalvontaan keskittyvän Nagios-palvelimen valvoma konekatras

vät alkutilanteessa kuuluneet valvonnan piiriin, joskin virtualisoiduista palvelimista on nähtävissä virtualisoinnin ohjauskonsolilta tietoja koneen muistin ja prosessorinkulutuksesta. Käytetty virtualisointialusta on VMWare ESX server.

Kutakin Nagios-palvelinta valvovat sen pystyttäneen ryhmän ylläpitäjät. Kaikissa ryhmissä on useampia henkilöitä ja kiertävä päivystysvastuu joten tiedossa on kenen tulisi olla CSC:llä paikalla ja tilanteesta selvillä.

CSC:llä on myös koneita joiden valvomista ei ole katsottu olennaiseksi. Näiden koneiden osalta vikojen havaitseminen on ollut sattumanvaraista. Jos joku ylläpitäjä on käynyt konesalissa ja huomannut koneen vilkuttavan hälytysvaloja, on viestiä laitettu eteenpäin vastuulliselle ryhmälle mikäli hän on katsonut sen tarpeelliseksi. Toinen tapa huomata virheitä on ollut palvelimen tai työaseman toimimattomuus, jonka jälkeen syytä on lähdetty selvittelemään.

3.2 Valvontavaihtoehdot

Reaktiivisessa valvontamallissa asiakkaat ilmoittavat ongelmista kun niitä syntyy. Ilmoitukset ovat tyypillisesti muotoa palvelu ei toimi, koneeseen ei saada yhteyttä, levy on rikki, levy on täynnä... Reaktiivinen valvonta on hyvin usein käytetty val-

vontatapa. Reaktiivisen valvonnan SWOT-analyysi on esitetty kaaviossa 2. Reaktiivinen valvonta ei vaadi erityisesti lisäresursseja ja minimoi ajan joka käytetään muuhun kuin varsinaisten ongelmien korjaamiseen. Haittapuolena ongelmat voivat paisua hankalasti korjattaviksi jolloin palvelukatkot venyvät pitkiksi sekä ennakoimattomiksi.

Taulukko 2: Reaktiivisen valvonnan SWOT-kaavio

Hyvää	**Huonoa**
• Minimoi valvontaan kulutetun ajan, koska se on täysin ulkoistettu • Työaika tulee käytettyä tehokkaasti vain ongelmien korjaamiseen • Ei tarvitse pystyttää yhtään ylimääräistä infrastruktuuria tuotantokoneiden lisäksi	• Huoltokatkot ovat pitkiä • Redundanttien järjestelmien rakentaminen lähinnä viivyttää ongelmien ilmenemistä, ei estä niitä
Mahdollisuudet	**Uhat**
• Yksittäisten komponenttien elinkaari on pidempi, sillä niitä käytetään niin pitkään kuin mahdollista	• Virheet voivat kasautua jolloin niiden korjaaminen on vaikeaa tai mahdotonta • Asiakastyytyväisyys laskee

Päivystävässä valvontamallissa sovitaan joukko ylläpitäjiä jotka vastuuvuorollaan tarkistavat koneiden toiminnan ja tekevät tarvittaessa korjaukset. Päivystävän valvonnan SWOT-analyysi on esitetty taulukossa 3. Päivystävän valvonnan etuna on erityisesti päivystäjien asiantuntemus sekä kyky reagoida yllättäviinkin ongelmiin sekä tilanteisiin jotka eivät välttämättä näy sähköisesti mitenkään (kuten vaikkapa kasvanut pölyn määrä laitteistossa). Valvontamallin haittapuolena on henkilöresurssien riittävyys: jos valvottavien laitteiden määrä kasvaa satoihin ylläpitäjää kohden, kiireessä tehty valvonta voi rutinoitua ja ongelmia voi alkaa jäädä huomaamatta, vaikkapa vuorossa olevan päivystäjän väsymyksestä johtuen. Asiantuntevat päivystäjät ovat myös arvonsa tuntevaa työvoimaa, jota ei ole yllin kyllin tarjolla.

Osittain automatisoitu valvonta tehdään koneavusteisesti, mikä suodattaa näkymiä valvottavien kohteiden tilasta päivystäjille. Osittain automatisoidun valvonnan SWOT-analyysi löytyy taulukosta 4. Näin rutiinitarkastukset saadaan tehtyä varmasti ja riittävän usein jotta niistä voidaan jalostaa vaikkapa trendianalyyse-

Taulukko 3: Päivystävän valvonnan SWOT-kaavio

Hyvää	**Huonoa**
• Ei tarvitse ylimääräistä infrastruktuuria • Virheet eivät ehdi kasaantua • Huoltokatkoja on useammin mutta lyhyempinä	• Sitoo paljon henkilöresursseja • Ei skaalaudu sadoille tai tuhansille koneille vähentämättä valvottavien asioiden määrää
Mahdollisuudet	**Uhat**
• Virheiden havaitsemistarkkuus ja korjausvasteaika ovat korkeat, riippuen henkilön koulutuksesta	• Tarkistukset tehdään pintapuolisesti ja jotain jää huomaamatta

jä. Automatiikan pystyttäminen vaatii asiantuntemusta sekä pystytysvaiheessa että käyttövaiheessa. Samoin käyttövaiheessa päivystäjän on osattava tarkistaa että kerätty data on loogista ja todenmukaista. Yksinkertaisemmat korjaukset voidaan halutessa jättää automatiikan huoleksi, mutta täysautomaattista valvontaa ei ole tässä yhteydessä harkittu. Automatiikkaa lisättäessä mahdollisten virhetilanteiden määrä kasvaa niin suureksi että koodattavaa riittää liikaa, eikä sittenkään päästä resurssitehokkuudessa samaan kuin vastaavan lisäylläpitäjän kouluttamisella.

Nykyisessä tilanteessa hyödynnetään kaikkia kolmea vaihtoehtoa ryhmien kesken. Tavoitteeksi otettiin vähintään päivystävän valvonnan käyttöönotto kaikilla ylläpidon osa-alueilla.

Täysin automaattinen valvonta on jätetty vertailusta pois, koska kaikkien mahdollisten virhetilanteiden tunnistaminen sekä korjaaminen vaatisi niin paljon työtä, että kustannus kasvaa suuremmaksi kuin koulutettujen asiantuntijoiden palkkaaminen. Asiantuntijoiden huomion ja työtehon suuntaamiseksi merkityksellisiin ongelmiin tarvitaan relevanttia tietoa sekä sopiva sekoitus valtaa, vastuuta ja raportointivelvollisuutta.

Sosiologit ovat selvittäneet yhdeksi ihmisen käytöksen muuttamisen malliksi neliosaisen mallin. Ensimmäisessä vaiheessa kerätään yksilöityä dataa. Toisessa vaiheessa siitä poimitaan merkityksellinen aines ja esitetään se yksilölle relevantissa yhteydessä. Kolmannessa vaiheessa ehdotetaan vaihtoehtoja miten datan perusteella voidaan joko jatkaa samaan malliin tai tavoitella muutosta johonkin suuntaan. Neljännessa vaiheessa toimitaan, ja toiminnan tuloksista kerätään lisää dataa jotta

Taulukko 4: Osittain automatisoidun valvonnan SWOT-kaavio

Hyvää	**Huonoa**
• Skaalautuu suurillekin kokonaisuuksille • Mahdollistaa yhdenmukaisen virheiden havaitsemisen ja ennakoinnin • Ei sido paljoa henkilökuntaa päivystykseen	• Ylimääräinen valvontainrastruktuuri pitää pystyttää • Valvonnan toimintakuntoon saattaminen on aluksi työlästä
Mahdollisuudet	**Uhat**
• Päätelmiä voidaan tehdä myös mittausten aikasarjoista ja trendeistä	• Vaatii edelleen päivystyksen, tuloksista ei ole hyötyä jos niitä ei hyödynnetä

kierto voi alkaa taas alusta. [25]

Visualisointipalvelun tapauksessa tämä tarkoittaa tehtäväkohtaisesti koostettuja näkymiä, trendianalyysejä sekä toimenpide-ehdotuksia. Näiden perustella päivystäjät voivat korjata pullonkauloja ja mitoittaa kapasiteettia tarvetta vastaavaksi. Kuvassa 9 on esitetty yksi käytössä oleva näkymä päivystäjälle, johon tulee ongelmien ilmetessä toimenpide-ehdotuksia tarkempaa diagnosointia ja korjaamista varten.

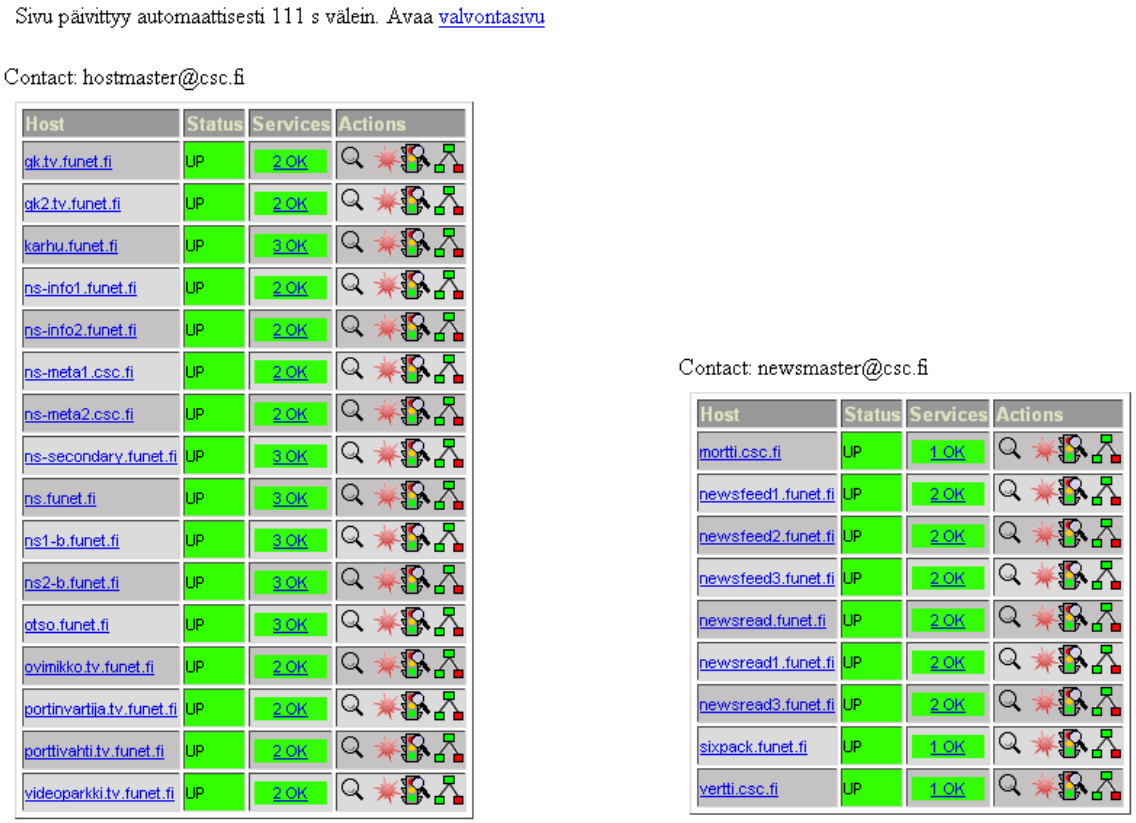
Seuraavaksi käydään läpi yksityiskohdat valvonnan teknisistä toteutustavoista.

3.2.1 Automatisoidut tiedon keräystavat

Mittausdataa voidaan hankkia joko ulkoisista antureista tai koneen sisäisistä prosesseista. Kun mittadataa on saatavilla, sen hyödyntäminen voi vaatia siirtämistä keskuskoneelle joka kokoaa yleisnäkymää aihepiiristä. Datan siirtoon on kolme perustapaa, PUSH, PULL sekä agenttimalli. Malleissa oletetaan dataa tuottavan koneen olevan lähtöpiste josta käsin viestintää tarkastellaan.

Proaktiivinen PUSH-tapa tarkoittaa että datan tuottanut kone lähettää itse siitä tiedoksiannon verkkoon, joko datan tuottamisen yhteydessä tai ajastetusti. Kone siis toisin sanoen lähettää mittausdataa tarjolle, kuluttaen samalla ennakoitavan määrän verkkokapasiteettia lähetysvälein. Syslog on esimerkki PUSH-tyyppisestä palvelusta.

Reaktiivinen PULL-tapa tarkoittaa että mittausdatan siirtoon mittauksen tehneeltä laitteelta tarvitaan ulkoinen yhteydenotto siirtävältä taholta. Mittaus voi olla joko ennalta tehty ja varastoitu tai suoritetaan pyynnön yhteydessä. Esimerk-



Kuva 9: Päivystäjänäkymä palveluiden saatavuuteen, yksinkertaistettuna toimii/ei toimi tasolle

kejä tästä on reitittimen kuormitus, josta saa lukeman pyydettäessä, mutta reititin ei sitä itse mainosta tasavälein verkkoon. Suurin osa SNMP:n mittauksista toimii PULL-periaatteella.

Agenttimallissa seurattavaan koneeseen asennetaan ohjelma, joka toimii koneen muun toiminnan ohessa joko lähettäen tietoja ulospäin tai odottaen toimintapyyntöjä ohjaavalta koneelta. Agentin asennus vaatii aluksi ylimääräistä ylläpitotyötä. Agenttiohjelmien avulla voidaan usein saada yksityiskohtaisempaa tietoa koneen tilasta kuin mihin ulospäin näkyvien toimintojen perusteella pystytään, esimerkiksi tallennusmedioiden kunnosta. Agenttiohjelman tulee olla yhteensopiva koneen käyttöjärjestelmän kanssa, ja sen toiminta riippuu osaltaan isäntäkäyttöjärjestelmän toimivuudesta.

Erillinen tiedonkeruukomponentti on käyttöjärjestelmäriippumaton lisälaite joka kerää tietoja koneen toiminnasta ja voi tarvittaessa tehdä toimenpiteitä järjestelmälle, kuten käynnistää koneen uudestaan. Yleisesti näitä kutsutaan nimellä Intelligent Platform Management Interface (IPMI). Dellin Remote Access Controller (DRAC) on tällainen lisälaite, vastaava toiminnallisuus saadaan myös virtualisoitujen konei-

den osalta koska virtuaalikoneen isäntäjärjestelmästä käsin voidaan seurata koneen resurssienkäyttöä ja tarvittaessa käynnistää se uudestaan.

Tiedonkeruuta verkon välityksellä voi tehdä tutkimalla tarjottujen palveluiden toiminnallisuutta, mutta lisäksi on muodostunut standardoituja tiedonkeruutapoja jotka eivät vaadi erillisen agenttiohjelmiston asentamista toimiakseen. Näitä ovat muun muassa Simple Network Management Protocol (SNMP) sekä syslog.

SNMP hyväksyttiin Internet-standardiksi 1990, ja siihen on ilmestynyt jatkokehitettyjä versioita (SNMPv2, SNMPv3) jotka parantavat tehokkuutta ja tietoturvaa [26, 27, 28]. Standardi määrittelee joukon tietotyyppejä joiden tulee olla samoja kaikissa samantyyppisissä mitattavissa laitteissa. Tyypillisesti SNMP:llä luetaan reitittimien siirtämien pakettien ja tavujen määrää. Verkkolaitteiden ominaisuuksiin liittyvät tietotyypit on määritelty Remote Monitoring (RMON) standardeissa [29].

SNMP sisältää neljä tapaa liikennöidä laitteiden kanssa: GET lukee tarkkailevalle koneelle arvon SNMP-yhteensopivasta laitteesta. GETNEXT lukee seuraavan arvon listojen läpikäymiseksi. SET asettaa laitteen muuttujalle arvon tarkkailevan koneen pyynnöstä. TRAP lähettää tarkkailtavalta laitteelta oma-aloitteisesti viestin tarkkailevalle koneelle. GET ja GETNEXT viestit ovat proaktiivisten tarkkailumallien käytössä ja TRAP viestit mahdollistavat reaktiivisen tarkkailun. Yleensä SNMP:n kanssa joudutaan tyytymään rajapintoihin jotka laite- tai ohjelmistovalmistajat ovat toteuttaneet.

Syslog on 1980-luvulta lähtien käytössä ollut de-facto standardi tapa lähettää yksirivisiä tekstimuotoisia ilmoituksia järjestelmän tilasta etukäteen määrätyille vastaanottajille. Tästä on sittemmin (vuonna 2001) koottu ohjeistus laajan käyttöönoton myötä [30]. Jokaiselle viestille on määritelty lähettävän järjestelmänosan koodi, vakavuusluokka sekä lähetysaika. Syslog-viesteille voidaan määritellä myös välityspalvelimia jotka toimittavat viestit edelleen arkistointipalvelimille. Tätä ei ole määritelty alkuperäisessä toteutuksessa, mutta monet toteutukset käyttävät ominaisuutta. Syslog-protokolla toimii viestien välittäjänä, joten se soveltuu reaktiiviseen valvontaan. Lisäksi logiviestit yleensä kootaan joka koneelle paikallisesti (/var/log -hakemistoon), mikä auttaa tapahtuneen ongelman jälkiselvittämistä.

Klassiselle syslog-protokollalle on kehitetty perillistä, mutta alkuperäisen hyvät ominaisuudet (yksinkertaisuus, lähes universaali tuki) asettavat seuraajalle odotuksia joita on hankala täyttää. Syslogin uudempi versio pyrkii parantamaan syslog-protokollan luotettavuutta ja tietoturvallisuutta, muun muassa määrittelemällä viestiformaatin joustavammin ja viestien siirtotien tarvittaessa kryptografisesti suojattavaksi. Käytettävää siirtotietä ei ole määritelty yksikäsitteisesti, mutta suositukse-

na on käyttää salattua TLS-protokollaa perinteisen UDP:n sijaan. Uusi standardi on kuitenkin alkuperäistä paljon monimutkaisempi ja sen tarjoamia etuja ei ole koettu tärkeiksi, joten käyttöönotto on ollut vähäistä. [31]

Round Robin Database tool eli RRDtool on avoimen lähdekoodin toteutus kiinteänkokoisesta tietokannasta, jonka koko määritellään tietokantaa perustettaessa ja uusi tieto säilötään korvaamalla vanhimmat merkinnät. RRDtool on komentorivityökalu joka tarjoaa mahdollisuudet tiedon tallennukseen sekä aikasarjakuvaajien piirtämiseen. RRDtool olettaa saavansa tietoa järjestyksessä sekä määrätyin väliajoin, ja sen tavanomaisin käyttötapa onkin kerätä merkintöjä reaaliaikaisesta valvonnasta verkon avulla. Jos tietoa ei ole saatavissa määräaikaan mennessä, RRDtool merkitsee sen tuntemattomaksi jotta se voidaan tarvittaessa kompensoida. Vaihtoehtoja RRDtoolille ovat esimerkiksi relaatiotietokannat (kuten MySQL) sekä teksti- tai XML-pohjainen tiedontallennus.

RRDtoolin normaali käyttötapa on tehdä mittauksia ennaltamäärätyin aikavälein, ja tallentaa tulokset tietokantaan. Kantaa luodessa määritetään miten pitkiä aikoja tietoa säilytetään ennen karkeistamista, ja tietokanta pysyy samankokoisena käytettäessä. Karkeistaessa mittapisteitä voidaan joko keskiarvoistaa, muistaa vain maksimi tai muistaa vain minimi. Näin saadaan riittävä määrä datapisteitä laajemmalta aikaväliltä, esimerkkinä viimeiset 24 tuntia, viimeisin viikko, viimeisin kuukausi, viimeisin vuosi tai viimeisimmät kaksi vuotta. Graafin mittojen pysyessä samana yhden datapisteen kattama aikaväli kasvaa, jolloin sen esittämiseen tarvitaan myös vähemmän mittauspisteitä.

Cacti on graafinen käyttöliittymä RRDtoolille jota ajetaan PHP verkko-ohjelmointikielellä. Cactin tarvitsemat määritykset pohjautuvat siten vahvasti RRDtoolin mahdollisuuksiin ja rajoituksiin. Cacti tarjoaa ryhmiteltyjä näkymiä eri mittasuureisiin, sekä mahdollisuuden tarkentaa ja selailla varsin vapaasti mitattua aikasarjaa eri väleiltä. Cacti tarjoaa myös mahdollisuuden ajastaa mittauksia tallennettavaksi RRDtoolilla, käyttäen muun muassa SNMP:tä mittausten keräämiseen.

3.2.2 Microsoftin tuotteet

Microsoftilla on kaksi tuotetta jotka ovat keskittyneet koneiden valvontaan ja raportointiin. Microsoft Operations Manager (MOM) [32, 33], jonka uudempi versio on nimeltään System Center Operations Manager (SCOM) kerää tietoja Microsoftin palvelimista, koostaa niistä kuvaajia ja lähettää tarvittaessa muistutuksia rajaarvojen ylittymisestä sähköpostitse ja tekstiviesteillä. Tietoa voi kerätä joko valvontakoneen ajoittaisilla tarkistuksilla tai palvelimille asennettavalla agenttiohjelmalla

joilla saadaan tarkempaa tietoa palvelimen toiminnasta.

Microsoftin Systems Management Server (SMS), uudemmalta nimeltään System Center Configuration Manager (SCCM) on pääasialliselta käyttötavaltaan ohjelmistojen jakelupalvelin työasemille. Kohdekoneille asennetaan agentti, joka kerää määritellyt tiedot (mm. laitteisto- ja ohjelmistokokoonpanon). Nämä tiedot siirretään kohdekoneilta käsin ajastetusti palvelimelle http-porttiin 80 käyttäen Background Intelligent Transfer Service eli BITS-protokollaa [34]. Siirto vaatii palvelimelta IIS- eli Internet Information Services palvelun olemassaolon. Tällöin yhteyden hitaus tai katkeilevuus ei muodostu ongelmaksi. Tietojen siirron onnistumiseksi myös nimipalvelimien pitää tukea dynaamista rekisteröitymistä, jotta smskone -pyynnöt päätyvät smskone.domain.fi palvelimelle asti.

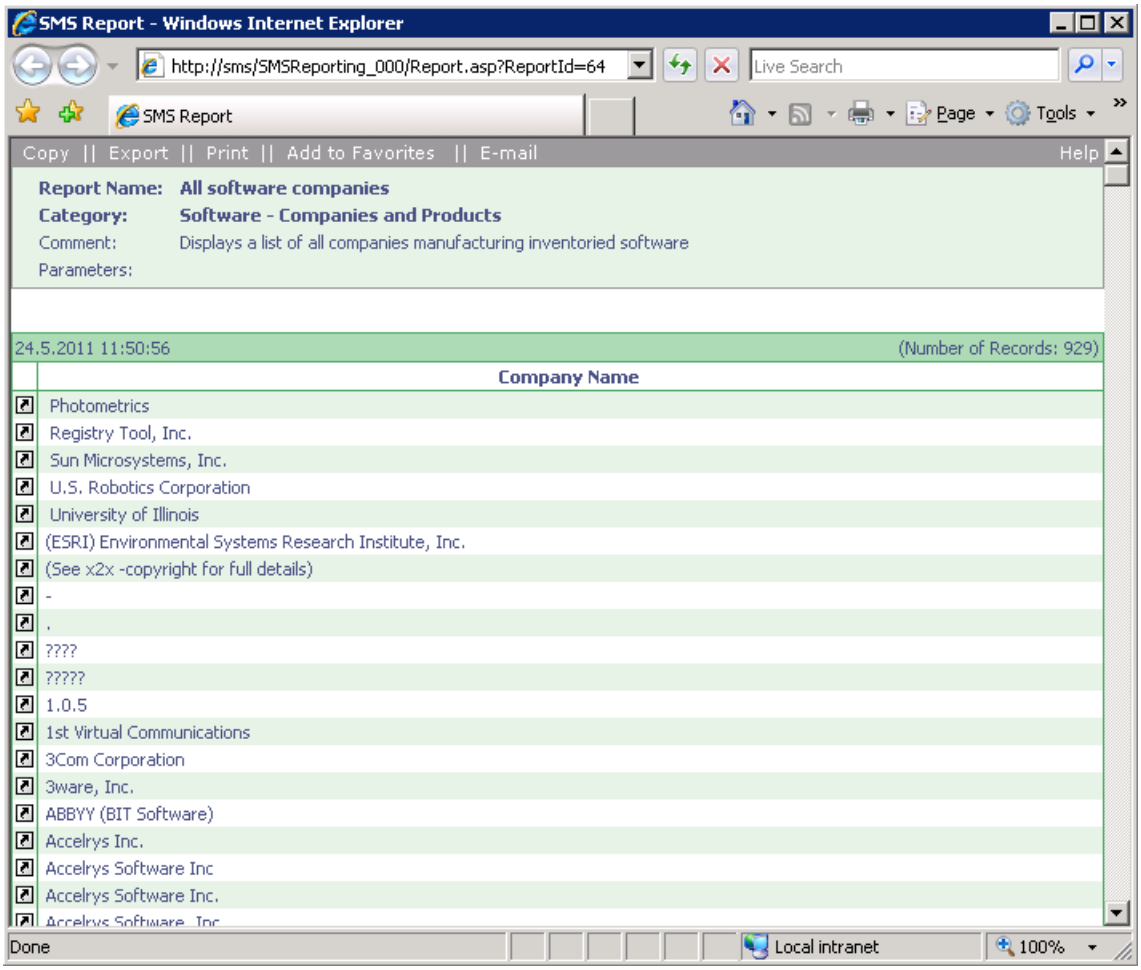
SMS-palvelimella voi myös tehdä raportointia valmiilla tai itse muokatuilla SQL-kyselyillä palvelimen tietokantaan. Näistä kyselyistä voidaan tehdä myös selaimella näkyviä graafeja sekä raportteja seurattavien koneiden tilasta. Hälytyksiä SMS ei lähetä, vaan tietojen hyödyntäminen riippuu niiden seuraajista. Kuvassa 10 on esitetty yksi SMS:n raportti-ikkuna, jossa on listattuna kaikkien keskitetyssä hallinnassa olevien koneiden ohjelmistojen valmistajat, riippumatta siitä onko ne asennettu SMS:n kautta tai erillisasennuksina.

SMS käyttää omaa nimeämisjärjestelmäänsä palveluiden tuottamiseen. Järjestelmä on muokattu versio DNS:stä, jossa koneen nimi rekisteröidään dynaamisesti DNS-palvelimelle jotta siihen saadaan yhteys koneennimi.domain.fi kyselyllä. Koneen nimi puolestaan pohjautuu Common Internet File System (CIFS) tarvitsemiin nimiin, joka tunnetaan myös nimellä Server Message Block (SMB) [35]. Jos protokollan vaatimia portteja ei ole palomuureissa avattuna, nimenselvitys ja sen myötä SMS:n yhteys asiakaskoneelle ei toimi.

SMS kerää tiedot asiakaskoneista agentin ja Windows Management Instrumentation (WMI) avulla [36]. Normaalisti WMI-rajapinta on käytettävissä vain koneella paikallisesti toimiessa, mutta agentin avulla tiedot saadaan käyttöön myös etäyhteyksiin. Rajapinnan käyttöön löytyy laajennusosia myös Nagiokseen, esimerkiksi Windowsin järjestelmälokien varoitusten ja hälytysten siirtämiseksi Nagios-valvontajärjestelmään on mahdollista [37].

3.2.3 Mittausdatan siirto

Tiedon siirtäminen järjestelmästä toiseen vaatii luottamussuhteiden määrittämistä, jotta saatu tieto voidaan todeta aidoksi ja lähde voidaan jäljittää. Koska pystytettävä valvontadatan visualisointipalvelu sijoittuu julkisesti saataviin koko maailmalle



Kuva 10: SMS-palvelimen raportti-ikkuna asennettujen ohjelmistojen valmistajista

näkyväksi, sille tulee asentaa tietoturvapäivitykset mahdollisimman automaattisesti sekä tarjottujen rajapintojen määrä tulee minimoida haavoittuvien palveluiden määrän rajoittamiseksi.

SSH-etäyhteysprotokollassa on mahdollista tehdä julkisen ja yksityisen avaimen pareja, jotka korvaavat käyttäjätunnus ja salasana -tunnistautumisen. Avainparia käytettäessä julkista avainta voidaan levittää vapaasti eteenpäin, yksityinen avain pidetään vain omassa tiedossa. Palvelimelle voidaan määrittää mitkä julkiset avaimet kelpaavat kirjautumiseen. Muitakin kirjautumisrajoituksia voidaan määrittää, kuten interaktiivisten komentojen puuttuminen, jatkotunnelien muodostamiskielto, IP-alueet joista avaimella on mahdollista kirjautua sekä ajettavat komennot kirjauduttaessa. [38]

Verkkotopologian kannalta koneelta ulospäin otettavat yhteydet vaativat vähemmän muutoksia palomuureihin kuin koneelle sisäänpäin avattavat yhteydet. Tähän

on vaikuttanut osaltaan vapaiden IPv4-osoitteiden väheneminen, jonka seurauksena eri verkkoympäristöissä on otettu käyttöön verkko-osoitemuunnoksia (Network Address Translation, NAT). Natin läpi kulkeva liikenne on lähtökohtaisesti yksisuuntaista siten että vain ulospäin otettavat yhteydet toimivat, kun taas osoitemuunnoksen sisäverkossa auki oleva palvelu vaatii muunnoksen tekevälle verkkolaitteelle portin edelleenohjauksen määrittelyä.

Palomuurit toimivat rajaamassa verkkosegmenttejä toisistaan sekä tarjoamalla lisärajausmahdollisuuden tarjottavista koneen palveluista. Esimerkiksi Windows-käyttöjärjestelmässä on oletusarvoisesti CIFS-palvelu käytössä, samoin kuin ylläpitokäyttöön varattu tiedostojenjako ja tulostimenjako. Verkon palomuurilla voidaan rajata sisäverkon palveluiden saatavuutta, ja koneelle asennettavalla ohjelmistopalomuurilla voidaan rajata yhteydenottopyyntöjä tarkemmin sekä verkosta riippumatta.

3.3 Yhteenveto

Olemassa oleva valvontainfrastruktuuri palvelee kelvollisesti ylläpitäjiä jotka ovat valvontajärjestelmät pystyttäneet ja käyttävät niitä omien vastuualueidensa seuraamiseen. Serverstatus-palvelun hyvät asiakaskokemukset halutaan laajentaa myös muihin datalajeihin, säilyttäen myös alkuperäinen palvelu samassa verkko-osoitteessa.

Tietolähteiden moninaisuuden myötä eri valvontatyökalut on suunniteltu virtaviivaisesti käyttöönotettaviksi omalla erikoistumisalallaan. Jos valvottavana on pelkästään verkkolaitteita, SNMP-rajapintaakin tukeva Nagios on hyvä valinta. Windows-työasemien valvontaan pääsee nopeiten käsiksi SMS-palvelimella, Windows-palvelimien osalta MOM-palvelimella. Valvontapalvelimen ominaisuuksia tutkiessa WMI on hyvä avainsana etsittäväksi jos valvontatyökalun halutaan tukevan Windowsia. Nagios on myös laajennettavissa valvomaan mitä moninaisempia palveluita. Cactin vahvuutena on helppokäyttöinen visualisointiliittymä. Verkkolaiteiden osalta SNMP on tuetuin valvontaprotokolla, ja Linuxin puolella vähintään syslog löytyy joka laitteesta.

Valvontainfrastruktuurin pystyttäminen vaatii osaamista ja perehtymistä valvontavaihtoehtoihin. Puoliautomaattisen valvonnan myötä rutiinitarkastukset saadaan tehtyä järjestelmällisesti ja kyllästymättä, jolloin ylläpitäjien huomiota vapautuu enemmän ilmenneiden ongelmien ratkaisemiseen.

4 Ratkaisumalli

Hankkeen toteuttamiseen liittyi useita vaiheita, joita käsitellään tässä luvussa. Aluksi käydään läpi henkilöstön kanssa tehdyt linjaukset sekä projektin tavoitteet. Valitun alustatekniikan yksityiskohdat käsitellään seuraavaksi, sitten siirrytään toteutetun järjestelmän määrityksiin ja toimintaan. Viimeisenä kappaleena käsitellään aiheesta syntyneitä johtopäätöksiä ennen koko työn yhteenvetoa.

4.1 Hankkeen valmistelu

Hanke koskettaa useita CSC:n toimintoja, joten ryhmien välinen yhteistyö on tarpeen valvonnan onnistumiseksi. Toteutusmallin esittelemiseksi ja hyväksyttämiseksi järjestettiin kaksi palaveria, joihin kutsuttiin palvelimen kanssa tekemisiin pääsevät ihmiset sekä infrastruktuurin ylläpidosta vastaavat. Neuvottelemalla eri osa-alueista vastaavien ryhmien kanssa päädyttiin toteutuskelpoiseen ratkaisuun CSC:n palvelunperustamisprosesseja noudattaen. Hankkeen hahmotteluvaiheessa tietoa kerättiin intranetin wiki-sivulle joka oli kaikkien ryhmien tutustuttavissa.

Alkuun esitettiin huoli nykyisten valvontajärjestelmien ylläpitäjiltä, että tuleeko projektissa tehtyä turhaa työtä jo kerran rakennetun järjestelmän uudelleenpystyttämiseksi. Samoin tietoturvasta supervalvontakoneella oltiin huolissaan. Ratkaisu linjattiin pelkästään vastaanottamaan olemassa olevaa valvontadataa, ei keräämään sitä itse, jolloin päällekkäistä valvontaa ei synny. Tietoturvan varmistamiseksi ratkaisumalliksi valittiin push-tyylinen liikenne, jossa dataa keräävät koneet tekevät ajastettuja siirtoja keskuskoneelle. Näin palomuureista ei tarvitse avata portteja jotka voisivat altistaa haavoittuvia palveluita verkkohyökkäyksille.

Toisessa palaverissa käytiin läpi verkkosijoitusta. Virtuaalikonekapasiteetin takia palvelin pystytettiin erilliseen verkkoon superkoneista, jolloin suorat NFS-siirrot kävivät liian hankaliksi toteuttaa. Samaten ylläpidon olemassa olevan asiantuntemuksen nojalla tallennustapa vaihtui NFS:stä SAN-tyyppiseksi, jolloin myös ZFS-tiedostojärjestelmää ei voitu käyttää tiedostojärjestelmätason tiivistämisen hyödyntämiseksi. Päätös osoittautui vuoden päästä hyvin perustelluksi, kun Oracle osti Sun Microsystemsin ja uudelleenhinnoitteli suuren osan tarjoamistaan palveluista [39].

Wiki-sivuille koottiin palaveripöytäkirjojen lisäksi linkkejä muiden ryhmien aikaisempiin projekteihin ja kehitysideoihin valvonnan tehostamisesta. Asia oli tullut useaan otteeseen esille hieman eri näkökulmista katsoen, joten näistä hankkeista muistuttaminen oli omiaan sitouttamaan muiden ryhmien edustajia hankkeen taakse.

Olennainen ero olemassa oleviin visualisointijärjestelmiin CSC:llä on mahdollisuus asettaa visualisointeja julkisesti tarjolle. Tämän linjauksen myötä datankeruumalli valittiin vastaanottavaksi. Selvitettäväksi jäi vielä autentikointimahdollisuuden toteuttaminen esimerkiksi CSC:n olemassa olevan Haka-mallin mukaiseksi tai vierastilipohjaiseksi. Tällöin asiakkaat saisivat lähes reaaliaikaista tietoa CSC:n julkiseksi valituista toiminnoista, nykyisen vuosittaisen paperisen vuosikertomuksen lisäksi.

Visualisointipalvelimen kohdeyleisöä ovat CSC:n laskentapalveluiden käyttäjät, toisin sanoen organisaation ulkopuoliset toimijat. Toinen kohdeyleisö on CSC:n johtoporras, jolle katsaus CSC:n toimintoihin, kuormitukseen ja saatavuuteen voi auttaa hankintojen suunnittelussa. Varsinaista kohdeyleisöä eivät ole palveluiden ylläpitäjät, koska valvontatieto siirretään valvontapalvelimelle viiveellä ja palvelimen saatavuutta ei taata esimerkiksi varapalvelinjärjestelyllä. Ylläpitäjille lähetettävät hälytykset hoidetaan tiedot keräävien laitteiden oheistoimintana, jotta havaittuihin puutteisiin voidaan reagoida mahdollisimman nopeasti.

4.2 Alustatekniikka

Palvelin pystytettiin virtuaalikoneeksi julkisesti saataville marraskuussa 2009. Käyttöjärjestelmänä toimii 64-bittinen versio Redhat Enterprise Linux 5:sta, koska sille on tukijärjestelmä jo käyttöönotettuna. Palvelimen nimeksi annettiin kamreeri.csc.fi ja sille tehtiin erillinen osio datan säilömistä varten, arviolla säilöä kaikista lähteistä tuleva data 5 vuoden ajan, osa datasta useampaan eri muotoon muunnettuna. Arvion perusteella datalevylle varattiin 200 GB tilaa. Palvelimesta otetaan varmuuskopiot jotta kerätty data olisi varmasti tallessa ja vakavammistakin vikatilanteista voitaisiin toipua enintään viikossa. Koska palvelin ei ole datankerääjä tai hälytysten lähettäjä, sen toipumisessa saa kestää päiviäkin.

Virtuaalikoneen valinnan edut ovat ensisijaisesti resurssitehokkuudessa. Palvelimen käyttö ei sido fyysistä tilaa, jäähdytystä tai virrankulutusta nykyistä enempää, lisäksi prosessointia tehdään vain sen verran kuin palvelin oikeasti tarvitsee. Loppu prosessointiajasta käytetään muiden samassa klusterissa toimivien virtuaalikoneiden hyväksi. Virtuaalipalvelin voidaan myös joustavasti siirtää klusterista toiseen toiminnan häiriintymättä. Koska palvelin ei tarvitse erityisiä fyysisiä kytköksiä, vaan verkkoyhteys riittää, ei virtualisointi ole este liitäntöjenkään puolesta.

Virtualisoinnin haittapuolet ovat taatun kapasiteetin puute, joka voi aiheuttaa palvelun hidastumista jos muut klusterin virtuaalikoneet tarvitsevat samalla runsaasti resursseja. Kapasiteetin joustavuudesta seuraa myös järjestelmän kellonajan voimakkaampi heittelehtiminen, joka voi muodostua ongelmaksi jos palvelu vaatii

tarkkaa ajastusta, mittausten ajoittamista tai tietoturvan nimissä synkronoituja ssh-siirtoja. Tyypillisenä ratkaisuna palvelin asetetaan synkronoimaan kellonsa ulkoisen Network Time Protocol (NTP) palvelimen kanssa.

Palvelimen ohjelmistot päätettiin asentaa jakelun RPM-paketeista niin pitkälti kuin mahdollista, jotta ne päivittyisivät automaattisesti. Koneen perusta pohjautuu LAMP-malliin: Linux käyttöjärjestelmänä, Apache http-palvelimena, MySQL tietokantamoottorina ja PHP dynaamisten sivujen luontikielenä. Järjestelmään lisättiin Rpmforge-repositorio laajennetun pakettivalikoiman saamiseksi osoitteesta http://apt.sw.be/. Sieltä asennettiin ensimmäisessä vaiheessa Cacti riippuvuuksineen oletuspolkuunsa. Datavarastohakemistot cactin puussa siirrettiin symlinkeillä osoittamaan palvelimen dataosiolle. Asennuksen yksityiskohtaiset vaiheet ja käytetyt komennot on dokumentoitu erilliseen ohjeeseen [40].

4.3 Tietoturva

Palvelu toteutettiin niin että koneelle tehdyllä käyttäjätasoisella tunnuksella voidaan suorittaa palvelun päivittäinen operointi, niin ettei pääsyä järjestelmään asennettujen ohjelmien muuttamiseen ole normaalisti. Tämä edellytti MySQL-käyttötunnusten oikeuksien määrittämistä tarvittaville tietokannoille käyttäjätunnuksen osalta, sekä kansioiden kirjoitusoikeuksien määrittämistä päivittäisen tarpeen huomioonottaen.

Ulkopuolelta otettavien yhteyksien käyttömahdollisuuksia rajoitettiin ssh:n authorized hosts toiminnolla niin, että kullakin datankeruukoneella on pääsy vain omaan datantuontihakemistoonsa. Samalla toiminnolla rajoitettiin käytettävissä olevat komennot viimeisimmän hyväksytyn aikaleiman lukemiseen sekä oman datatiedostonsa siirtämiseen. Yksi vaihtoehto lisäturvan saamiseksi olisi käyttää salasanasuojattuja avaimia sekä agenttia, jolle syötettäisiin salasana keräinkoneen käynnistämisen yhteydessä, joka sitten käyttäisi salasanallisia avaimia ajastetusti ja automaattisesti niin kauan kun kone on pysynyt yhtäjaksoisesti päällä. Menetelmän haittapuolena ovat pitkittyneet tiedonsiirtoviiveet keräinkoneiden uudelleenkäynnistysten yhteydessä, joten agenttia ei otettu vielä tässä vaiheessa käyttöön. [41]

Palveluun siirrettävät datat valittiin ainakin aluksi siten, että ne ovat julkistamiskelpoisia eli eivät sisällä salassa pidettävää tai luottamuksellista tietoa. Kunhan näkymät saadaan säädettyä kuntoon asiakkaiden, johdon ja ylläpidon osalta, datalähteiden määrää kasvatetaan palvelemaan paremmin kunkin kohderyhmän tarpeita.

Olemassa oleviin palomuureihin ei tarvinnut tehdä muutoksia kamreerin toiminnan mahdollistamiseksi, koska valvontadata kerätään muilla olemassa olevilla jär-

jestelmillä ja vain siirretään ajastetusti kamreerin käyttöön. Täten myös palvelun myötä aukeavien uusien haavoittuvuuksien määrä minimoitiin. Yhteydenottojen nopeutta rajoitettiin myös ohjelmistopalomuurin säännöllä, joka rajaa epäonnistuneiden yhteydenottojen määrän kamreerille tietystä IP-osoitteesta tietyssä aikaikkunassa pieneksi, esimerkiksi sallien vain viisi epäonnistunutta yritystä minuutissa samasta osoitteesta [42]. Tämä pienentää olennaisesti sanakirjahyökkäysten tehoa.

4.4 Toiminta

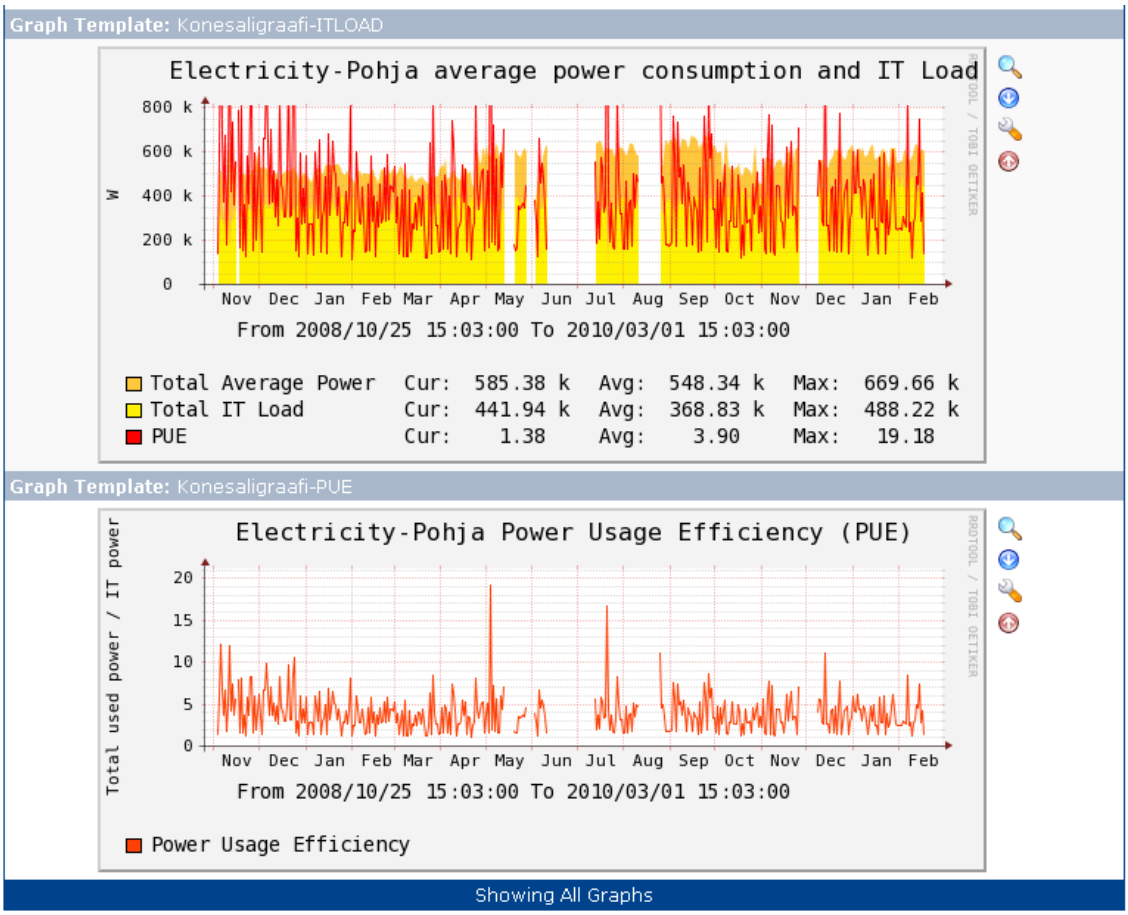
Jokaiselle valvonnan piirissä olevalle keräimelle määritetään automaattiset ajastetut tiedostonsiirrot valvontakoneen kamreeri.csc.fi osoitteeseen, ennaltamäärättyyn raakadatapolkuun. SQL-siirtojen tapauksessa datankeruukone hakee ensin kamreerilta tiedon viimeisimmästä onnistuneesta tiedonlisäysajankohdasta, tekee omaan tietokantaansa haun muutoksista annetun ajankohdan jälkeen ja siirtää uudet tiedot valvontakoneelle.

SQL-datan siirrosta palvelimien välillä on yleisesti käytössä oleva ratkaisu nimeltään SQL-replikointi, mutta siinä tietoturvamalli on toiseen suuntaan avoin – kopioiva taho ottaa yhteyttä päätietokannan sisältävään koneeseen. Replikoinnissa myös master-kone tekee binaarilokia muutoksistaan, kun tässä tapauksessa tietokannat ovat 32- ja 64-bittisiä ja siten eivät suoraan binaariyhteensopivia. Tämän ratkaisun tietoturvamallissa kaikki siirrot tehdään ottamalla yhteyttä ajastetusti visualisointipalvelimelle.

Kamreerilla pyörivät cron-ajastetut tarkistukset jotka hakevat raakadata-hakemistoista uusia lisäyksiä, ja siirtävät ne kamreerin paikalliseen SQL-tietokantaan. Onnistuneen siirron päätteeksi päivitetään aikaleimatiedostot osoittamaan viimeisintä tallennettua ajankohtaa.

Kuvassa 11 näkyy Kamreerin virrankulutusnäkymä yhden konesalin osalta. Raakadatan katkonaisuus tulee tästä kuvasta hyvin esille - mittauksessa on ollut taukoja ja virhetilanteita jolloin kaikkia virrankulutuslukemia ei ole saatu talteen. Tauot ovat olleet päivien tai kuukausien mittaisia, jolloin mitään mittauksia ei ole saatu, graafissa tämä näkyy tyhjinä osioina. Ylemmässä kaaviossa kokonaisvirrankulutus ja IT-laitteiden virrankulutus on eritelty väreillä. IT-laitteiden yhteiskulutus on saatu laskemalla jokaisen UPS-ulostulon kuormat yhteen. Kaikki IT-laitteet ovat kiinni UPS-pistokkeissa. Kokonaisvirrankulutus on saatu UPS-järjestelmän sisäänottotehosta, jossa on mukana myös jäähdytyslaitteiston virrankulutus, valaistus sekä UPS-järjestelmän tehohäviöt. Kun UPS-lukemien talteenotossa on tapahtunut virheitä, IT-kuorman summa on pudonnut jopa kolmasosalla, joka on aiheuttanut

vastaavasti PUE-arvoon mittausvirheestä johtuvan piikin. Näitä on datassa useita, mikä vääristää PUEn keskiarvoa todellista suuremmaksi. PUE käsitellään tarkemmin seuraavassa luvussa ”Käyttötavat”.



Kuva 11: Kamreerin virrankulutusnäkymä yhdestä konesalista sekä PUE-arvo

Tiedonsiirtoketju toimii sähkönkulutuksen seurannan osalta näin: työasema, jossa on fyysinen COM-portti, on yhteydessä UPS-laitteistoon ja hakee sieltä 30 minuutin välein kuormitus- sekä loisvirtalukemat. Nämä tallennetaan työaseman paikalliseen 32-bittiseen MySQL-kantaan. Työasemalle on ajastettu myös 30 minuutin välein ssh-etäyhteyden otto kamreeri-koneelle, ja sieltä viimeisimmän hyväksytyn aikaleiman hakeminen. Tätä leimaa käytetään hakemaan paikallisesta SQL-kannasta leiman jälkeen tulleet muutokset, jotka tallennettetaan XML-dumpiksi sekä siirretään kamreerille.

Kamreerilla viiden minuutin välein ajastettu prosessi tarkistaa onko uutta tietoa saapunut joltain kerääjäkoneelta vastaanottohakemistoon. Tämä tieto tallennetaan kamreerin paikalliseen 64-bittiseen MySQL-kantaan, tiedosto poistetaan ja päivitetään viimeisin vastaanotettu aikaleima keräinkoneen luettavaksi. Tiedoista valitaan

graafin kannalta olennaiset lukemat ja ne muunnetaan komentojonotiedoston avulla aikajärjestyksessä edeten RRD-muotoon. Tiedot säilytetään siis kahdessa eri muodossa kamreerilla, RRD-tiedostoissa joista voidaan muodostaa nopeasti katsottavat graafit sekä SQL-kannassa, josta voidaan tehdä jatkolaajennuksia muille myöhemmin lisättäville visualisointipalveluille.

Kun data on saatu näin käsiteltyä, verkkopalvelu Cactin käyttäjät voivat selatessaan palvelua piirtää RRD-tiedostoista muodostettuja kuvaajia sähkönkulutuksesta. Palvelimen ajastettu prosessi ajaa myös rrdtoolin muodostamaan pysyvällä nimellä löytyvän päivittyvän kuvan tarjolle WWW-polkuun, josta se voidaan liittää muille julkisille sivuille antamaan yleiskatsaus sähkönkulutuksesta viimeisen 30 minuutin tarkkuudella.

4.5 Käyttötavat

Aluksi eriteltiin UPS:ltä saaduista tiedoista kokonaisvirrankulutus runkoverkosta otettuna. Toiseksi datamittauspisteeksi valittiin summa UPSien lähtötehoista, joka on toisin sanoen IT-laitteiden kuluttama kuorma kun valaistusta ja jäähdytystä ei ole laskettu mukaan. Laskennalliseksi mitta-arvoksi lisättiin tehonkäytön hyötysuhde (Power Usage Effectiveness, PUE), joka on tietoteollisuudessa tällä hetkellä yleisin käytettävä tehokkuustunnusluku [43].

PUE lasketaan seuraavalla kaavalla:

$$\mathrm{PUE} = \frac{\text{Kokonaisteho}}{\text{IT-kuorma}} \tag{2}$$

Toisin sanoen, kaikki teho jota ei käytetä IT-kuorman pyörittämiseen huonontaa hyötysuhdetta. Tästä seuraa että jäähdytykseen tulee käyttää mahdollisimman vähän energiaa, ja hukkalämmön hyödyntäminen mihinkään joka vaatisi lisäenergian käyttöä huonontaa myös hyötysuhdetta. Yleisesti tehokkainta PUE-arvon kannalta on hankkiutua IT-laitteiden tuottamasta ylijäämälämmöstä eroon mahdollisimman suoraviivaisesti lauhduttimilla ulkoilmaan. Suomessa tähän on hyvät mahdollisuudet, koska ilmasto on viileää suuren osan vuodesta ja korvausilmaa ei tarvitse koneellisesti jäähdyttää.

Koska IT-kuormat summattiin yhteen, PUE-arvossa havaittiin useita korkeita piikkejä. Syyksi paljastui katkonainen mittausdata eri UPS-lukemista. Yhdenkin mitta-arvon puuttuminen tiputti IT-kuorman summaa yli kolmasosalla, aiheuttaen hyötysuhteen laskennallisen romahtamisen ja PUE-piikin. Ratkaisuna on tuoda IT-kuormat erikseen RRD-tiedoston arvoiksi, summata ne vasta graafia piirrettäessä ja

merkitä tuntemattomat arvot tuntemattomiksi myös RRD:n puolella, jotta RRDtool osaa interpoloida puuttuvat arvot viereisistä arvoista.

PUE-arvon saaminen graafissa näkyviin ei ollut aivan suoraviivaista. RRDtoolin graafissa ei ole luonnostaan tukea useammalle mitta-asteikolle, ja sadoissa kilowateissa mitattavat tehoarvot dominoivat asteikkoa 1,2 luokassa olevan PUE:n rinnalla. Ratkaisuna oli kertoa PUE-arvo graafia piirrettäessä kertoimella 100 000, jolloin vaihtelu erottuu teholukemien kanssa samalla asteikolla. Kerroin saatiin katsomalla konesalien virrankulutusten maksimiarvoja ja siirtämällä PUE-arvot samalle dekadille.

PUE-piikit ovat graafissa tarkoituksella huomiota herättäviä, jotta ne ohjaavat tutkimaan mikä on aiheuttanut sähkönkulutuksen hyötysuhteen heikkenemisen. Automaattisen skaalaamisen ansiosta korkeat piikit kuitenkin painavat normaalin toiminnan aikaiset lukemat graafissa niin alas ettei niitä saa luettua. Vaihtoehtoisena mittarina on olemassa PUEn käänteisluku Data Center Infrastructure Efficiency (DCIE), joka lasketaan jakamalla IT-kuorma kokonaisteholla. Tällöin lukeman vaihteluväli on 0-100% välillä.

RRDtoolin tietokannan täydentämisessä tuli huomioida erityisesti aikajärjestyksessä pysyminen. Tietokannassa on laskuri viimeisimmän syötetyn arvon ajanhetkestä, joka alustetaan tietokantaa luodessa. Kanta ei suostu ottamaan vastaan vanhempaa arvoa kuin viimeisin syötetty on, joten muiden laitteistojen tekemät mittaukset tulee myös kerätä ja muuntaa aikajärjestyksessä. MySQL osoittautui tässä hyväksi apuvälineeksi valmiiden aikamuunnostensa ansiosta, joilla tietoa voi paitsi hakea aikajärjestyksessä, myös aikamääreet voi muuntaa eri esitysmuotoihin kuten sekuntipohjaiseen unixtimeen.

Alussa mittausdata siirrettiin käsin erillisestä huoltoverkosta, jonka ainoa yhteys ulkomaailmaan kulki VPN-keskittimen kautta. Kun paljastui, että keskittimen ominaisuuksiin ei kuulunut edes rajoitettu verkkosiltaus ulkomaailman ja sisäverkon välillä, päätettiin verkkotopologiaa muuttaa niin että virrankulutusta mittaavat laitteet siirrettäisiin toiseen sisäverkkoon josta on pääsy kamreerille.

4.6 Datan jalostaminen

Kerätysta datamäärästä merkitystellisten tapahtumien louhiminen on hyödyllistä varsinkin palveluiden ylläpitäjille. Louhimisen yleissääntönä voidaan pitää trendistä poikkeamista. Tapahtumaa tulee korostaa muun muassa jos:

- Liikenne jostain IP-lohkosta kasvaa merkittävästi

- Laskentaytimien käyttö poikkeaa vuosirytmistä
- Konesalin lämpötilat poikkeavat vuorokausirytmistä
- Tehonkulutus poikkeaa merkittävästi vuosirytmistä

Tiedonlouhinta tarjoaa erinäisiä automatisoituja menetelmiä datan sovittamiseksi ennustemalliin ja datan ryhmittelyyn [44]. Olennainen asia hälytystasoja määrittäessä on kiinnittää muutosnopeuden sallittu poikkeama odotetusta muutosnopeudesta. Liian pieni kynnys aiheuttaa vääriä hälytyksiä, liian suuri jättää merkityksellisiä muutoksia huomiotta. Suhteelliset muutokset antavat skaalariippumattomuutta, esimerkkinä tallennuslevyjen käyttöasteen kasvaminen 10% päivässä.

Datasta voidaan myös laskea tunnuslukuja keskinäisistä suhteista, kuten konesalin toimintojen suhteellisen lisäkuorman mittari PUE, tai laskentaa suorittavien prosessoriydinten määrän suhde virrankulutukseen tai konesalin lämpötilaan (mittapisteinä voi käyttää myös prosessorien tai kovalevyjen lämpötilasensoreita). Yksittäisiä mittaustuloksia voi aggregoida keskiarvoiksi tai koneryhmien yhteisstatukseksi. Nämä toimenpiteet ovat kuitenkin perinteisempää tiedon esitysmuotojen muokkausta, eivät varsinaista algoritmipohjaista tiedonlouhintaa.

4.7 Johtopäätökset

Valvontadatapalvelimen asennuksen yhteydessä tuli tarpeelliseksi selvittää myös eri palveluiden väliset riippuvuussuhteet. Näitä tietoja tarpeen myös mittaustietojen tulkitsemisessa. Tiedonkeruupaikat ja kerätyn tiedon merkitykset on hyvä esittää samassa yhteydessä kuin mittaustuloksetkin, jotta kuka tahansa kiinnostunut voi tulkita niitä oikein. Systematisoitu tapa esittää kuvattavaa järjestelmää auttaisi sekä järjestelmän kuvauksessa sen käyttäjille että laskentakaavojen virittämisessä visualisointijärjestelmälle kuten Cactille. Ongelmaksi tässä muodostuu että visualisointiohjelmien määritykset ovat ohjelmakohtaisia joten järjestelmäkuvaus-ohjelma tulisi myös ohjelmakohtaiseksi ilman uutta standardia.

Puuttuvien mittausarvojen huomioiminen ja kompensoiminen tulee pitää mielessä järjestelmää suunnitellessa, jotta käytetyt kaavat pätevät osittaisenkin datan osalta. Työn ensimmäisessä toteutusvaiheessa käytetty IT-kuormien summa kärsi mittausarvojen puutteesta, jolloin PUE-arvon varianssi oli odotettua suurempi.

Tehonmittauksessa tulee myös selvittää tehokertymän mittausmahdollisuudet hetkellisten arvojen sijaan. RRDtoolin ominaisuuksiin kuuluu Counter-tyyppinen mittari joka on tarkoitettu kertymälaskurien käytettäväksi.

Cactin esityspohjat ovat kehittyneet RRDtoolin versioiden myötä siten, että uusimmissa versioissa on mahdollista käyttää graafissa kahta erillistä pystyakselin asteikkoa. Työn ensimmäisen toteutusvaiheen Cactissa tätä ominaisuutta ei vielä ollut, joten PUE-arvon sovittamiseksi graafin skaalassa näkyväksi se kerrottiin samaan kokoluokkaan kuin tehomittausarvot.

Muunnokset MySQL:stä RRD-tiedostoiksi sekä RRD-tiedostojen esittämistavat jouduttiin suunnittelemaan tapauskohtaisesti, joka muodostuu ongelmaksi jos tietolähteitä on tuhansia. Muunnoksissa pitää olla tiedossa hyödynnettävä data sekä sen riippuvuussuhteet jotta graafit voidaan laskea ja piirtää oikein. Käytetyn Cacti-ohjelman ominaisuuksiin kuuluu osittain automatisoitu tietojenkeruu SNMP-protokollalla, mutta sitä ei käytetty tässä tapauksessa koska tietoturvamallina haluttiin pitää push-tyyppinen liikennöinti.

Työn kuluessa todettiin että avoimen lähdekoodin ratkaisujen käytöstä saadaan järjestelmän kehitykselle jatkuvuutta, koska projektit ovat osoittautuneet pitkäikäisiksi ja päivittyviksi. Ylläpitäjälle tulee valinnan hetkiä lähinnä projektien haarautuessa useammaksi rinnakkaiseksi tuotteeksi, jolloin tulee valita minkä polun seuraamista jatkaa. Esimerkiksi työssä käytetyistä Nagios-valvontapalvelimista on haarautunut avoimempi Icinga-valvontapalvelin [45].

Virtuaalikoneen käyttämisen edut ovat palvelun riippumattomuus alustalaitteiston ikääntymisestä, sillä keskittämällä virtuaalikoneraudalle suuri määrä palvelimia varmistetaan että riippuvuussuhteista ja redundanssista huolehtiminen ovat ylläpidolla tärkeysjärjestyksessä korkealla.

PUEn käyttö ainoana tehokkuusmittarina on ongelmallista Suomen olosuhteissa, jossa koneiden tuottamalle hukkalämmöllekin on kehitettävissä käyttöä. Onhan Suomessa saatu muun muassa sähkön ja lämmön yhteistuotannolla nostettua yhteistuotantoa käyttävien voimaloiden kokonaistehokkuutta jopa 90% asti [46]. Samalla kokonaispäästöjä on saatu pudotettua 30% pienemmiksi verrattuna saman energiamäärän tuotantoon erillisissä laitoksissa. Yhteistuotannolla tehdyn kaukolämmön hyödyntämisen edellytys on riittävän laaja kaukolämpöverkko, jossa on tarpeeksi asiakkaita tarjotulle lämpömäärälle.

Tietokoneiden tuottaman hukkalämmön erityispiirre on suhteellisen matala lämpötila – poistoilma on korkeimmillaankin vain 37-asteen luokkaa (Celsius) kun käytössä on puhaltimien avulla toteutettu ilmajäähdytys. Näin matala lämpötila ei suoraan kelpaa kaukolämpöverkkoon ilman lämpötilan nostoa kylmälaitteilla, mikä taas vaatii lisäenergiaa ja huonontaa PUE-arvoa. [47, 48] Vaihtoehtoisia mittareita on ehdotettu PUEn korvaajaksi, jotka keskittyvät erityisesti virtapihimmän ja

suorituskykyisemmän laskutehon huomiointiin [47]. Ehdotus uudeksi mittariksi on hyödynnetyn kokonaisjärjestelmän tehosuhde (System Power Efficiency, SPE), joka on esitetty kaavassa 3.

$$\text{Systeemin tehosuhde SPE} = \frac{P_{tot}}{P_{IT} + P_{repl}} \tag{3}$$

Kaavassa P_{tot} on kokonaisteho, P_{IT} on IT-laitteiston käyttämä teho, P_{repl} on säästynyt teho muissa toiminnoissa joka on korvattu IT-laitteiston tuottamalla lämmöllä. Vapaajäähdytyksessä lisätermi on nolla ja kaava antaa saman arvon kuin PUE. Jos taas IT-laitteiston sivutuotteena tuottamaa lämpöä käytetään muun lämmitystarpeen korvaamiseen, voidaan laskea säästetty teho siirtohäviöineen ja verrata sitä tilanteeseen, jossa sama lämmitysteho olisi tuotettu seuraavaksi parhaalla saatavissa olevalla menetelmällä. Tällaisia lämmityskohteita voivat olla muun muassa toimistokerrosten tai asuinrakennusten lämmitys, ulkokatoksen lämmitys, läheisen kasvihuoneen lämmitys tai uima-altaan lämmitys. Koska laitteet tuottavat käytössä ollessaan joka tapauksessa lämpöä, sen hyödyntäminen muiden lämpölähteiden korvaamisessa riippuu lähinnä infrastruktuurista, jäähdytyksen tehokkuudesta ja lämmönsiirron vaatimasta lisäenergiasta. Mahdollinen käytettävä lisäenergia joka kuluu lämmönsiirtoon kohteeseen näkyy edelleen kokonaistehon kasvuna. Jos IT-lämpöteho käytetään pidemmän matkan päässä hyödyksi, mahdolliset siirtohäviöt vähennetään P_{repl} arvosta. Tarvitun lisäenergian ja inframuutosten myötä saavutetuille säästöille voidaan laskea hinta, jota voi verrata lämmityskustannuksiin ilman IT-lämpötehon hyötykäyttöä. Paras tapa varmistaa infrastruktuurin olemassaolo on suunnitella se valmiiksi jo konesalin rakennusvaiheessa. Muussa tapauksessa remontointi aiheuttaa pitkän käyttökatkoksen ja mahdollisesti pölyä salitiloista siivottavaksi.

Kaavan 3 päällimmäisenä ongelmana on mittauksen tarkkuus. IT-laitteiston siirrettyä tuottaman lämpönsä jäähdyttimeen (esimerkiksi vesi tai ilma), matkalla käyttökohteeseen tapahtuu häviöitä. Tämän lisäksi jäähdytysaineen lämpötila ei ehdi kohota niin korkeaksi että se olisi suoraan hyödynnettävissä kaukolämpöön, jossa vaadittu lämpötila on minimissään 80 astetta. Lämmitystehosta voidaan käyttää vain osa hyödyksi, jossa tapauksessa P_{repl} ei olisi suoraan konesalista poistettu lämpöteho. Tällöin tarvittaisiin useampia mittapisteitä kuin pelkästään konesalista saatavilla olevat teholukemat. Ottamalla SPE-kaava käyttöön konesalien ekologisuuden vertailussa voitaisiin silti saada hyödynnettyä tietojenkäsittelyn sivutuotteena syntyvää lämpöä monipuolisemmin kuin suorinta tietä ulkoilmaan johtamalla.

5 Yhteenveto

Työssä todettiin valvonnan edut toimintavarmuuden lisäämisessä ja palvelusopimusten täyttämisessä. Lähtötilanteeseen ja kehitysvaihtoehtoihin perehtymisen jälkeen valvontadatan visualisointipalvelin valittiin toteutettavaksi avoimilla ohjelmistoilla, jotta ratkaisu olisi sovellettavissa muihinkin organisaatioihin koosta riippumatta.

Olemassa olevista palveluista todettiin saatavan runsaasti mitattavaa ja valvottavaa dataa joka on hyödyntämiskelpoista sekä ylläpitäjille vikojen ennakoinnissa ja korjaamisessa, että asiakkaille lähes reaaliaikaisten tietojen saamisessa palveluiden tilasta. Tiedon visualisoimista tutkittiin ihmisen havainnointikykyyn sovittaen.

Käytettävissä olevat valvontarajapinnat käytiin läpi, sekä käytössä olleet palvelut projektin alussa. Tiedonsiirron automatisoinnissa huomioon otettavat alustaseikat sekä tietoturvallisuusnäkökulmat pohdittiin, toteutustavaksi valittiin datan puskurointi datankeruukoneille sekä keruukoneiden suorittamat ajastetut siirrot valvontapalvelimelle.

Visualisointipalvelin suunniteltiin yhteistyössä CSC:n muiden ryhmien kanssa, jotta olemassa oleva osaaminen tulisi täysimääräisesti hyödynnetyksi ja jatkokehitys olisi mahdollisimman sulavaa eri ryhmien kesken. Palvelin pystytettiin virtuaalikoneena, ja kerätty data säilöttiin eri jalostusasteillaan jatkohyödyntämistavat huomioiden.

Alkuperäisten tavoitteiden mukaan saatiin selvitettyä että CSC:n alkutilanteessa olemassa olevat valvontadatan keruujärjestelmät ovat pääosin soveltuvia toimimaan visualisointipalvelimen kanssa. Poikkeuksena näistä ovat lähinnä Windows-työasemat ja palvelimet, joiden liittäminen valvottavien järjestelmien joukkoon vaatii vielä lisätutkimusta. Myös järjestelmän alkuvaiheen pystyttämistavoite saavutettiin, siten että datalähteeksi saatiin tehonkulutus.

Tiedonkeruupaikat ja kerätyn tiedon merkitys kaipaavat systematisointia, jotta niitä voi skaalautuvasti työstää erilaisiin visualisointijärjestelmiin sekä tarjota graafien tulkitsijoille sekä datan jatkokäyttäjille. Samoin kerätyn datan muuntaminen muodosta toiseen hyötyisi systemaattisesta esittämisestä.

Koska CSC on julkishallinnon organisaatio ja valvontadata voi olla jatkohyödyntämiskelposta, harkittavaksi tulee ottaa myös datan julkaiseminen avoimena datana. Aiheesta on kirjoitettu opas ”Julkinen data - johdatus tietovarantojen avaamiseen”. Etenemisjärjestys on listata organisaatiolla olevat datavarannot sekä arvio niiden tietojen luottamuksellisuudesta (julkista, salaista, osittain salaista). Jos tehdään päätös datan avaamisesta tai käsittelystä avaamiskelpoiseen muotoon, kannattaa alussa pystyttää pilottiprojekti pienen datamäärän avaamiseksi ja kerätä siitä kokemuksia.

Teknisesti data tulee asettaa pysyvästi löydettävään osoitteeseen Internetissä koneluettavassa muodossa, kuten XML tai JSON. Mukaan tulee liittää koneellisesti luettava käyttölisenssi, joka avoimen datan osalta voi olla esimerkiksi Creative Commons 0 -lisenssi [49]. Tällöin muun muassa datan muokkaaminen, jatkojulkaisu ja kaupallinen käyttö ovat sallittuja ilman erillisiä pyyntöjä. Jatkohyödyntämistä ajatellen tarjotulle datalle tulee myös tarjota tulkintaopas. [50, 51] CSC:lle pystytetyssä järjestelmässä sekä virtamittauksen MySQL-tietokannasta tehdään välivaiheena XML-muotoinen vedos, että graafien piirtämiseen käytetystä RRDtoolista on tehtävissä XML-muotoinen vedos, jolloin palvelussa nähtyihin graafien datapisteisiin pääsee käsiksi.

Viitteet

[1] G. F. Hughes. Improved disk-drive failure warnings. *Reliability, IEEE Transactions on*, page 350, 2002. ISBN 0018-9529. Saatavissa: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1028408.

[2] H. Jin. A Case for Redundant Arrays of Inexpensive Disks (RAID). *High Performance Mass Storage and Parallel I/O:Technologies and Applications*, 2001. ISBN 9780470544839.

[3] David Teigland. Volume Managers in Linux, 2001. Saatavissa: http://www.usenix.org/event/usenix01/freenix01/full_papers/teigland/teigland_html/. Viitattu 22.05.2011.

[4] Ben Tiefert. How to convert a Western Digital "Black" drive into a "Raid Edition" drive, 2009. Saatavissa: http://www.stringliterals.com/?p=20. Viitattu 22.05.2011.

[5] Jon Tate, Gareth Coates, Ivo Gomilsek, and Andy Lewis. *Designing and Optimizing an IBM Storage Area Network*. IBM Redbooks, 2002. ISBN 9780738425313. Saatavissa: http://www.redbooks.ibm.com/abstracts/sg246419.html.

[6] Wikipedia. List of file systems, 2011. Saatavissa: http://en.wikipedia.org/wiki/List_of_file_systems. Viitattu 23.05.2011.

[7] Nicole Maloney. Oracle Unveils Next-Generation Sun ZFS Storage Appliance Product Line, 2010. Saatavissa: http://www.oracle.com/us/corporate/press/173538. Viitattu 28.04.2011.

[8] B. Callaghan, B. Pawlowski, and P. Staubach. NFS Version 3 Protocol Specification, Internet Engineering Task Force. RFC 1813 (Informational), June 1995. Saatavissa: http://www.ietf.org/rfc/rfc1813.txt.

[9] S. Shepler, B. Callaghan, D. Robinson, R. Thurlow, C. Beame, M. Eisler, and D. Noveck. Network File System (NFS) version 4 Protocol, Internet Engineering Task Force. RFC 3530 (Proposed Standard), April 2003. Saatavissa: http://www.ietf.org/rfc/rfc3530.txt.

[10] S. Shepler, M. Eisler, and D. Noveck. Network File System (NFS) Version 4 Minor Version 1 Protocol, Internet Engineering Task Force. RFC 5661 (Proposed

Standard), January 2010. Saatavissa: http://www.ietf.org/rfc/rfc5661.txt.

[11] Shane Kerr. Use of NFS Considered Harmful, 2000. Saatavissa: http://www.time-travellers.org/shane/papers/NFS_considered_harmful.html. Viitattu 29.04.2011.

[12] Suomen viestintäministeriö. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta, 2008. Saatavissa: http://www.finlex.fi/fi/esitykset/he/2008/20080048. Viitattu 22.05.2011.

[13] J. Postel. Domain Name System Structure and Delegation, Internet Engineering Task Force. RFC 1591 (Informational), March 1994. Saatavissa: http://www.ietf.org/rfc/rfc1591.txt.

[14] K. Zeilenga. Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, Internet Engineering Task Force. RFC 4510 (Proposed Standard), June 2006. Saatavissa: http://www.ietf.org/rfc/rfc4510.txt.

[15] Microsoft. Active Directory Technical Specification, 2011. Saatavissa: http://msdn.microsoft.com/en-us/library/cc223122%28v=PROT.13%29.aspx. Viitattu 23.05.2011.

[16] R. Droms. Dynamic Host Configuration Protocol, Internet Engineering Task Force. RFC 2131 (Draft Standard), March 1997. Saatavissa: http://www.ietf.org/rfc/rfc2131.txt. Updated by RFCs 3396, 4361, 5494.

[17] Alison Cartlidge, Ashley Hanna, Colin Rudd, Ivor Macfarlane, John Windebank, and Stuart Rance. *An Introductory Overview of ITIL V3.* itSMF UK, 2007. ISBN 0-9551245-8-1. Saatavissa: http://www.itsmfi.org/files/itSMF_ITILV3_Intro_Overview_0.pdf.

[18] Antti Seppälä. ITIL-viitekehyksen mukaiset palvelutuen ratkaisuprosessit, 2007. Saatavissa: ftp://www.cs.joensuu.fi/pub/Theses/2007_MSc_Seppala_Antti.pdf. Viitattu 28.04.2011.

[19] Edward Tufte. *The Visual Display of Quantitative Information.* Graphics Press, 1983. LCCN 83156861.

[20] Veijo Kyläverkko. AYY Trinet - Network Statistics, 2011. Saatavissa: http://netstat.ayy.fi/mrtg/. Viitattu 24.05.2011.

[21] Colin Ware. *Information Visualization: Perception for Design.* Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2004. ISBN 1558608192.

[22] CSC — Tieteen tietotekniikan keskus Oy. Funet Weathermap, 2011. Saatavissa: http://www.csc.fi/hallinto/funet/status/weathermap. Viitattu 24.05.2011.

[23] CSC tutuksi, 2011. Saatavissa: http://www.csc.fi/csc. Viitattu 09.05.2011.

[24] Harri Salminen. NIC.FUNET.FI archive service, 2011. Saatavissa: http://www.csc.fi/english/institutions/funet/networkservices/nic. Viitattu 09.05.2011.

[25] Thomas Goetz. It's time to redesign medical data, 2010. Saatavissa: http://www.ted.com/talks/thomas_goetz_it_s_time_to_redesign_medical_data.html. Viitattu 28.05.2011.

[26] J.D. Case, M. Fedor, M.L. Schoffstall, and J. Davin. Simple Network Management Protocol, Internet Engineering Task Force. RFC 1067, August 1988. Saatavissa: http://www.ietf.org/rfc/rfc1067.txt. Obsoleted by RFC 1098.

[27] R. Presuhn. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force. RFC 3416 (Standard), December 2002. Saatavissa: http://www.ietf.org/rfc/rfc3416.txt.

[28] U. Blumenthal and B. Wijnen. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), Internet Engineering Task Force. RFC 3414 (Standard), December 2002. Saatavissa: http://www.ietf.org/rfc/rfc3414.txt. Updated by RFC 5590.

[29] S. Waldbusser, R. Cole, C. Kalbfleisch, and D. Romascanu. Introduction to the Remote Monitoring (RMON) Family of MIB Modules, Internet Engineering Task Force. RFC 3577 (Informational), August 2003. Saatavissa: http://www.ietf.org/rfc/rfc3577.txt.

[30] C. Lonvick. The BSD Syslog Protocol, Internet Engineering Task Force. RFC 3164 (Informational), August 2001. Saatavissa: http://www.ietf.org/rfc/rfc3164.txt. Obsoleted by RFC 5424.

[31] R. Gerhards. The Syslog Protocol, Internet Engineering Task Force. RFC 5424 (Proposed Standard), March 2009. Saatavissa: http://www.ietf.org/rfc/rfc5424.txt.

[32] Andreas Rott. Self-Healing in Distributed Network Environments. *Advanced Information Networking and Applications Workshops, 2007, AINAW '07*, 2007. ISBN 978-0-7695-2847-2. Saatavissa: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4221038.

[33] Microsoft Technet. Microsoft Operations Manager 2005, 2011. Saatavissa: http://technet.microsoft.com/en-us/systemcenter/om/bb498244. Viitattu 25.05.2011.

[34] Microsoft. Background Intelligent Transfer Service, 2011. Saatavissa: http://msdn.microsoft.com/en-us/library/bb968799.aspx. Viitattu 20.05.2011.

[35] Storage Networking Industry Association. Common Internet File System (CIFS) Technical Reference, 2002. Saatavissa: http://www.snia.org/tech_activities/CIFS/CIFS-TR-1p00_FINAL.pdf. Viitattu 24.05.2011.

[36] Microsoft Technet. How SMS Uses WMI, 2011. Saatavissa: http://technet.microsoft.com/en-us/library/cc180909.aspx. Viitattu 25.05.2011.

[37] Matthew Jurgens. Check WMI Plus, 2011. Saatavissa: http://www.edcint.co.nz/checkwmiplus/. Viitattu 25.05.2011.

[38] Patrick Gosling. ssh - authorized_keys HOWTO, 2006. Saatavissa: http://www.eng.cam.ac.uk/help/jpmg/ssh/authorized_keys_howto.html. Viitattu 23.05.2011.

[39] Math Faculty. Sun/Oracle Support Changes, University of Waterloo, 2010. Saatavissa: http://www.math.uwaterloo.ca/MFCF/info/sun_oracle_changes.shtml. Viitattu 28.05.2011.

[40] Joni Nevalainen. Setting up Cacti on a RHEL Linux server, 2011. Saatavissa: http://staff.csc.fi/jnevala/help/datavis/cacti-setuplog.txt. Viitattu 25.05.2011.

[41] Kirk Bauer. *Automating UNIX and LINUX Administration.* APress L. P., 2003. ISBN 1590592123.

[42] Kevin van Zonneveld. Block brute force attacks with iptables, 2007. Saatavissa: http://kevin.vanzonneveld.net/techblog/article/block_brute_force_attacks_with_iptables/. Viitattu 28.05.2011.

[43] Mark Fontecchio. Power usage effectiveness (PUE), 2008. Saatavissa: http://searchdatacenter.techtarget.com/definition/power-usage-effectiveness-PUE. Viitattu 23.05.2011.

[44] Kurt Thearling. Data Mining and Analytic Technologies, 2010. Saatavissa: http://www.thearling.com/index.htm. Viitattu 25.05.2011.

[45] Amanda Mailer. Icinga vs. Nagios –Tabled, 2010. Saatavissa: https://www.icinga.org/2010/09/02/icinga-vs-nagios-tabled/. Viitattu 28.05.2011.

[46] Energiateollisuus ry ry. Suomen yhdistetty lämmön ja sähkön tuotanto, 2008. Saatavissa: http://www.energia.fi/fi/ajankohtaista/lehdistotiedotteet/2008/suomen%20yhdistetty%20l%C3%A4mm%C3%B6n%20ja%20s%C3%A4hk%C3%B6n%20tuotanto.html. Viitattu 25.05.2011.

[47] Teemu Muukkonen. Tieto- ja viestintätekniikan ympäristövaikutukset – haastattelututkimus konesalien sähkönkulutuksesta Suomessa. Master's thesis, TKK, 2009. Saatavissa: http://www.cse.tkk.fi/Tietoliikenne/Diplomityot/pdfs/diplomityo-Teemu_Muukkonen.pdf.

[48] C.D. Patel, R. Sharma, C.E. Bash, and A. Beitelmal. Thermal considerations in cooling large scale high compute density data centers. In *Thermal and Thermomechanical Phenomena in Electronic Systems, 2002. ITHERM 2002. The Eighth Intersociety Conference on*, pages 767 – 776, 2002. ISSN 1089-9870.

[49] Creative Commons Suomi. CC0 1.0 Yleismaailmallinen, 2002. Saatavissa: http://creativecommons.org/publicdomain/zero/1.0/deed.fi. Viitattu 25.05.2011.

[50] Antti Poikola. Julkinen data - johdatus tietovarantojen avaamiseen, 2010. ISBN 978-952-243-145-5. Saatavissa: http://www.julkinendata.fi/. Viitattu 11.05.2011.

[51] Valtionkonttori. Avoin data, 2011. Saatavissa: http://data.suomi.fi/. Viitattu 24.05.2011.