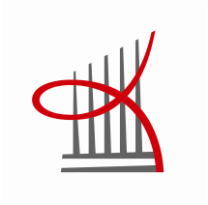


PALVELINVALVONTA JA -YLLÄPITO

Jussi Kuvaja

Opinnäytetyö
Joulukuu 2014
Tietojenkäsittelyn
koulutusohjelma
Tietoverkkopalvelut

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tietoverkkopalveluiden suuntautumisvaihtoehto

KUVAJA, JUSSI:
Palvelinvalvonta ja -ylläpito

Opinnäytetyö 42 sivua, joista liitteitä 18 sivua
Joulukuu 2014

Opinnäytetyö on tehty Barona ICT Services Oy:lle. Opinnäytetyön aiheena oli kirjoittaa virtualisoinnin perusteista sekä ohjeistus palvelinvalvontaan ja -ylläpitoon. Ohjeiden tarkoituksena oli luoda palvelinvalvonnasta kiinnostuneille ihmisille ja aloittaville järjestelmänvalvojille peruskäsitys valvontaohjelmistoista ja palvelinhälytyksistä. Opinnäytetyöhön koottiin yleisimpien palvelinhälytysten aiheuttajat ja niiden korjaustavat.

Lopputuloksena on ohjeistus yleisimpien palvelinhälytyksien ratkaisemiseksi. Ohjeistuksiin on koottu hälytysten aiheuttajat sekä selitetty kuvin ja kirjallisin ohjein, miten kyseiset hälytykset ratkaistaan.

Ohjeistuksesta tuli tarpeeksi kattava yrityksen tarkoituksiin, ja se antaa lukijalle peruskäsityksen palvelinvalvonnasta ja palvelinvalvontaohjelmista. Opinnäytetyö auttaa myös ymmärtämään virtualisoinnin perusteorian, joka on hyödyksi palvelinvalvontatyössä. Opinnäytetyössä liitteenä olevaa ohjeistusta pystytään päivittämään työntekijöiden toimesta jälkeenpäin.

Osa kuvamateriaaleista sisältää asiakasyritysten ja palvelimien nimiä, jotka ovat luottamuksellisia, joten ne on tummennettu kuvista. Yrityssalaiset järjestelmät rajattiin pois tästä raportista ja niistä tehtiin erillinen ohjeistus.

Asiasanat: palvelimet, ylläpito, monitorointi, virtualisointi.

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Option of Network Services

KUVAJA, JUSSI:
Server Monitoring and Management

Bachelor's thesis 42 pages, appendices 18 pages
December 2014

The aim of this thesis was to write a manual for server monitoring and management in addition to an overview of basics of virtualization. This thesis was commissioned by Barona ICT Services Oy. The purpose of the manual was to give a general idea of monitoring programs and server alarms for people who are interested in these subjects and for new employees of the commissioned company. The thesis includes the most common causes of server alarms and instructions about how to fix these problems.

The final result is a manual which may be used to solve problems that trigger the most common server alarms. The manual includes a written guide with images and explanations of the possible causes of the alarms and instruction about how to fix them.

The thesis gives basic idea of server monitoring and management programs. It helps to understand the basic idea of virtualization and server monitoring. The manual attached to the thesis, is for the use of the company and cab be updated by any employee whenever needed.

Some of the images contain names of companies and servers which are confidential, and are therefore censored. Company confidential systems were excluded from this thesis and are only in the separate manual attached.

Key words: servers, management, monitoring virtualization.

SISÄLLYS

LYHENTEET JA TERMIT

CPU	Central Processing Unit, keskusyksikkö
Hypervisor	Palvelimelle asennettava ohjelmisto, jonka päälle pystytään asentamaan virtuaalipalvelimia
IP	Internet Protocol
NAS	Network-Attached Storage, tallennuspalvelin mikä on suoraan yhteydessä verkkoon
SAN	Storage Area Network, verkko missä jaetaan tallennuslaitteita useammalle palvelimelle
SLA	Service Level Agreement, palvelutasosopimus
SQL	Structured Query Language, standardoitu kyselykieli
TEP	Tivoli Enterprise Portal, palvelimien hallintaohjelmisto
TIP	Tivoli Integrated Portal, ohjelmisto joka kerää palvelimilta tulleet hälytykset
Type 1 hypervisor	Type 1 hypervisor-mallissa hypervisor asennetaan suoraan palvelimeneen ilman, että palvelimella tarvitsee olla käyttöjärjestelmää.
Type 2 hypervisor	Type 2 hypervisor-mallissa hypervisor asennetaan palvelimella olevan käyttöjärjestelmän päälle.
VMware	Maailman johtavin virtualisointiohjelmistoyritys

1 JOHDANTO

Opinnäytetyö käsittelee virtualisointia sekä sisältää ohjeet palvelinvalvontaan ja -ylläpitoon. Opinnäytetyössä käydään läpi palvelinvalvontaan tarvittavia ohjelmia ja niiden toiminnallisuuksia. Opinnäytetyön ohjeet on kirjoitettu palvelinvalvonnasta kiinnostuneille ihmisille ja aloitteleville järjestelmänvalvojille. Liitteenä oleva salattu osuus, joka on poistettu lopullisesta työstä, on kirjoitettu Barona ICT Services yrityksen Monitoring Frontline -ryhmän työntekijöille.

Olen ollut töissä Monitoring Frontline -palvelinryhmässä puoli vuotta, jonka aika olen huomannut ohjeistuksien puutteellisuuden. Ohjeiden löytäminen on ollut aikaa vievää ja hankalaa. Aikaisemmin ohjeita oli useassa eri lähteessä ja niiden etsiminen tuotti uusille työntekijöille vaikeuksia. Tästä syystä aloin kokoamaan ohjeita ja toimintamalleja opinnäytetyöhöni. Opinnäytetyön teoriaosuudessa keskityin kirjoittamaan virtualisoinnista, palvelinvalvonnasta ja niiden osa-alueista. Virtualisointi liittyy isolta osin myös palvelinvalvontatyöhön, koska suurin osa valvottavista palvelimista on virtuaalipalvelimia.

Opinnäytetyön tavoitteena on koota kattavat ja helposti ymmärrettävät ohjeet palvelinvalvonnasta kiinnostuneille ihmisille sekä Monitoring Frontlinen -ryhmän uusille työntekijöille. Myös kokeneemmat työntekijät pystyvät tarkistamaan työtavat ohjeista. Opinnäytetyön tarkoituksena on helpottaa uusien työntekijöiden perehdyttämistä ja työn aloittamista. Liitteenä olevaa ohjetta pystytään myös päivittämään ja muokkaamaan helposti yhteen paikkaan.

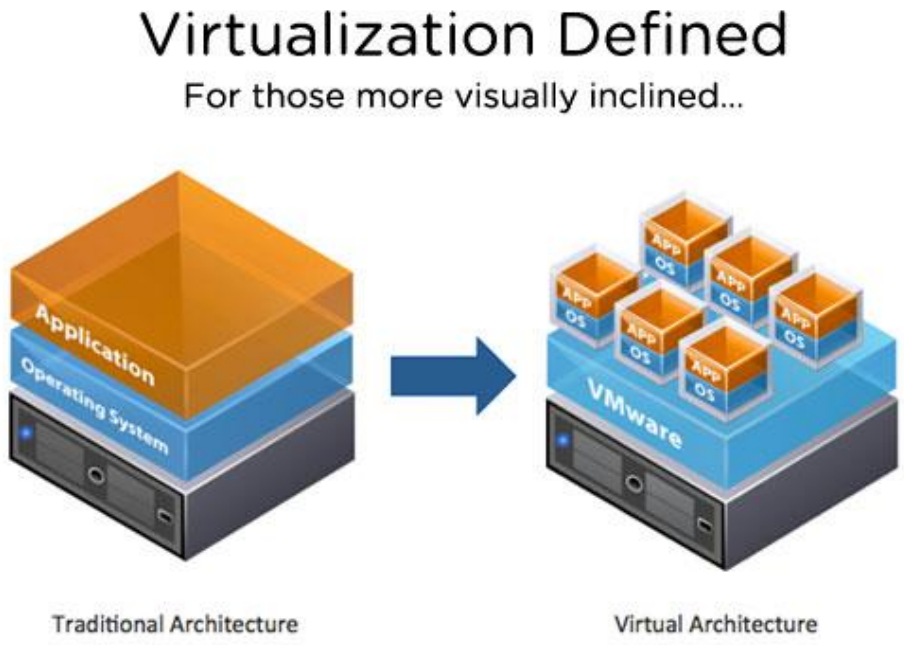
2 VIRTUALISOINTI

2.1 Palvelinkeskusten synty

Tiedonjako on mullistunut viimeisen 30 vuoden aikana valtavasti. 1980-luvulla suurin osa työtavoista perustui paperiseen arkistointiin ja kommunikointiin. Tietotekniikkaa käytettiin vain esimerkiksi palkanlaskentaan ja tilinpitoon. Nykyään kuitenkin suurin osa järjestelmistä toimii tietokoneilla. Tätä muutosta on edesauttanut Internetin globalisoituminen ja yritysten halu kommunikoida asiakkaidensa kanssa reaaliajassa. Tämän tuloksena palvelinkeskukset tarvitsevat suuren määrän palvelimia ja isot tilat palvelinkeskuksille. (Golden 2008, 13.)

2.2 Mitä on virtualisointi?

Virtualisointi tarkoittaa käytännössä yhden fyysisen koneen prosessorin, muistin, kiintolevyn tai verkon jakamista yhdelle tai useammalle virtualikoneelle. Virtualisointi jakaa tai erottaa fyysisen koneen laitteiston ominaisuudet käyttöjärjestelmästä. Yksi osa käyttöjärjestelmää tukee yhtä osaa ohjelmistoa tai sovellusta. Virtualisessa ympäristössä yhdellä fyysisellä koneella pyörii sovellus, hypervisor, joka erottaa koneen fyysiset ominaisuudet, jotta ne voidaan jakaa usealle virtuaalikoneelle (kuva 1). Jokainen näistä virtuaalikoneista voi toimia eri käyttöjärjestelmällä, jonka ei tarvitse olla sama kuin fyysisen koneen käyttöjärjestelmä, johon virtuaalikoneet on asennettu. Virtuaalikone, joka on asennettu fyysiseen koneeseen, ei ole tietoinen siitä, että se saattaa jakaa fyysisen koneen ominaisuuksia yhden tai useamman virtuaalikoneen kanssa. Jokainen virtuaalikone luulee olevansa suoraan yhteydessä fyysisen koneen laitteistoon. Yhden virtuaalikoneen kaatuminen ei vaikuta muihin virtuaalikoneisiin. (Golden 2008, 10–11.)



KUVA 1. Virtualisoinnin määritelmä (VMware 2014b)

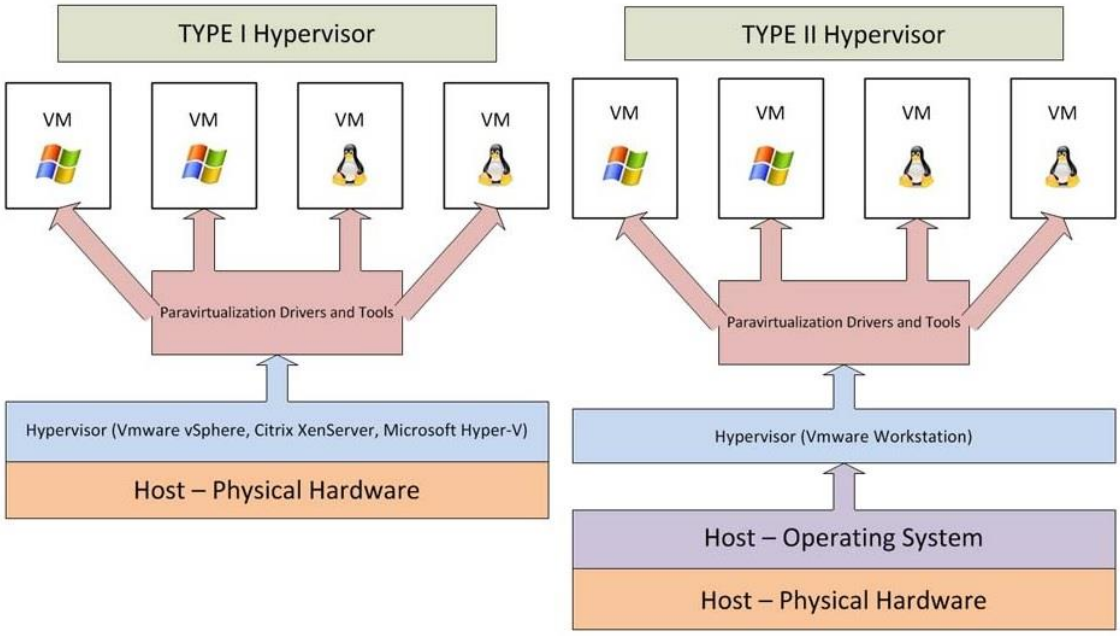
2.3 Miksi virtualisoida?

Yksi tärkeimpiä syitä virtualisoinnin suosioon on kustannusten alentaminen. Koska virtualisointi vähentää tarvittavien fyysisten servereiden määrää, alentaa se täten käyttökustannuksiakin. Koska palvelinkeskukset maksavat miljoonia euroja, palvelinvirtualisointi säästää merkittävän määrän rahaa. Palvelinvirtualisointi ei säästä rahaa vain fyysisten laitteiden hankinnasta vaan myös energiakuluista sekä palvelinylläpitokustannuksista. (Golden 2008, 15.)

2.4 Hypervisor

Hypervisor on ohjelmisto, joka valvoo isäntäkoneen ominaisuuksien jakamisen virtuaalikoneiden kesken. Hypervisor voidaan asentaa isäntäkoneelle kahdella eri tavalla. Tyypin 1 hypervisor tilanteessa hypervisor asennetaan suoraan fyysiseen koneeseen ilman käyttöjärjestelmää (kuva 2). Tämä tarkoittaa sitä, että ensimmäinen asia, mitä koneelle asennetaan, on hypervisor. Tyypin 2 hypervisor puolestaan asennetaan jo käytössä olevan käyttöjärjestelmän päälle. Vaikka tyypin 2 hypervisorissa on niin sanottu pysähdys

koneen fyysisen laitteiston ja hypervisorin välillä, ei se nykyaikaisilla laitteilla lisää viivettä. (Kleyman 2012.)



KUVA 2. Tyypin 1 ja 2 hypervisor -malli (Kleyman 2012, muokattu)

2.5 Virtualisoinnin huonot puolet

Matthew Garret, Linux-hakkeri ja pilvipalveluiden ekspertti (Vaughan-Nicholson 2014), sanoo että yksi suurimpia riskejä virtualisoinnissa on hypervisor. Yhden hypervisorin alla voi olla kymmeniä virtuaalikoneita, joista esimerkiksi yhdellä käsitellään luottamuksellisia käyttäjätietoja ja rahansiirto-operaatioita ja toisella puolestaan toimii huonosti koodattu verkkosivusto. Virtuaalikone voidaan kaapata tämän huonosti koodatun verkkosivun kautta, mikä aiheuttaa riskin myös muille samassa hypervisorissa oleville koneille. Hypervisorin huono puoli on siinä, että virtuaalikoneiden tietoturva on rakennettu suojelemaan ulkoa tulevat uhat, mutta ei hypervisorista päin tulevia. Garretin mukaan on vain ajan kysymys, koska ensimmäiset hypervisorin kautta tulevat hyökkäykset tapahtuvat. Hän sanoo, että jos joku saa haltuunsa hypervisorin, peli loppuu siihen, koska olemme kaikki uhan alla. Virtuaalikone voi olla täydellisesti suojattu mutta jos hy-

pervisor ei ole suojattu, virtuaalikoneen suojauksella ole mitään merkitystä. (Vaughan-Nicholson 2014.)[1]

Toinen virtualisoinnin huonoista puolista on alkuinvestoinnin hinta. Virtualisointiohjelmien ja lisenssien ostaminen palvelimille on erittäin kallista, minkä vuoksi virtualisointia tulee pitää pitkän ajan sijoituksena. Pitkässä juoksussa kuitenkin vähenevät sekä palvelimen ylläpitokustannukset että palvelinkeskuksen sähkö- ja tilakustannukset.

[1] ”Once someone gets to the hypervisor then it's game over, everyone can be compromised. You can have a perfectly secure VM, but if the hypervisor isn't secure, than your security doesn’t matter.” (Vaughan-Nicholson 2014.)

3 VIRTUALISOINNIN TAVAT

3.1 Palvelinvirtualisointi

Palvelinvirtualisointi, joka on myös yleisin virtuaalisointitapa, jakaa fyysisen palvelimen resurssit virtuaalipalvelimille. Yhdelle fyysiselle palvelimelle asennetaan yksi tai useampi virtuaalipalvelin, joista jokainen virtuaalipalvelin luulee, että se on yksinoikeutettu fyysisen koneen resursseihin. Todellisuudessa virtualisointiohjelma hypervisor kontrolloi virtuaalipalvelimen pääsyä fyysisen koneen laitteistoon. Yhdelle fyysiselle palvelimelle voidaan asentaa useita virtuaalipalvelimia, jotka voivat käyttää montaa eri käyttöjärjestelmää keskenään. Jokainen virtuaalipalvelin toimii itsenäisesti, ja jos joku näistä palvelimista kaatuu tai käynnistetään uudelleen, ei se vaikuta muihin palvelimiin. (Golden 2008, 21.)

Kun fyysiselle palvelimelle asennetaan useita virtuaalipalvelimia, tulevat fyysisen palvelimen resurssit paremmin hyödynnettyä. Useat palvelimet hyödyntävät vain 15 prosenttia palvelimen resursseista, mikä on erittäin huono hyötysuhde (VMware 2014a). Jos yhdelle fyysiselle palvelimelle asennettaisiin viisi tai kuusi virtuaalipalvelinta, tulisi palvelimen resurssit huomattavasti paremmin käyttöön. Samalla vähentyvät palvelinhuolto- ja ylläpitokustannukset.

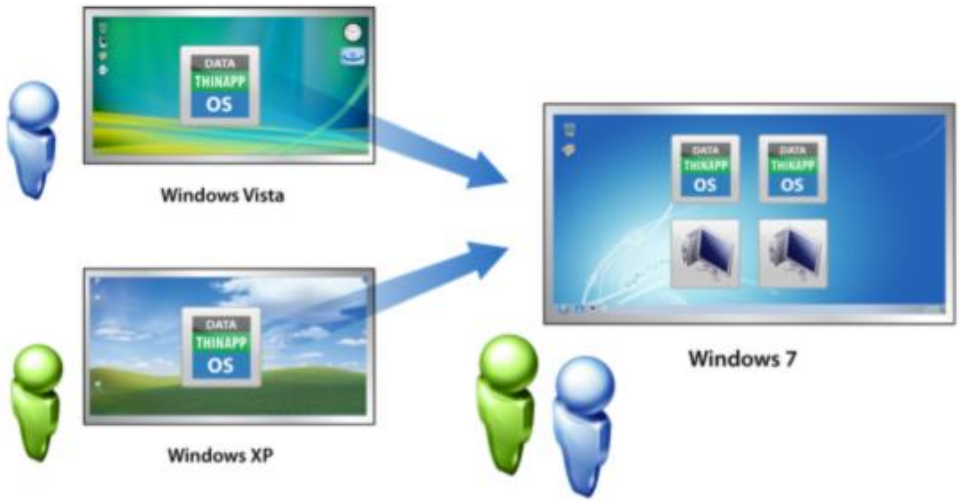
3.2 Työpöytävirtualisointi

Työpöytävirtualisoinnissa luodaan käyttäjälle henkilökohtainen virtuaalikone palvelinkeskukseen. Tällä virtuaalikoneella on valmiiksi asennettu käyttöjärjestelmä, johon käyttäjä pääsee käsiksi omalla päätelaitteellaan. Tämä vähentää fyysisten koneiden käyttökustannuksia, koska samalla fyysisellä koneella voi olla monta käyttäjää. Fyysisen koneen ei myöskään tarvitse olla niin tehokas, koska ohjelmistojen käyttö tapahtuu palvelimen päässä, eikä se kuormita käyttäjän fyysistä konetta. Samalla myös yrityksen energiakustannukset pienenevät. (Golden 2008, 17.)

Työpöytävirtualisointi vähentää myös palvelimen ylläpitokustannuksia, koska uuden virtuaalikoneen voi luoda muutamassa minuutissa. Uusien ohjelmistojen asentaminen ja ohjelmien päivittäminen käyttäjän koneelle tapahtuu huomattavasti helpommin. Samalla käyttäjän omien ohjelmien asentaminen vaikeutuu, sillä virtuaalikoneella ei ole CD-asemaa eikä USB-porttia, joita hän voisi käyttää. Käyttäjän ei myöskään tarvitse odottaa tunteja IT-tukea paikalle, sillä tukihenkilöllä on välitön yhteys virtuaalikoneeseen palvelimen kautta. Työpöytävirtualisointi sopii varsinkin uusien ohjelmistojen testaamiseen, sillä se on eristetty muista yrityksen koneista. Työpöytävirtualisointi myös vapauttaa työntekijän työpisteeltään, sillä hän voi käyttää virtuaalikonetta miltä tahansa fyysiseltä koneelta. Tämä tietenkin riippuu työpaikan turvamäärityksistä, sillä joissakin tapauksissa ulkopuolisesta verkosta ei sallita pääsyä yrityksen verkkoon. (Golden 2008, 17.)

3.3 Ohjelmistovirtualisointi

Ohjelmistovirtualisointi erottaa ohjelmiston koneen käyttöjärjestelmästä ja muista ohjelmista sekä vapauttaa ohjelmistot käyttöjärjestelmäriippuvuudesta ja ohjelmistoasennuksista. Tämä tarkoittaa esimerkiksi sitä, että Windows 7 -käyttöjärjestelmällä voidaan suorittaa Windows XP -käyttöjärjestelmälle tehtyjä ohjelmia (kuva 3). Ohjelmistovirtualisoinnilla pystytään myös suorittamaan ohjelmia, jotka eivät normaalisti toimisi samalla käyttöjärjestelmällä yhtä aikaa. (SimplicIT 2012.)



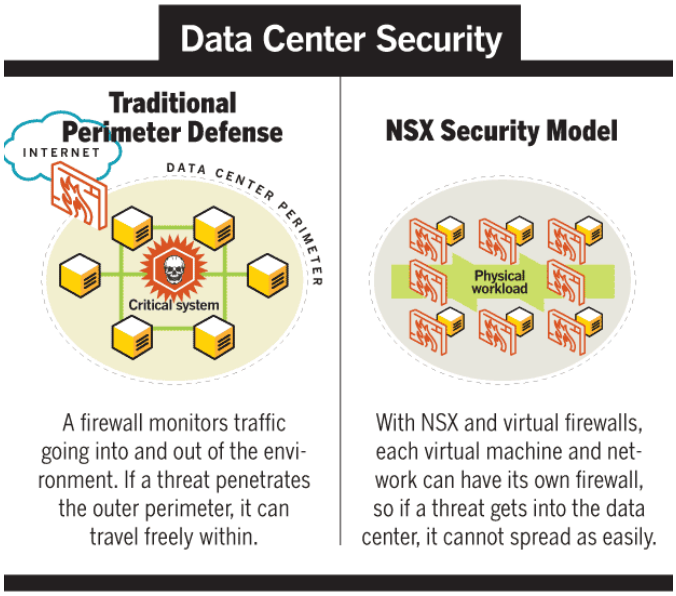
Kuva 3. Ohjelmistovirtualisointi eri käyttöjärjestelmillä (SimplicIT 2012)

Ohjelmistovirtualisointiin on kaksi eri tapaa: etäohjelmisto tai ohjelmiston suoratoisto. Etäohjelmiston tapauksessa ohjelma pyörii palvelimella, johon käyttäjä yhdistää. Etäohjelmisto käynnistetään esimerkiksi työpöydän pikakuvakkeen kautta, jonka jälkeen ohjelmisto näyttäisi käynnistyvän kuin paikallisetkin ohjelmat, mutta todellisuudessa ohjelmistoa käytetään palvelimelta. Etäohjelmiston hyviin puoliin kuuluvat käyttöjärjestelmäriippumattomuus ja yhteensopivuus käyttäjän tietokoneella olevien muiden ohjelmien kanssa. Palvelujen saatavuus myös paranee, sillä jos palvelin syystä tai toisesta kaatuu, voidaan palvelut siirtää toiselle palvelimelle hetkessä. Ohjelmistopäivitysten asentaminen yksinkertaistuu, koska enää ei tarvitse päivittää kaikkia yrityksen koneita, vaan riittää että palvelimen ohjelmisto päivitetään. Etäohjelmiston heikkoutena on jatkuvan verkkoyhteyden tarve. Jos yhteys katkeaa, loppuu myös etäohjelmiston käyttö, koska palvelimeen, jolla ohjelma pyörii, ei saada enää yhteyttä. (Rouse, M. 2011.)

Ohjelmiston suoratoistossa, toisin kuin etäohjelmistossa, tarvittava ohjelma suoritetaan käyttäjän koneella. Kun käyttäjä haluaa aukaista ohjelmiston, ladataan siihen tarvittavat komponentit palvelimelta. Tässä tapauksessa palvelimelta ladataan vain tarvittavat osat ohjelmiston käynnistämistä varten ja loput ohjelmasta ladataan taustalla. Latauksen valmistuttua voidaan ohjelmistoa käyttää ilman verkkoyhteyttä. Suoratoistossa ohjelmat eristetään käyttöjärjestelmästä sekä muista ohjelmista, mikä takaa yhteensopivuuden. Suoratoisto-ohjelman voi jättää tietokoneelle seuraavaa kertaa varten tai se voidaan automaattisesti poistaa ohjelman sulkeuduttua. (Rouse, M. 2011.)

3.4 Verkkovirtualisointi

Verkkovirtualisointi luo virtuaalisen verkon kahden tai useamman palvelimen välille. Verkkovirtualisoinnissa luodaan ohjelmistopohjainen looginen verkko, jossa toimivat esimerkiksi kytkin, reititin, palomuuri ja kuormantasaus aivan kuin normaalissakin verkossa. Verkkovirtualisoinnissa tärkeimpänä tekijänä on tietoturva, sillä virtuaaliverkkoon voidaan asentaa useita virtuaalipalomuureja. Näille palomuureille voidaan asentaa estoja helposti, ilman että yrityksen tarvitsisi ostaa uusia fyysisiä palomuureja tai muuttaa vanhojen palomuurien asetuksia (kuva 4). Nämä palomuurit voidaan laittaa valvomaan sekä sisäverkkoon tulevaa ja lähtevää liikennettä että sisäistä liikennettä.
(Kusnetzky, D. 2011, 23–26.)



Kuva 4. Perinteisen ja virtuaalisen palomuurin ero (Butler 2014)

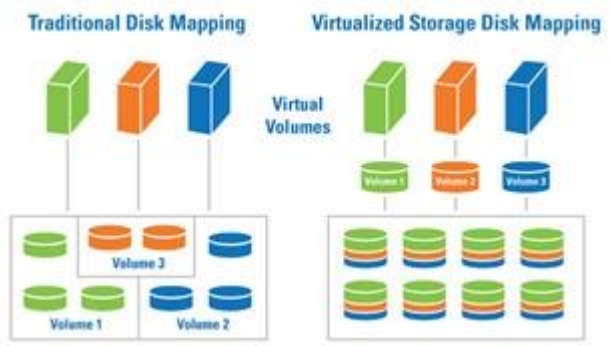
Virtuaaliverkko voidaan eristää sisäisesti siten, että verkossa vain tietyt koneet näkevät tietyt palvelimet. Tämä vähentää huomattavasti verkon haavoittuvuutta, sillä jos verkkoon tulee haittaohjelma, ei se näe kaikkia verkkoon kuuluvia laitteita. Perinteisessä verkkoympäristössä on vain ulkoinen palomuuri, joka valvoo sisäverkkoon tulevaa ja sieltä lähtevää liikennettä. (Kusnetzky 2011, 25–26.)

Verkon luotettavuus myös paranee virtualisoinnissa, sillä virtuaaliverkkoon voidaan liittää kaksi tai useampi verkontarjoaja. Näin yhden verkon kaatuminen ei kaada koko yrityksen verkkoa. Jotkut yritykset haluavat pitää tietyt arkaluontoiset tiedostot ja palvelut erillisillä palvelimilla, joihin pääsee käsiksi vain tietyt käyttäjät tai palvelut. Tämä onnistuu helposti virtualisoinnilla ilman erillisen fyysisen verkon ja palvelimen käyttöönottoa. (Kusnetzky 2011, 25.)

3.5 Tallennusvirtualisointi

Tallennusvirtualisointi on useamman fyysisen palvelimen kiintolevyjen yhdistämistä yhdeksi tai useammaksi virtuaaliseksi tietovarannoksi. Yhdistetty tietovaranto näkyy käyttäjälle tai toiselle palvelimelle yhtenä kiintolevynä tai asemana. Tästä menetelmästä käytetään nimitystä Storage Area Network (SAN). Tallennusvirtualisointi jakaa tallennuskapasiteetin usean eri kiintolevyn välillä. Tämä nopeuttaa tiedon lukua ja kirjoittamista kiintolevylle lisäten samalla yksittäisen fyysisen palvelimen suorituskykyä. Tavanomaisessa tiedontallennusprosessissa yksittäinen palvelin saattaa ylikuormittua ruuhkaisimpina aikoina, kun taas tallennusvirtualisoinnissa hajautetut virtuaalikiintolevyt helpottavat palvelimia selviämään ruuhkatilanteista. (Rouse, M. 2014.)

Tiedon hajauttaminen ja kopioiminen usealle virtuaalikiintolevylle parantaa myös vikasietoisuutta, koska yhden fyysisen palvelimen kaatuminen ei aiheuta käyttökatkoksia. SAN-järjestelmää edeltänyt, vieläkin useassa paikassa käytössä oleva, Network Attached Storage (NAS) on SAN-järjestelmään verrattuna erittäin kömpelö. Jos NAS-järjestelmän käyttäjän pitäisi saada lisää tallennustilaa palvelimellensa, hänen pitää ostaa uusi kiintolevy, kun taas SAN-järjestelmässä hän voisi ottaa toiselta palvelimelta jääneen ylimääräisen tallennustilan käyttöönsä (kuva 5). (GyGem 2008.)



Kuva 5. NAS ja SAN -varastoinnin malli (One Cloud Solutions 2013)

Eri käyttöjärjestelmät, kuten Windows, Linux tai Unix, käyttävät erilaisia ohjelman suoritus-, tiedontallennus- ja noutomekanismeja, mikä ei aiheuta ongelmia tallennusvirtualisoinnissa, joka on käyttöjärjestelmäriippumaton. Tiedontallennusvirtualisoinnissa kaikki käyttöjärjestelmät voivat käyttää samaa tallennuslaitetta ja niiden tiedostoja. (Kusnetzky 2011, 32.)

4 PALVELINVALVONTA JA -YLLÄPITO

4.1 Palvelinvalvonta

Palvelinvalvonnan tarkoituksena on seurata aktiivisesti palvelinten tilaa ja ennakoida mahdollisia ongelmia palvelimilla. Palvelimella valvottaviin asioihin kuuluvat yleensä verkkoyhteydet, levyasemat, prosessorin sekä muistin käyttö ja palvelimella olevat ohjelmistot ja palvelut. Yritykselle kriittisten palveluiden, kuten sähköpostin tai tietokantojen toimimattomuus, saattaa aiheuttaa koko yrityksen liiketoiminnan pysähtymisen. Joillekin yrityksille vain muutaman tunnin liiketoiminnan estyminen aiheuttaa kymmenien tuhansien eurojen menetyksen ja jopa sakkoja asiakasyrityksiltä. Tämän takia palvelinvalvonnan pitää olla ennaltaehkäisevää, tehokasta ja luotettavaa.

Ennaltaehkäisevillä toimilla voidaan esimerkiksi lisätä palvelimen täyttyville levyasemille lisää tallennustilaa tai ylikuormittuville palvelimille lisää muistia ja prosessoreita. Ennaltaehkäisevillä toimilla voidaan myös poistaa levytilaa tai prosessoreita vähemmän käytössä olevilta palvelimilta. Näillä toimilla saadaan palvelinympäristö optimoitua. Virtuaalisessa ympäristössä palvelinten optimointi on huomattavasti helpompaa kuin niin sanotussa fyysisessä ympäristössä. Virtuaalisessa ympäristössä voidaan muutamalla klikkauksella antaa palvelimelle lisää levytilaa tai prosessoreita, kun taas fyysisessä ympäristössä jouduttaisiin lisääminen tehdä käsin konesalissa.

4.2 Valvontaympäristö

Työnantajani valvontaympäristö koostuu muutamasta konesalista. Osa näistä konesaleista on hajautettu eri puolille Suomea. Tämä on tehty sen takia, ettei esimerkiksi tulipalo tai verkkoyhteyksien katkeaminen aiheuta koko yrityksen verkon katkeamista tai tietojen menettämistä. Jotkut yritykset myös haluavat, että varmuuskopiot sijaitsevat maantieteellisesti eri paikoissa. Suomessa suurimpana riskinä voidaan pitää tulipaloa, mutta esimerkiksi Amerikassa riskeinä ovat myös pyörremyrskyt ja maanjäristykset.

Jokaisessa työnantajani palvelinkeskuksessa on sisällä kymmeniä palvelimia. Suurimpaan osaa näistä palvelimista on asennettu kymmeniä virtuaalipalvelimia. Isoimmat palvelinkeskukset sisältävät noin tuhat virtuaalipalvelinta, joten valvottavia palvelimia on runsaasti. Melkein kaikki palvelinhälytykset liittyvät virtuaalipalvelimiin, mutta aina silloin tällöin fyysiset palvelimet hälyttelevät. Nämä hälytykset johtuvat yleensä palvelimella olevien fyysisten osien rikkoutumisesta, mikä vaatii rikkoutuneen osan vaihtamisen paikan päällä.

4.3 Valvontaohjelmistot

Palvelinvalvonta ja -ylläpito on kehittynyt suurin harppauksin viimeisimpien vuosikymmenien aikana. Suurimpana syynä tähän on valvontaohjelmien kehittyminen ja virtualisointi. Nykyaikaiset valvontaohjelmat tuovat palvelimilla toimivien ohjelmien tapahtumat reaaliaikaisesti järjestelmävalvojalle. Valvontaohjelmat antavat myös tarkan kuvan palvelimen kuormituksesta ja mahdollisista ongelmista, esimerkiksi verkkoyhteyksistä tai levyasemien täyttymisistä. Nämä asiat edesauttavat mahdollisten ongelmien ennakoimista ja vianselvitystä. Nykyaikainen palvelinympäristö voi kattaa tuhansia palvelimia, joten valvontaohjelmiston pitää olla helppokäyttöinen ja luotettava.

Omassa työssäni käytän IBM Tivoli Integrated Portal, IBM Tivoli Enterprise Portal ja VMware vSphere Client -ohjelmistoja. Kyseiset ohjelmistot ovat helppokäyttöisiä, joten järjestelmävalvojan ei tarvitse käydä viikkoja kestävää koulutusta läpi oppiakseen niiden peruskäytön. Seuraavissa kappaleissa käydään läpi näiden ohjelmien perustoiminnot ja valikot.

5 VALVONTATYÖKALUT

5.1 Tivoli Integrated Portal

Jokaiseen työnantajani valvottavaan palvelimeen on asennettu ”Windows Monitoring Agent”, joka valvoo palvelimen toimintaa ja mahdollisissa vikatilanteissa generoi hälytyksen TIP:iin. TIP:stä näkee aktiiviset ja käsittelyssä olevat hälytykset. Jokainen yritys voi muokata TIP-ohjelmaa ja siihen kuuluvia valvontaryhmiä omien tarpeidensa mukaan, joten alla olevien ohjeiden nimet ja valikot vaihtelevat yrityksestä riippuen.

Monitoring Frontline 24x7 -hälytysikkunan saa auki Monitoring-alasvetovalikosta (kuva 13. numero 1). Samasta valikosta löytyvät Monitoring Frontline 24x7 Handled, Monitoring Frontline, Monitoring Frontline Handled -valikot. Monitoring Frontline 24x7 -valikko kannattaa asettaa aloitussivuksi ”Omat aloitussivut” -valikosta, jolloin kyseinen ikkuna aukeaa aina ohjelman käynnistyessä välilehteen (kuva 6. numero 2).

Kuva 6. Tivoli Integrated Portal – Monitoring Frontline -ikkuna

Kuvassa 6, kohdassa kolme on TIP-hälytysrivi, jonka selitykset on kerrottu alla olevassa taulukossa yksi.

Taulukko 1. TIP-hälytysrivien selitykset (Tossavainen 2014, muokattu)

Acknowledged (suomeksi äkkäys)	Kun hälytys muodostuu, on se automaattisesti ”No”, kunnes hälytyksestä tehdään tiketti tai hälytys äkätään, jolloin se muuttuu ”Yes”.
Count	Montako kertaa hälytys on toistunut
First Occurrence	Milloin hälytys muodostui ensimmäisen kerran
Last Occurrence	Milloin hälytys uusiutui viimeisimmän kerran
Node	Miltä palvelimelta hälytys on muodostunut, esim. nimi.yritys.100.local. Ensimmäisenä on palvelimen nimi. Toisena on asiakkaan nimi. Kolmantena on site, tässä tapauksessa 100. Tämä kertoo miltä siteltä kyseistä palvelinta hallitaan.
Summary	Hälytyksen syy
ENFServiceType	Kertoo hälytyksen palveluntasosta
ITMSitType	S eli Sample hälyä ei saa poistaa, sillä nämä hälytykset kuittautuvat itsestään, kun tilanne korjautuu. P eli Pure Eventti pitää poistaa, kun hälytyksestä on tehty tiketti ja se on hoidettu, poisto tapahtuu ”Monitorin Frontline 24x7 Handled” -välilehdeltä. Jos Pure Eventtiä ei poista, ei uudet hälytykset samasta asiasta muodostu TIP:iin.
EnfTicketRef	Kun hälytyksestä tehdään tiketti, tulee tiketinnumero kyseiseen kenttään.
ENFComment	Vapaa kommenttikenttä
EnFFamily	Kertoo mikä käyttöjärjestelmä tai verkkolaite on kyseessä
ENFLocation	Kertoo missä palvelinkeskuksessa kyseinen palvelin sijaitsee
OwnerUID	Kertoo kuka on tehnyt hälytyksestä tiketin
Customer	Asiakkaan nimi
EnfoNode	Kertoo palvelimella olevan agentin nimen
Identifier	Valvonnan tekninen situaatiotunniste

Kuvan 6 kohta neljä kertoo hälytysten määrän. TIP päivittyy 60 sekunnin välein ja kuvan 6 kohta viisi kertoo kuinka monta uutta hälytystä on tullut, montaako hälytystä on päivitetty ja moniko hälytys on poistunut automaattisen päivityksen jälkeen. Kuvan 6 kohta kuusi kertoo sekunteina, kuinka paljon aikaa on seuraavaan päivitykseen.

Hälytystä tuplaklikkaamalla saadaan auki yksityiskohtaiset tiedot hälytyksestä ja palvelimesta. Kun hälytysriviä klikkaa hiiren oikealla napilla aukeaa valikko, jossa on useita eri toimintoja hälytyksen käsittelyyn. Alla olevassa taulukossa kaksi on listaus tärkeimmistä toiminnoista.

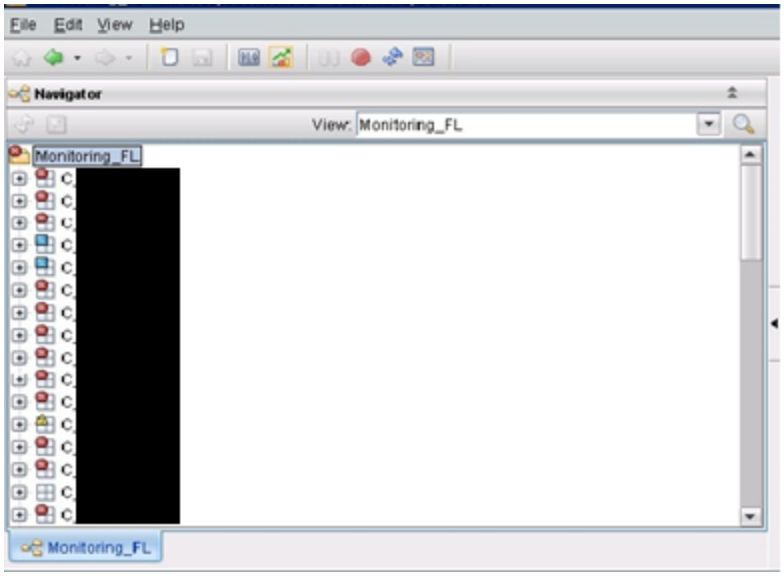
Taulukko 2. TIP-toiminnot

Acknowledge	Hälytyksen kuittaaminen
De-Acknowledge	Hälytyksen asettaminen käsittelemättömäksi
Delete	Hälytyksen poisto, mitä käytetään Pure-hälytyksissä.
Ping	Hälytyksen kohdepalvelinta voidaan pingata, joko koneelta (host) tai palvelimelta (server).
Create Ticket	Luo tiketin Monitoring Classic -jonoon.
GroupeGreatTicket	Tällä toiminnolla voidaan niputtaa hälytyksiä yhden tiketin alle maalaamalla halutut hälytykset.
CreateTicketOnDuty	Luo tiketin Monitoring OnDuty -jonoon.
CreateTicketFrontline	Luo tiketin Monitoring Frontline -jonoon.
SetENFTicketRef	Tällä voi niputtaa useita hälytyksiä maalaamalla ne ja kirjoittamalla tikettinumeron.
SetENFComment	Tällä voidaan kommentoida aktiivisia hälytyksiä.
ViewAlertHistoryToNode	Tällä voidaan katsoa hälytyshistoria kyseisellä palvelimella.
Haku	Aukaisee hakupalkin, johon kirjoittamalla palvelimen nimen voidaan hakea palvelimella olevia aktiivisia hälytyksiä.

5.2 Tivoli Enterprise Portal

Tivoli Enterprise Portal (TEP) on palvelinylläpidon yksi tärkeimmistä työkaluista. TEP-ohjelmaa käytetään palvelimella olevien pysähtyneiden ohjelmien käynnistämiseen ja sieltä näkee esimerkiksi palvelimilla olevien asemien täyttöasteet, prosessorin kuorman ja palvelimen ohjelmat.

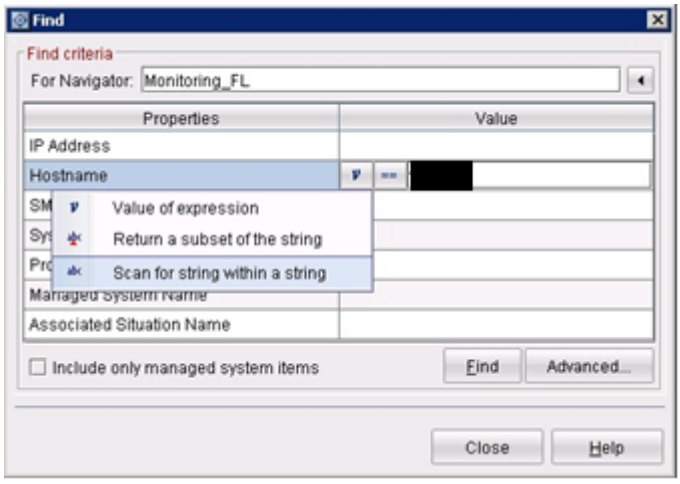
Aukaistuasi TEP-ohjelman löytyy vasemmasta laidasta ”Monitoring_FL”-kansion alta lista asiakkaista ja heidän palvelimistaan (kuva 7). Palvelimen voi hakea käsin painamalla ”+” -nappia halutun asiakkaan kohdalla tai painamalla suurennuslasia.



Kuva 7. TEP – Monitoring_FL-kansio

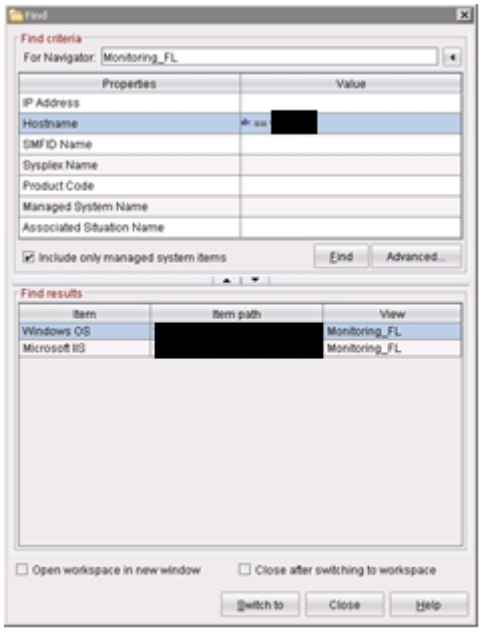
Palvelimien haku TEP:ssä tapahtuu seuraavien olevien ohjeiden mukaisesti (kuva 8; kuva 9).

1. Laita ruksi ”Include only managed system items” -valintaan
2. Paina V-kirjainta ja valitse ”Scan for string within a string”
3. Syötä palvelimen nimi ”Hostname ”-kenttään
4. Paina “Find”



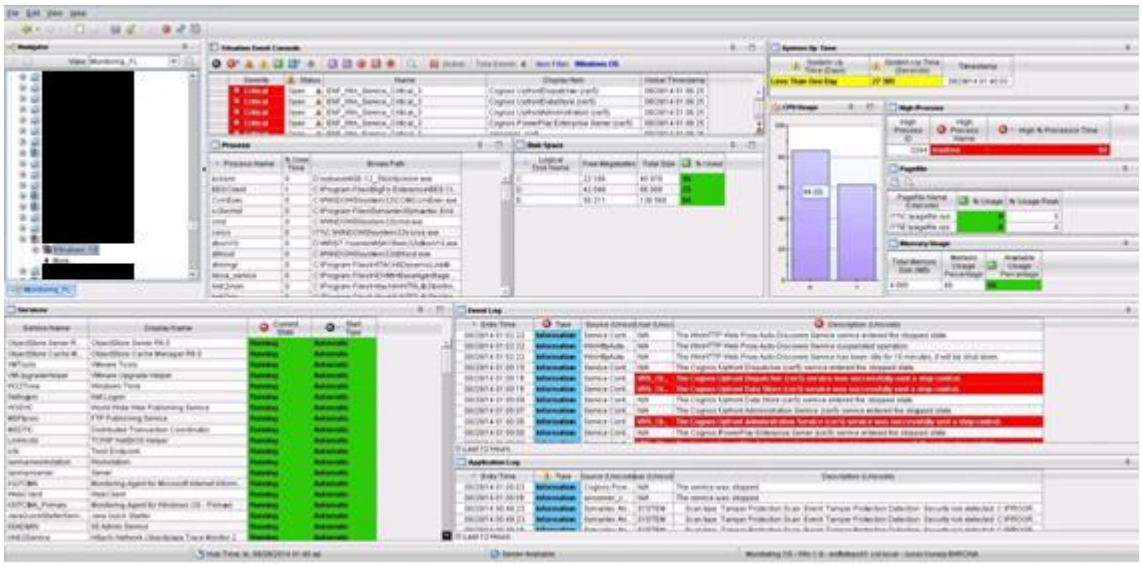
Kuva 8. Palvelimien haku TEP:ssä

Aukeavasta valikosta valitaan Windows OS tai Linux OS palvelimesta riippuen. Valinta voidaan tehdä tuplaklikkaamalla tai painamalla Enter-näppäintä.



Kuva 9. Hakutulokset TEP:ssä

Palvelimen latauduttua ruutuun, pitäisi näkymän olla kuvan 10 mukainen.



Kuva 10. TEP:n yleisnäkymä

Alla olevassa taulukossa on kerrottu TEP:n ikkunoiden selitykset (taulukko 3).

Taulukko 3. TEP:n ikkunoiden selitykset

Situation Event Console	Aktiiviset hälytykset, palveluiden nimet ja aikaleimat
Process	Palvelimilla päällä olevat prosessit
Disk Space	Palvelimen levyt ja niiden täyttöasteet
System Up Time	Kuinka kauan palvelin on ollut ylhäällä edellisestä uudelleenkäynnistämisestä
CPU Usage	Montako prosessoria palvelimella on ja niiden prosentuaalinen käyttö
High Process	Mikä ohjelma vie eniten prosessoritehoja
Pagefile	Pagefilen käyttö ja niiden sijainnit
Memory Usage	Muistin koko ja vapaana olevan muistin määrä
Services	Palvelimella olevat palvelut, niiden tilat ja käynnistystapa
Event Log	Palvelimen System log, viimeisen vuorokauden ajalta
Application Log	Palvelimen Application Log viimeisen vuorokauden ajalta. Viemällä hiiren tapahtuman päälle aukeaa tarkempi kuvaus tapahtumasta.

5.3 VMware vSphere Client

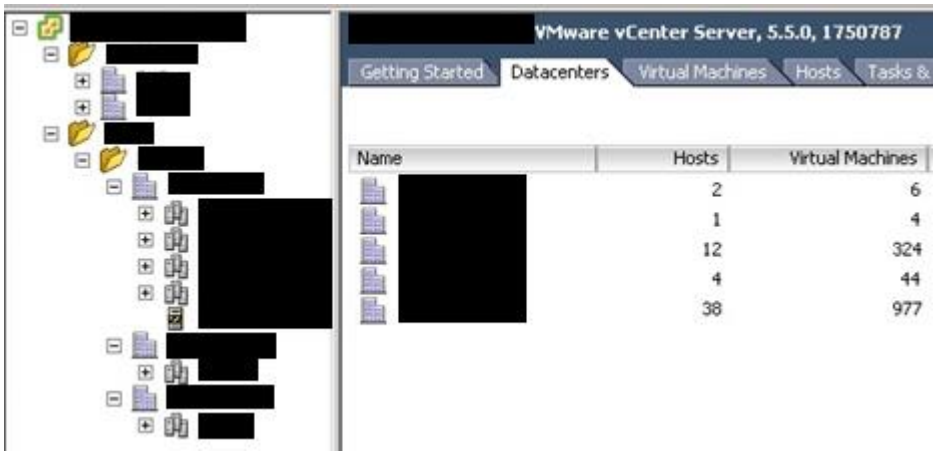
VMware vSphere Client on virtualisointiohjelmisto, jolla pystytään luomaan sekä muokkaamaan virtuaalipalvelimia ja -koneita. Suuri osa valvottavista palvelimista on virtuaalisia, joten kyseinen ohjelma on erittäin hyödyllinen palvelinten ylläpidossa. Ohjelman suurin hyöty, Monitoring Frontline -ryhmälle, tulee esille palvelinten uudelleenkäynnistyksessä ja kirjauduttaessa console-istuntoon.

5.4 VMware vSphere Client -toiminnot

Ohjelmaan kirjaudutaan sisään siihen annetuilla tunnuksilla. Joihinkin palvelinkapasiteetteihin päästään kirjautumaan sisään laittamalla ruksi ”Use Windows session credentials” kohtaan (kuva 11). Kirjautuessa sisään tulee ”IP address / Name” -kenttään halutun palvelinkapasiteetin nimi.

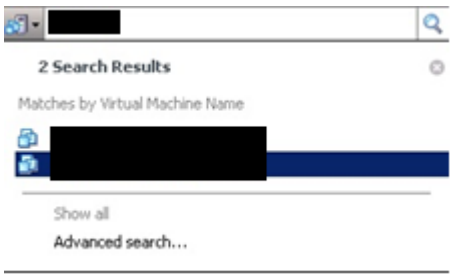
Kuva 11. Kirjautuminen VMware vSphere Client -ohjelmaan

Kirjauduttaessa palvelinkapasiteettiin nähdään sen sisältämät kapasiteetit ja asiakkaat painamalla kansioiden vieressä olevia plus-nappeja (kuva 12).



Kuva 12. VMware vSphere Client – Asiakkaat ja kapasiteetit

Helpoiten halutun palvelimen löytää, kun käyttää ohjelman oikeassa yläkulmassa olevaa hakutoimintoa (kuva 13).

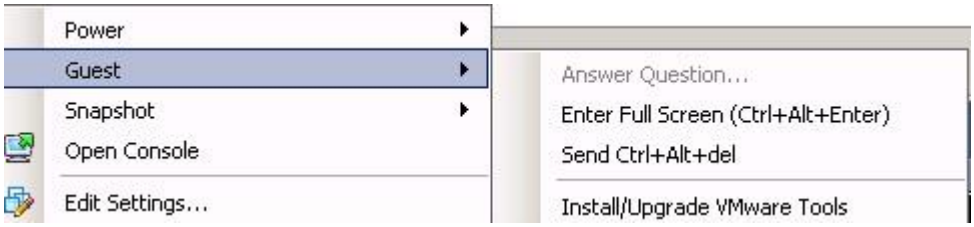


Kuva 13. VMware vSphere Client – palvelimen haku

Kun haluttu palvelin on haettu, aukeaa palvelimen ”Getting started” -välilehti. Kyseisestä välilehdestä nähdään onko palvelin isäntäkone (Host), palvelinkeskus (Datacenter), klusteri (Cluster) vai virtuaalipalvelin (Virtual Machines). Samalla välilehdellä voidaan myös sammuttaa virtuaalikone (Shut down the virtual machine), pysäyttää virtuaalikone (Suspend the virtual machine) tai muokata virtuaalikonetta (Edit virtual machine settings). ”Summary”-välilehden ”General” kohdasta nähdään esimerkiksi mitä käyttöjärjestelmää virtuaalikone käyttää, kuinka monta virtuaalista CPU:ta (Central Processing Unit) sillä on, kuinka paljon muistia sille on annettu ja virtuaalikoneen IP-osoite (Internet Protocol) (kuva 14). Virtualikoneelle voidaan tehdä muutoksia ”Commands” kohdasta. Virtuaalikoneelle annetun muistin ja CPU:n määrän näkee ”Resource Allocation”-välilehdeltä. Virtuaalikoneen suorituskykyä voidaan seurata ”Performance”-välilehdeltä. Aktiiviset hälytykset näkee ”Alarms”-välilehdeltä. Palvelimelle voidaan kirjautua sisään ”Console”-välilehdeltä.

Kuva 14. VMware vSphere Client – Summary-välilehti

VSphere Clientin yläpalkista ”Inventory”-välilehden alta löytyvästä ”Virtual Machine”-valikosta voidaan esimerkiksi käynnistää kone uudelleen tai console-istunnossa oltaessa lähettää ”Ctrl+alt+del”-komento. Kuvissa 15 ja 16 olevat komennot on selitetty alla olevassa taulukossa (taulukko 4).



Kuva 15. VMware vSphere Client – Guest-toiminnot

Kuva 16. VMware vSphere Client – Power-valikko

Taulukko 4. VMware vSphere Client -toimintojen selitykset

Power On	Käynnistää virtuaalikoneen
Power Off	Samuuttaa virtuaalikoneen
Suspend	Pysäyttää virtuaalikoneen
Reset	Vastaa virtuaalikoneen sammuttamista virtanapista. Käytetään esimerkiksi jos kone on jäänyt ”Shutting down”-tilaan.
Shut Down Guest	Sammuttaa virtuaalikoneen
Restart Guest	Uudelleen käynnistää virtuaalikoneen
Enter Full Screen (Ctrl+Alt+Enter)	Avaa console-istunnon koko ruudulle
Send Ctrl+Alt+Del	Lähettää ”Crtl+Alt+Del”-komennon virtuaalikoneelle

6 PALVELINHÄLYTYKSET

6.1 Palvelinhälytyksien syntyminen

Windows Monitoring Agent kerää palvelimelta tietoja, esimerkiksi levyn täyttymisestä, prosessorin käytöstä ja ohjelmien tilasta. Jos jokin palvelimella oleva ohjelma pysähtyy tai levyn täyttöaste ylittää sille asetetun hälytysrajan, luo agentti siitä hälytyksen TIP:iin. Alla olevissa kappaleissa käydään läpi kuinka hoidetaan yleisimmät palvelinhälytykset ja mistä nämä johtuvat.

6.2 Ping failed -hälytykset

Suuri osa ”Ping failed” -hälytyksistä johtuu yleensä palvelimien uudelleenkäynnistyksistä. Kannattaa siis käydä tarkastamassa TEP:stä ”Situation Event Console” -välilehdeltä, onko palvelin juuri käynnistetty (kuva 17). Jos välilehdellä on ”ENF_reboot_log_event” -tapahtuma, on palvelin juuri uudelleenkäynnistetty. ”Global Timestamp” -välilehdeltä varmistetaan vielä, että uudelleenkäynnistäminen on tapahtunut hälytyksen tulon aikaan. Palvelin saattaa myös hälyttää pysähtyneestä palvelusta kuvan 17 mukaisesti (esimerkissä ”gpsvc”). Palvelu kuitenkin yleensä nousee itsestään ylös, kunhan palvelin on uudelleenkäynnistynyt. Palvelinta voidaan myös tarvittaessa pingata TIP:n kautta ja varmistaa, että se on toiminnassa (kuva 18). Kun palvelin on noussut ylös, ei se enää näy harmaana TEP:ssä. Jotkut palvelimet käynnistyvät toisia hitaammin. Joillakin palvelimilla uudelleenkäynnistys kestää vain muutaman minuutin, kun taas toisilla kymmeniä minuutteja. Jos palvelin ei kuitenkaan nouse ylös tunnin sisään, on se jäänyt uudelleenkäynnistyksessä jumiin ja se pitää käynnistää uudelleen.

Kuva 17. Situation Event Console -näkymä

Kuva 18. Palvelimen pingaus TIP:ssä

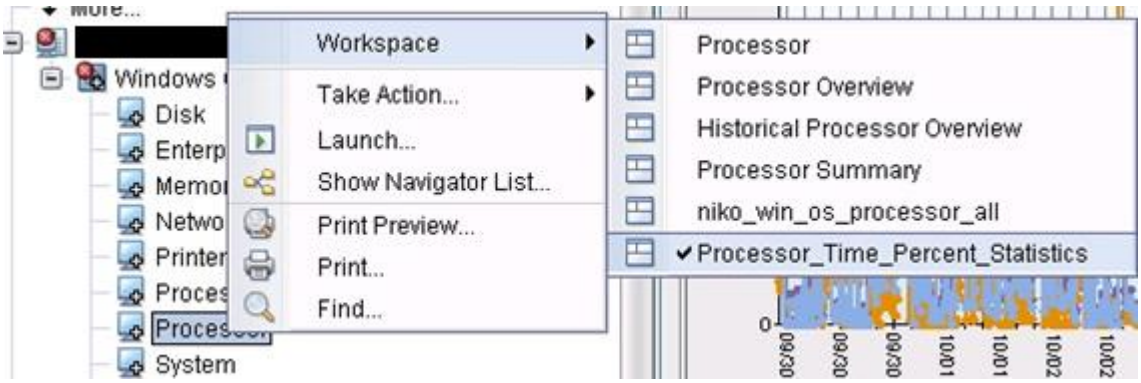
6.3 CPU, Memory available ja Pagefile -hälytykset

CPU, Memory available ja Pagefile -hälytykset johtuvat palvelimilla tapahtuvasta kovasta kuormituksesta. Suurin osa hälytyksistä on niin sanotusti harmittomia ja ne poistuvat parissa tunnissa. Näitä hälytyksiä on kuitenkin seurattava aktiivisesti työvuoron aikana. TEP:in kautta voidaan käydä tarkastamassa historiatiedoista, onko palvelimen prosessorin tai muistin käyttö normaalia. Palvelinta kuormittavan prosessin pystyy näkemään TEP:in ”High Process” -valikosta (kuva 19). Esimerkissä käytetään palvelimen prosessorinkäyttöä (kuva 19; kuva 20; kuva 21)

Kuva 19. TEP - High Process -valikko

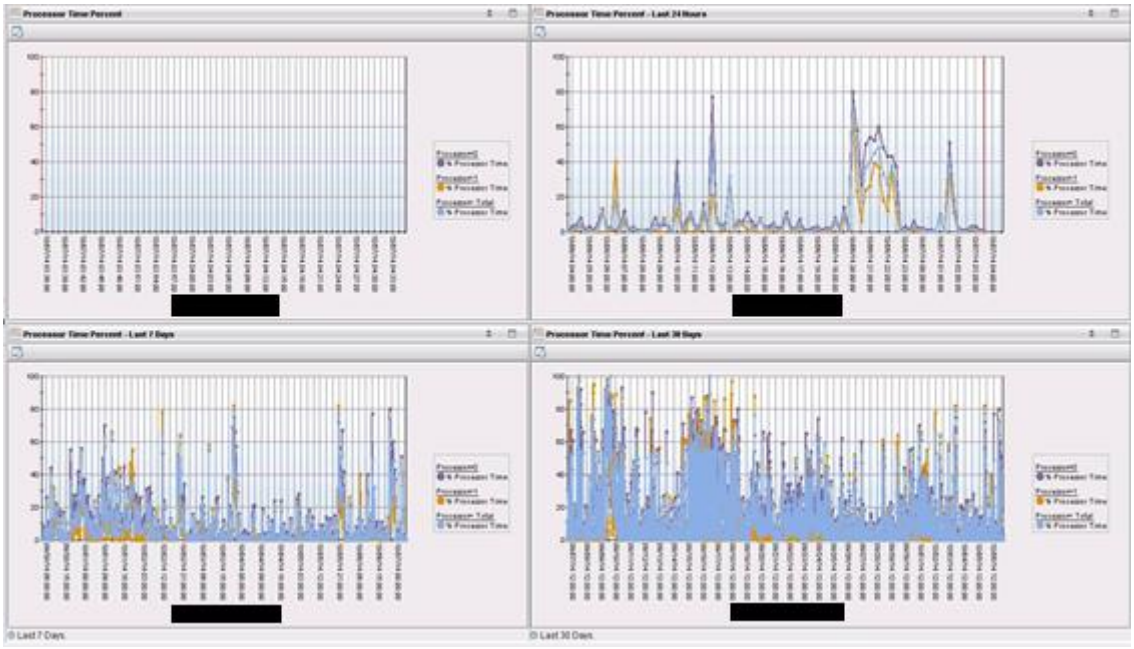
Esimerkkikuvassa (kuva 19) ”kntcma.exe”, eli ”Monitoring agent for Widows OS” -prosessi, vie prosessorista 100 prosenttia. Tämä prosessi kuormittuu, kun se käsittelee suuria määriä Windowsin tapahtumalokeja (IBM 2013). Toinen yleinen prosessi, joka kuormittaa prosessoria on ”svchost.exe”. Kyseinen prosessi on tietokoneen oma prosessi, joka sisältää muita yksittäisiä palveluita, esimerkiksi ”Windows Defenderin”. (Microsoft 2014). Kolmas yleinen prosessoria kuormittava prosessi on ”sqlserv.exe”. Tämä prosessi kuormittuu, kun palvelimella suoritetaan SQL-ajoja. Yllä mainitut prosessit

ovat yleensä myös niitä prosesseja, jotka kuormittavat palvelimen fyysistä RAM-muistia (Random Access Memory) sekä virtuaalista Pagefile-muistia.



Kuva 20. Palvelinprosessorin historiatiedot -valikko

Paina palvelimen nimen alapuolelta löytyvää ”Windows OS” -painikkeen plus-näppäintä. Avautuvassa valikossa pääsee tarkastelemaan tarkemmin esimerkiksi levyn, muistin ja prosessorin käyttöä. Painamalla hiiren oikeaa näppäintä ”Processor”-välilehdellä ja valitsemalla ”Workspace”-valikosta ”Processor_Time_Percent_Statistics” päästään tarkastelemaan CPU:n historiastatistiikkaa (kuva 20). Ikkunaan aukeaa viimeisimmän tunnin, 24 tunnin, 7 päivän ja 30 päivän historiatiedot (kuva 21). Näistä tiedoista voidaan päätellä onko prosessorin käyttö aina samaan aikaan päivästä tai viikosta normaalia.



Kuva 21. Prosessorien historiatiedot

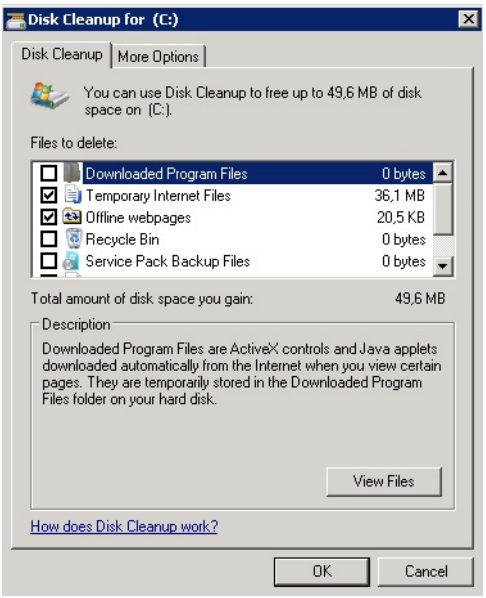
6.4 Disk space critical -hälytykset

Disk space critical -hälytykset tulevat, kun levyn täyttöaste nousee yli hälytysrajan. Suurimmassa osaa palvelimia hälytysraja on asetettu 95 % täyttöasteelle. Suurin osa näistä hälytyksistä johtuu päivityksistä, joita asennetaan palvelimille. Nämä päivityksistä johtuvat hälytykset yleensä poistuvat, kun päivitykset ovat asentuneet palvelimelle. Jos jokin asema menee 100 % täyteen, estyy kyseisen palvelimen toiminta ainakin osittain. Yleisin asema, joka palvelimilla täyttyy, on C-asema. Tämän aseman siivoamiseen on ohjeet seuraavassa kappaleessa 6.4.1.

6.4.1 C-aseman siivous

C-asemalle asennetaan palvelimella olevat ohjelmat ja siellä sijaitsee myös palvelimella olevien käyttäjien henkilökohtaiset tiedostot sekä temp- eli väliaikaiskansiot. Asema täyttyy yleensä varsinkin sen takia, koska temp-kansioihin jää vanhoja käyttämättömiä tiedostoja. Jotkut ohjelmat tallentavat myös tilapäisiä tiedostoja Windowsin väliaikaistiedostoihin (Temporary Files), mikä täyttää asemaa. Aseman täyttyminen hidastaa palvelinta ja saattaa pahimmassa tapauksessa estää palvelimen toiminnan. Alla olevissa ohjeissa käydään läpi, miten C-aseman siivous tapahtuu.

1. Kirjaudu palvelimelle
2. Tyhjennä työpöydällä oleva ”Roskakori”. Yllättävän monesti ”Roskakori” on täynnä vanhoja tiedostoja
3. Tyhjennä ”C:\temp”. Tässä kannattaa käyttää omaa harkintaa, että onko kyseisessä kansiossa tärkeitä tiedostoja. Yli puoli vuotta vanhat tiedostot voi yleensä surutta poistaa.
4. Tyhjennä ”C:\Windows\Temp” käyttäen samaa harkintaa kuin kohdassa kolme
5. Avaa ”Disk Cleanup” kirjoittamalla Käynnistä-valikkoon ”cleanmgr”. Jos ohjelmaa ei löydy Käynnistä-valikosta, voidaan se lisätä palvelimelle seuraavassa kappaleessa 6.4.2 olevien ohjeiden mukaisesti. Jos ohjelma kysyy minkä aseman haluat analysoida, valitse C-asema. Ohjelman analysoitua C-aseman tiedostot ilmoittaa se kuinka paljon sillä voidaan vapauttaa levytilaa (kuva 22). Painamalla OK-nappia poistaa ”Disk Cleanup” valitut tiedostot.



Kuva 22. Cleanmgr-ohjelmaikkuna

6. Poista “C:\Windows\logs\servermanager.log” -tiedosto. Kyseinen tiedosto täyttyy aina kun Server Manager -ohjelmaa käytetään ja se luodaan uudestaan Server Manager -ohjelman käynnistyessä.

(FileSystem C: D: E: Critical 2014.)

6.4.2 Cleanmgr-ohjelman lisääminen Server 2008 ja Server 2008 R2 -palvelimille

Koska kaikissa palvelimissa ei ole automaattisesti käytössä ”cleanmgr”-ohjelmaa, voidaan se saada käyttöön siirtämällä kaksi tiedostoa tiettyihin kansioihin. Tiedostot, jotka pitää siirtää, ovat ”cleanmgr.exe” ja ”cleanmgr.exe.mui”. Nämä kyseiset tiedostot löytyvät alla olevan kuvan 23 mukaisista kansioista. ”Cleanmgr.exe” pitää siirtää ”%systemroot%\System32” -kansioon ja ”cleanmgr.exe.mui” pitää siirtää ”%systemroot%\System32\en-US” -kansioon. Tämän jälkeen voidaan avata ”cleanmgr”-ohjelma kirjoittamalla Käynnistä-valikon hakukenttään ”cleanmgr”.

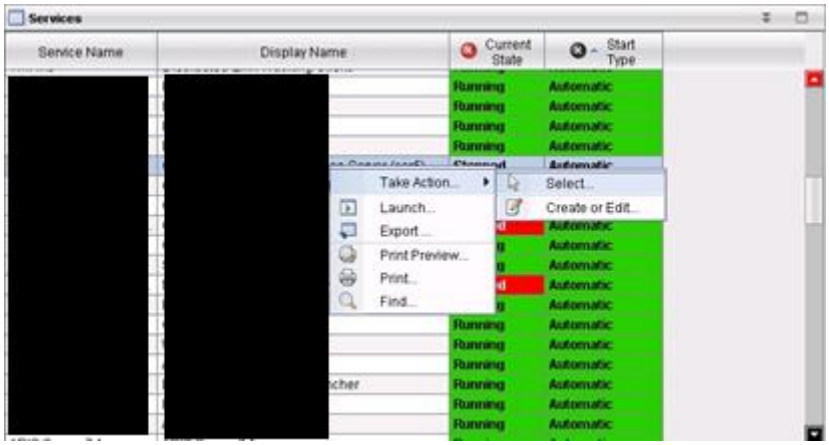
Operating System	Architecture	File Location
Windows Server 2008 R2	64-bit	C:\Windows\winsxs\amd64_microsoft-windows-cleanmgr_31bf3856ad364e35_6.1.7600.16385_none_c9392808773cd7da\cleanmgr.exe
Windows Server 2008 R2	64-bit	C:\Windows\winsxs\amd64_microsoft-windows-cleanmgr.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9cb6194b257cc63\cleanmgr.exe.mui
Windows Server 2008	64-bit	C:\Windows\winsxs\amd64_microsoft-windows-cleanmgr.resources_31bf3856ad364e35_6.0.6001.18000_en-us_b9f50b71510436f2\cleanmgr.exe.mui
Windows Server 2008	64-bit	C:\Windows\winsxs\amd64_microsoft-windows-cleanmgr_31bf3856ad364e35_6.0.6001.18000_none_c962d1e515e94269\cleanmgr.exe.mui
Windows Server 2008	32-bit	C:\Windows\winsxs\x86_microsoft-windows-cleanmgr.resources_31bf3856ad364e35_6.0.6001.18000_en-us_5dd66fed98a6c5bc\cleanmgr.exe.mui
Windows Server 2008	32-bit	C:\Windows\winsxs\x86_microsoft-windows-cleanmgr_31bf3856ad364e35_6.0.6001.18000_none_6d4436615d8bd133\cleanmgr.exe

Kuva 23. Cleanmgr-ohjelmistopolku (FileSystem C: D: E: Critical 2014)

6.5 TEP-palvelun käynnistäminen ja pysäyttäminen

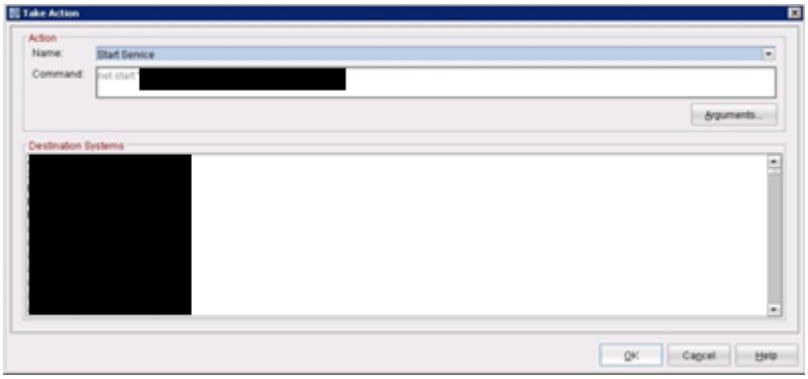
Pysähtyneet palvelut käynnistetään TEP:stä, Service-valikosta.

1. Klikkaa haluttua palvelun nimeä hiiren oikealla näppäimellä
2. Valitse ”Take Action” ja ”Select” (kuva 24)



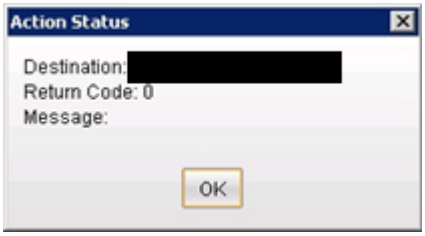
Kuva 24. TEP:in palvelulistaus Service-valikossa

3. Valitse Name-valikkoon ”Start Service” listasta (kuva 25)
4. Paina ”OK”



Kuva 25. Palvelun käynnistäminen TEP:ssä

Jos palvelun käynnistäminen onnistui, palautuu ”Return Code” arvona ”0” (kuva 26). Jos palvelun käynnistäminen epäonnistui, palautuu arvo ”4”. Palvelun pysäyttäminen tapahtuu samalla tapaa kuin käynnistäminen sillä poikkeuksella, että Name-valikkoon valitaan ”Stop Service”.



Kuva 26. Palvelun käynnistäminen -ilmoitus TEP:ssä

6.6 SQL failed -hälytykset

Suurin osa SQL-ajoista tapahtuu yön aikana, koska silloin ajojen aiheuttama kuorma palvelimille sekä verkkoliikenteelle ei haittaa muita käyttäjiä. Tämä tarkoittaa myös sitä, että yön aikana tulee iso osa SQL failed -hälytyksiä. Nämä hälytykset johtuvat ajojen epäonnistumisista. SQL-ajot eivät ole kriittisimpiä asioita, sillä jotkut palvelimet toteuttavat ajoja jopa 15 minuutin välein. Ajojen tarkastamisen voi tehdä joko TEP:stä tai kirjautumalla palvelimelle seuraavien olevien ohjeiden mukaan.

6.6.1 SQL-ajon tilan tarkistaminen TEP:stä

1. Avaa SQL-palvelin TEP:ssä
2. Avaa Jobs -valikko ja sieltä ”Job Summary” (kuva 27).

Kyseisestä valikosta nähdään tarkalleen, mitkä SQL-ajot ovat epäonnistuneet. Taulusta näkee myös koska ajo on epäonnistunut ja koska seuraava ajo tulee olemaan.

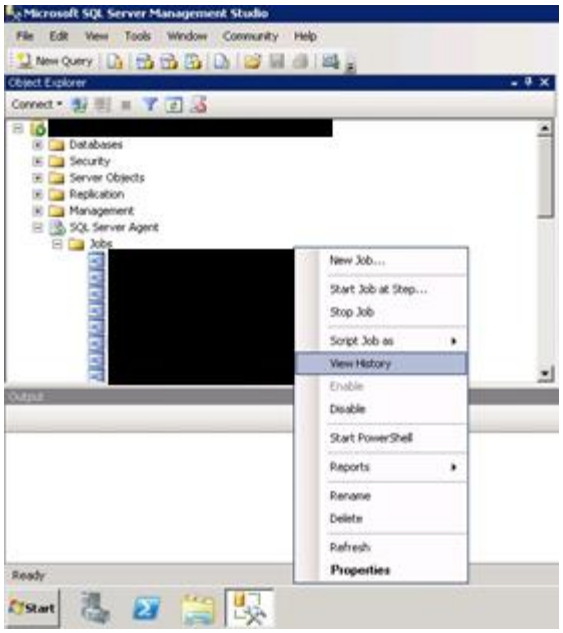
Kuva 27. Job Summary -valikko TEP:ssä

6.6.2 SQL-ajon tarkistaminen palvelimelta ja uuden ajon suorittaminen

1. Kirjaudu palvelimelle
2. Avaa palvelimella Käynnistä-valikosta ”SQL Server Management Studio”
3. Käytä SQL Server 2008 kirjautumiseen ”Windows Authentication” vaihtoehtoa tai käyttämällä vaadittuja kirjautumistunnuksia. (kuva 28)

Kuva 28. SQL Server Management Studio – kirjautuminen ohjelmaan

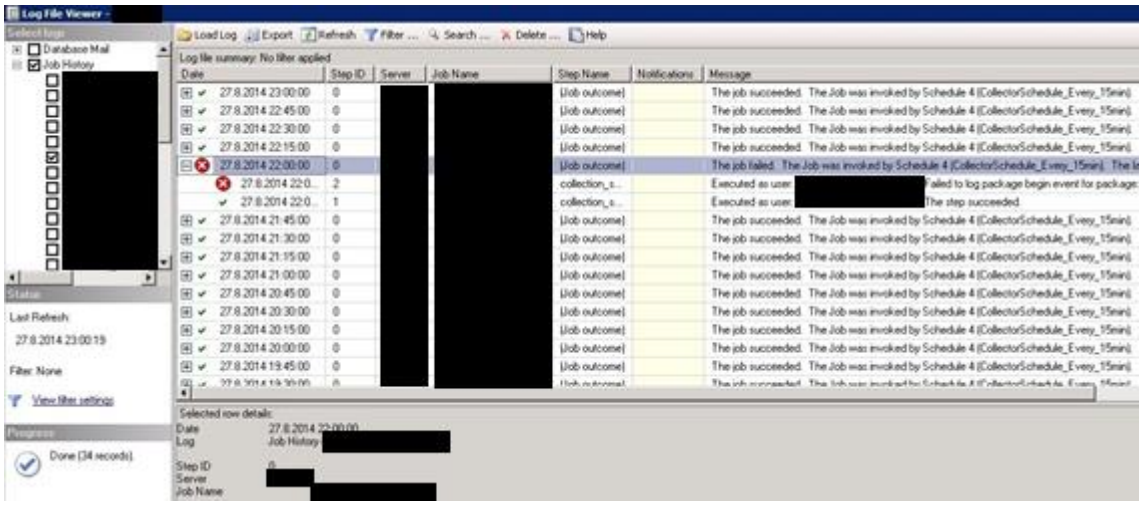
4. Avaa haluttu ajo Jobs-valikosta (kuva 29)



Kuva 29. SQL Server Management Studio -valikot

5. Klikkaa hiiren oikealla ja valitse ”View History” (kuva 29)

Esimerkissä SQL-ajo epäonnistui kello 22:00 ja epäonnistumisen syy lukee ”Message” kentässä (kuva 30). Samalla nähdään myös, että SQL-ajo onnistui kello 22:15.

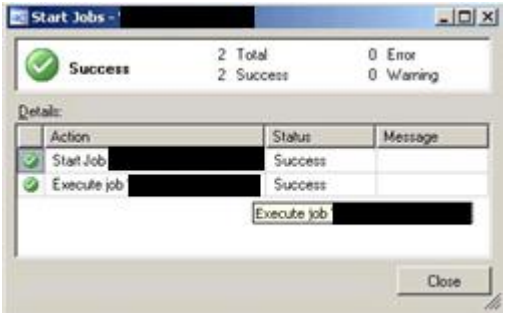


Kuva 30. SQL Server Management Studio – SQL-ajojen historiatiedot

6. Tässä tapauksessa hälytys ei ole enää aktiivinen, koska seuraava ajo onnistui
7. Jos ajoja on vain kerran päivässä, voidaan uusi ajo suorittaa välittömästi. Valitse Jobs-valikosta ”Start Job at Step…” -vaihtoehto (kuva 31).

Kuva 31. SQL Server Management Studio – SQL-ajon käynnistäminen

SQL-ajo saattaa kestää kymmenistä sekunneista useaan minuuttiin. Kun ajo on suoritettu, antaa ohjelma kuvan 32 mukaisen ilmoituksen.



Kuva 32. SQL Server Management Studio – onnistunut SQL-ajo

6.7 Windows Monitoring Agent offline -hälytykset

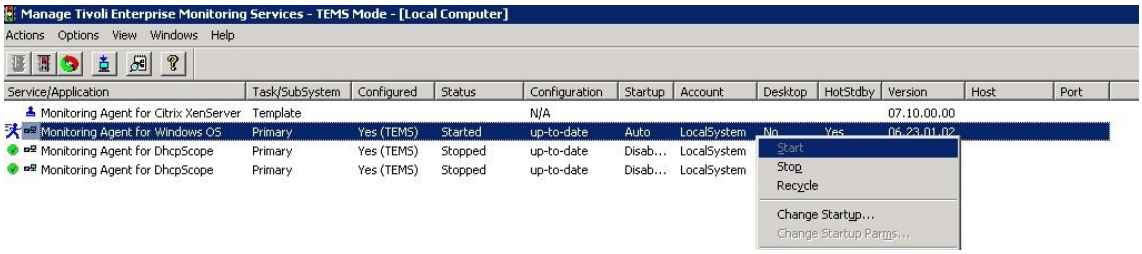
”Windows Monitoring Agent” -ohjelma on jokaisella valvottavalla Windows-palvelimella pyörivä ohjelma. Jos agentti menee offline-tilaan, ei uusia hälytyksiä synny TIP:iin eikä palvelimesta saa tietoja TEP:ssä. Jos agentti ei vastaa kyselyyn, syntyy siitä hälytys ja palvelin muuttuu harmaaksi TEP:ssä. On hyvä kuitenkin huomioida, että palvelimen uudelleenkäynnistyksen yhteydessä saattaa näitä hälytyksiä syntyä. Osa agenteista voidaan käynnistää TEP:in kautta kuten normaalit palvelut, mutta jotkut agentit vaativat palvelimelle sisäänkirjautumisen ja agenttisovelluksen uudelleenkäynnistämisen.

6.7.1 Windows Monitoring Agent käynnistäminen

Alla olevissa ohjeissa kerrotaan, kuinka monitoring agent käynnistetään palvelimelta.

1. Kirjaudu sisään palvelimelle
2. Avaa Käynnistä -valikosta ”IBM Tivoli Monitoring” -kansiosta löytyvä ”Manage Tivoli Monitoring Services”

Jos agentti on päällä, on sen tila Status-kentässä ”Started”, kun taas jos agentti on pois päältä, on tila ”Stopped”. Startup-kentästä näkee onko agentin tarkoitus nousta palvelimen uudelleenkäynnistyksen yhteydessä automaattisesti (Auto), viivästetysti (Delayed) tai onko agentti pois käytöstä (Disabled). Agentin käynnistäminen tapahtuu klikkaamalla haluttua agenttia hiiren oikealla ja painamalla ”Start”. Jos agentti näyttäisi olevan päällä, mutta on silti harmaana TEP:ssä, voidaan painaa ”Recycle”, jolloin agentti käynnistyy uudelleen (kuva 33).



Kuva 33. Tivoli Enterprise Monitoring Services -hallintapaneeli

6.7.2 Monitoring agentin käynnistäminen Service-valikosta

Alla olevissa ohjeissa käydään läpi monitoring agentin käynnistäminen Services-valikosta.

1. Avaa Käynnistä-valikko ja aukaise ”Administrative Toolsin” kautta ”Services”-hallintatyökalu

Services-ohjelmasta näkee kaikki palvelimella pyörivät palvelut ja niiden kuvaukset. Tätä kautta pystyy käynnistämään myös TEP:ssä näkyviä palveluita.

2. Valitse haluttu agentti, klikkaa hiiren oikealla ja paina ”Start” (kuva 34). Agentin voi käynnistää myös ohjelman vasemmassa yläkulmassa olevasta Start-näppäimestä

Kuva 34. Monitoring agentin käynnistäminen Service-valikosta

7 POHDINTA

Opinnäytetyön teoriaosuudessa kerrotaan virtualisoinnista ja sen osa-alueista. Tämä osuus on hyödyksi työskennellessä virtuaalipalvelimien kanssa. Teoriaosuus antaa yleiskuvan virtualisoinnista ja helpottaa ymmärtämään virtuaalipalvelimien kanssa työskentelyä.

Palvelinvalvonta ja -ylläpito -osuudessa kerrotaan järjestelmänvalvojalle tärkeistä ylläpitosovelluksista, niiden ominaisuuksista, toiminnallisuuksista ja miksi palvelimia valvotaan. Osuudessa kerrotaan myös työpaikkani palvelinvalvontaympäristöstä. Tämä on hyödyksi varsinkin aloittaville työntekijöille ja se toimii myös ohjenuorana kokeneemmille työntekijöille.

Palvelinhälytykset-osuudessa käydään läpi yleisimpien palvelinhälytysten syyt ja niiden korjaaminen. Hälytyksien korjaaminen on havainnollistettu kuvien avulla, jotta ohjeet olisivat mahdollisimman selkeät. Palvelinhälytyksien korjaaminen helpottuu huomattavasti, koska ohjeet tulevat löytymään yhdestä paikasta.

Ohjeistus on onnistunut mielestäni hyvin, koska siinä käsitellään suurinta osaa yleisimmistä palvelinhälytyksistä. Ohjeet ovat myös helppolukuiset ja ymmärrettävät. Aluksi kirjasin ylös yleisimpiä hälytyksiä ja niiden syitä. Tämän jälkeen aloin kokoamaan hälytyksien korjaustoimenpiteitä yrityksen omien ohjeiden ja omien kokemuksieni perusteella. Ohjeiden kirjoittamisen jälkeen olen itse testannut ohjeiden toimivuutta noin kuukauden ajan. Ohjeet ovat mielestäni riittävät yleisimpien palvelinhälytyksien korjaamiseen.

Uusien palvelinhälytysohjeiden päivittäminen on helppoa opinnäytetyössä liitteenä olevaan ohjeeseen. Tarkoituksena on päivittää ohjeita uusien hälytyksien korjaamiseen lisäämällä kuvat ja kirjalliset ohjeet olemassa olevaan tiedostoon. Olen huomannut omien kokemuksieni perusteella, että työn sujuvuuden kannalta on parempi, jos ohjeet ovat yhdessä paikassa. Tämän takia toivonkin, että työnantaja panostaisi tulevaisuudessa ohjeiden löytymiseen yhdestä paikasta.

LÄHTEET

Butler, B. 15.09.2014. How network virtualization is used as a security tool. Networkworld.com. Luettu 20.10.2014.
http://www.networkworld.com/article/2606388/virtualization/how-network-virtualization-is-used-as-a-security-tool.html

FileSystem C: D: E: Critical. Knoppi Article: 112. Enfo Oyj. Luettu 02.10.2014. (Ei julkinen).

GyGem. 2008. SAN & NAS 101.GyGem. Katsottu 22.10.2014.
https://www.youtube.com/watch?v=vdf6CvGQZrk

IBM, 2013, Windows OS Agent. Luettu 05.10.2014
https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli+Monitoring/page/Windows+OS+Agent

Kleyman, B. 2012. Hypervisor 101: Understanding the virtualization market. Data Center Knowledge. Luettu 20.10.2014.
http://www.datacenterknowledge.com/archives/2012/08/01/hypervisor-101-a-look-hypervisor-market/

Kusnetzky, D. 2011. Virtualization: A Manager's Guide, Sebastopol, CA. O'Reilly Media Inc.

Microsoft, 2014. What is svchost.exe?. Luettu 05.10.2014
http://windows.microsoft.com/en-us/windows/what-is-svchost-exe#1TC=windows-7

One Cloud Solutions 2013. Storage Virtualization. One Cloud Solutions. Luettu 22.10.2013 http://www.onecloudsol.com/virtualization.html

Rouse, M. 2011. App virtualization (Application virtualization). TechTarget. Luettu 21.10.2014
http://searchvirtualdesktop.techtarget.com/definition/app-virtualization

Rouse, M. 2014. Storage Are Network (SAN). TechTarget. Luettu 22.10.2014
http://searchstorage.techtarget.com/definition/storage-area-network-SAN

SimplicIT. 2012. Application virtualization. Simplicit365. Luettu 20.10.2014.
http://www.simplicit365.com/application-virtualization.php

Tossavainen, A. 2014. Monitoring and management -ohjeistus. Enfo Oyj intranet. Kuopio. (Ei julkinen).

Vaughan-Nicholson S. 29.03.2014. Hypervisors: The cloud's potential security Achilles heel. Zdnet. Luettu 31.10.2014. http://www.zdnet.com/hypervisors-the-clouds-potential-security-achilles-heel-7000027846/

VMware, 2014a, Virtialization. WMware. Luettu 16.10.2014.
http://www.vmware.com/virtualization/

VMware, 2014b, Virtialization basics, How Virtualization works, Luettu 16.10.2014, http://www.vmware.com/files/images/diagrams/vmw-virtualization-defined.jpg

LIITEET

Liite 1. Palvelinvalvonta ja -ylläpito liiteohjeistus (salattu)