Petri Levomäki

VERKONVALVONTAJÄRJESTELMÄN KÄYTTÖÖNOTTO

Tieto- ja viestintätekniikan koulutusohjelma

2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VERKONVALVONTAJÄRJESTELMÄN KÄYTTÖÖNOTTO

Levomäki, Petri
Satakunnan ammattikorkeakoulu
Tieto- ja viestintätekniikan koulutusohjelma
Syyskuu 2018
Ohjaaja: Aromaa Juha, DI
Sivumäärä: 23
Liitteitä: -

Asiasanat: tietoverkot, verkonvalvonta, monitorointi, ylläpito

---

Opinnäytetyössä tutkittiin verkonvalvontajärjestelmiä, ja otettiin käyttöön verkonvalvontajärjestelmä keskisuuressa asiakasyrityksessä, jossa tällaista järjestelmää ei vielä ennestään ollut. Järjestelmäksi valittiin avoimeen lähdekoodiin perustuva Zabbix.

Työssä tutustuttiin verkonvalvonnan periaatteisiin ja tekniikoihin yleisesti. Zabbix -ohjelmisto ja sen keskeisimmät ominaisuudet esitellään. Käytännön osiossa kuvataan järjestelmän käyttöönotto asiakasyrityksessä.

DEPLOYMENT OF A NETWORK MONITORING SYSTEM

Levomäki, Petri
Satakunta University of Applied Sciences
Degree Programme in Information and communication technology
September 2018
Supervisor: Aromaa Juha, M.Sc.
Number of pages: 23
Appendices: -

Keywords: data networks, monitoring, surveillance

Network monitoring systems were investigated in this thesis. Such a system was deployed in a medium size enterprise, which didn't yet have any monitoring system for network surveillance. Zabbix, which is an enterprise-class open source distributed monitoring solution, was chosen.

Network monitoring principles and technologies were studied generally. Zabbix software and its main features were presented. The customer enterprise deployment was described in the practical portion of the thesis.

SISÄLLYS

1 JOHDANTO

Verkonvalvonnan eli monitoroinnin avulla verkon ja järjestelmien ylläpitäjät pysyvät tietoisina verkon tilasta ja siitä mitä siellä tapahtuu. He voivat tarkkailla esim. verkkoyhteyksiä, palvelimien ja muiden verkkolaitteiden toimintaa laitetasolla, sekä näissä toimivien palveluiden toimintaa. Tarkoituksena on tunnistaa mahdollisia ongelmakohtia, jotka voivat vaarantaa liiketoiminnan jatkuvuuden, sekä vikatilanteissa nopea reagoiminen ja vian perimmäisen syyn selvittäminen.

Asiakasyrityksessä ei vielä ennestään ollut mitään keskitettyä monitorointiratkaisua. Koska kriittisimmät palvelut toimivat yrityksen omilla palvelimilla lähiverkossa, on kyseinen ratkaisu huomattavan tarpeellinen ja hyödyllinen. Ennestään vikatilanteen sattuessa ei ollut välttämättä edes käsitystä mistä sitä lähdetään etsimään.

Yhdessä yrityksen ICT-järjestelmäpäällikön kanssa monitorointijärjestelmäksi valittiin avoimeen lähdekoodiin perustuva Zabbix -verkonvalvontaohjelmisto. Syinä valinnalle oli ohjelman monipuolisuus, huomattavan laaja muokattavuus ja maksuttomuus. Ohjelman ympärille on myös parinkymmenen vuoden aikana kehittynyt laaja yhteisö ja kehitys on jatkuvaa.

2 VERKON MONITOROINTI YLEISESTI

Verkon monitorointia suunnitellessa pitää ottaa huomioon ainakin seuraavat asiat:

- Data, joka verkon eri elementeistä kerätään. Data jaetaan datapisteisiin, eli yksittäisiin tietoelementteihin, jotka palauttavat jonkun tietyn arvon. Lisäksi jokaiselle datapisteelle tulisi määrittää taajuus, kuinka usein sen tieto kerätään, sekä säilytysaika historian tarkastelua varten. Pidemmältä aikaväliltä riittää yleensä aikaväliltään harvennettu data trendien analysoimista varten. Näin säästetään levytilaa.

- Monitorointiohjelmisto, joka kerää datan, käsittelee sen ja esittää käyttäjälle hyödyllisellä tavalla, esim. muodostaen kaavioita ja raportteja, sekä hälytyksiä asioista, jotka vaativat huomiota

- Tapa tai protokolla, jolla data siirtyy monitoroitavista elementeistä monitorointiohjelmistolle

(1)

2.1 FCAPS

FCAPS-malli on ITU:n Telecommunications Management Network (TMN) standardin määrittelemä kehysrakenne televerkkojen ylläpitoon ja hallinnointiin, jonka idea sopii myös dataverkkoihin

- **Fault Management** eli vikatilanteiden hallinta käsittää verkossa ilmenevän vian tunnistamisen, eristämisen sekä selvittämisen

- **Configuration Management** eli asetuksien hallinta käsittää asetuksien keräämisen eri verkkolaitteista sekä niiden varastoinnin ja lisäksi myös asetusten muutoksien seurannan. Koska monet verkon ongelmatilanteet liittyvät vääriin asetuksiin, tätä voidaan pitää tärkeänä ennakoivan verkonvalvonnan kannalta

- **Accounting** käsittää palveluntarjoajien verkossa tapahtuvan resurssien käytön laskutusta varten. Muissa verkoissa tämän korvaa **administration**, joka viittaa verkon käyttäjille määritettäviin käyttölupiin

- **Performance Management** käsittää verkon suorituskyvyn seurannan, esim. verkkoelementtien vasteajat, käyttötasot, verkkoliikenteen pakettien menetykset ym.

- **Security Management** käsittää pääsynvalvonnan verkon dataan ja asetuksiin, jolloin estetään näiden luvaton käyttö

(2)

Monitoroinnin avulla voidaan kerätä tietoa kaikkiin edellä mainittuihin kohtiin, mutta tässä työssä keskitytään lähinnä suorituskyvyn seurantaan ja vikatilanteiden tunnistamiseen.

2.2 Yleisiä monitorointitekniikoita ja protokollia

2.2.1 Ping

Ping on työkalu, jolla voidaan testata IP-verkossa olevan laitteen saavutettavuutta. Ping lähettää kohdelaitteelle *ICMP echo request*-paketteja, joihon laite vastaa omilla *echo reply* -paketeillaan. Työkalulla voidaan seurata onnistuneesti ja epäonnistuneesti siirrettyjen pakettien määrää, sekä siirtojen viivettä eli *latenssia*. (3)

2.2.2 Simple Network Management Protocol (SNMP)

SNMP on verkonhallintaan käytettävä protokolla. SNMP:llä voidaan kerätä tietoa verkkolaitteista monitorointitarkoituksessa ja mahdollisesti myös hallita näiden asetuksia. Laitteet voivat myös tiettyjen määriteltyjen arvojen perusteella lähettää ”hälytyksen” hallintajärjestelmälle. SNMP:n käyttö perustuu seuraaviin elementteihin:

- **Agentti** on ohjelma, joka toimii SNMP:tä tukevassa laitteessa ja jolla on pääsy laitteessa olevaan MIB-tietokantaan.

- **MIB** (**management information database)** sisältää tietoa laitteen toiminnasta hierarkisesti järjestetyissä *object ID* (OID) –tietueissa.

- **SNMP manager** on osa verkonhallintajärjestelmää (*network management system*, NMS). SNMP manager kerää tietoa laitteista (*get*-toiminto) ja mahdollisesti myös lähettää asetusmuutoksia (*set*-toiminto) agenttien kautta. Agentti voi puolestaan *trap*-toiminnolla lähettää tietyissä määritellyissä tilanteissa ilmoituksen managerille.

SNMP käyttää tiedonsiirtoon UDP protokollaa porttinumerolla 162. SNMP:stä on käytössä kolmea eri versiota:

- **SNMPv1,** alkuperäinen ja vanhentunut, laajalti käytöstä poistettu versio.

- **SNMPv2c** tuo parannuksia alkuperäiseen versioon verrattuna mm. joukkolähetys toiminnolla, jolla voidaan lähettää isompia tietokokonaisuuksia ja tauluja kerralla, sekä parannellulla virheenraportoinnilla. Sekä versio 1 ja 2c käyttävät tietoliikenteen turvaamiseen vain *community*-merkkijonoa, joka pitää molemmilla liikenteen osapuolilla olla sama. Tiedonsiirtoa ei salata mitenkään eikä lähettäjää todenneta, joten tietoturva on heikkoa.

- **SNMPv3** parantaa tietoturvaa tuomalla tiedon salauksen ja eheyden tarkistuksen, sekä lähettäjän todentamisen.

(3)

2.2.3 Syslog

Syslog on standardi ja protokolla lokiviestien käsittelyyn. Useat verkkolaitteet tukevat tätä protokollaa ja muodostavat lokiviestejä toiminnastaan, jotka voidaan lähettää näitä keräävälle palvelimelle. Viesteihin tallentuu myös vakavuusaste, eli esim. onko kyseessä vain ilmoitus, varoitus tai vakavampi hälytys, jonka avulla viestejä voidaan lajitella ja mahdollisesti tehdä toimenpiteitä.
(3)

2.2.4 Windows käyttöjärjestelmän monitorointityökalut

Windowsissa on sisäänrakennettuna työkaluja ja palveluita monitorointitarkoitukseen:

- **Performance counterit** ovat tietueita, joihin tallentuu laajalti tietoja järjestelmän eri osa-alueista, kuten laitteiston (prosessori, muisti, kiintolevyt) ja eri sovellusten ja palveluiden suorituskyvystä.

- **Eventlog** on lokijärjestelmä, johon Windows kerää tietoa eri tapahtumista, kuten sovellusten aiheuttamista virheistä tai tietoturvaa koskevista asioista esim. epäonnistuneet kirjautumisyritykset.

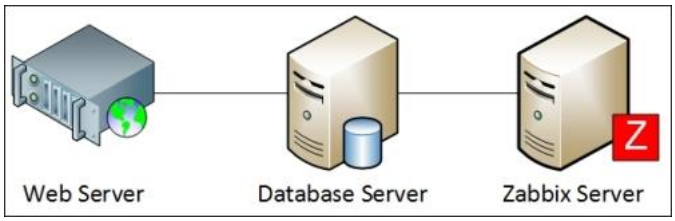
(3)

3 ZABBIX VERKONVALVONTAJÄRJESTELMÄ

Zabbix on avoimeen lähdekoodiin perustuva monitorointijärjestelmä palvelimien, verkkolaitteiden ja sovellusten toiminnan ja suorituskyvyn monitorointiin. Zabbixin loi latvialainen Alexei Vladishev, joka aloitti ohjelman kehityksen yrityksen sisäisenä projektina työskennellessään pankissa vuonna 1998. Myöhemmin projekti laajeni itsenäiseksi ja ensimmäinen versio julkaistiin 2001. Nykyään Zabbixin kehityksestä vastaa Zabbix LLC yritys toimitusjohtajanaan Vladishev. Zabbixia jaetaan GPLv2 lisenssin alaisena. Tämän työn toteutukseen on käytetty versiota 3.4.9.
(4)

3.1 Rakenne

Zabbixin ydin koostuu palvelimesta (Zabbix server), tämän käyttämästä tietokantajärjestelmästä, sekä web-käyttöliittymästä (Web-frontend). Nämä voivat kaikki sijaita samalla tai eri fyysisillä palvelimilla (Kuva 1).



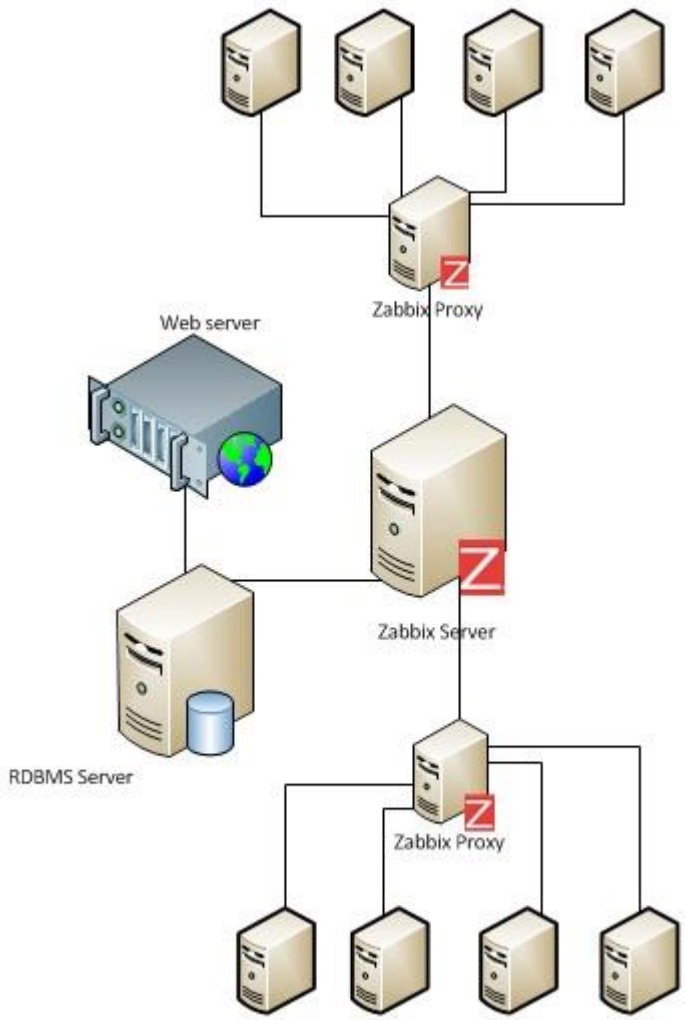
Kuva 1: Zabbix-palvelinarkkitehtuuri (5)

Zabbix-palvelin on keskeisin komponentti, joka käsittelee monitorointidataa ja luo hälytykset ym. Palvelin voidaan asentaa vain Unix-pohjaisille käyttöjärjestelmille näiden suorituskyvyn ja vikasietoisuuden vuoksi.

Tietokanta on kaiken monitorointidatan ja asetusten tallennuspaikka. Tietokantajärjestelmistä on tuettuna ainakin MySQL, Oracle, PostgreSQL ja IBM DB2. Microsoftin SQL Server ei ole tuettuna.

Palvelinta hallinnoidaan web-käyttöliittymän kautta. Käyttöliittymä vaatii virallisesti toimiakseen Apache web-palvelimen ja PHP:n. Myös Nginx:iä on käytetty web-palvelimena.

Laajemmissa verkoissa voi olla myös *Zabbix proxy* –välityspalvelimia, jotka keräävät ja välittävät monitorointidataa pääpalvelimelle. Näin saadaan prosessori- ja I/O-kuormaa jaettua tasaisemmin (Kuva 2).



Kuva 2: Zabbix-välityspalvelinarkkitehtuuri (5)

3.2 Datan keruu

Datan keräämiseen kohdelaitteilta Zabbix tukee monia eri tapoja ja protokollia, joista tässä on esitelty tässä työssä käytetyt.

3.2.1 Zabbix-agentti

Agentti on ohjelma, joka voidaan asentaa kohdelaitteelle, mikäli laitteessa on agenttia tukeva käyttöjärjestelmä. Käytännössä kaikki nykyiset käyttöjärjestelmät (Windows, Linux, Mac OS jne.) ovat tuettuna. Agentin kautta voidaan kerätä laajalti dataa, mitä ei välttämättä muilla keinoilla saisi kerättyä, mutta agenttien asennus ja konfigurointi jokaiselle laitteelle vaatii lisätyötä.

3.2.2 SNMP

Zabbix serverissä on sisäänrakennettuna myös SNMP-tuki, jolloin se voi toimia SNMP managerina ja kerätä dataa esim. verkkolaitteista, jotka tukevat SNMP:tä, mutta joihin ei voi asentaa Zabbix-agenttia.

3.2.3 Simple check

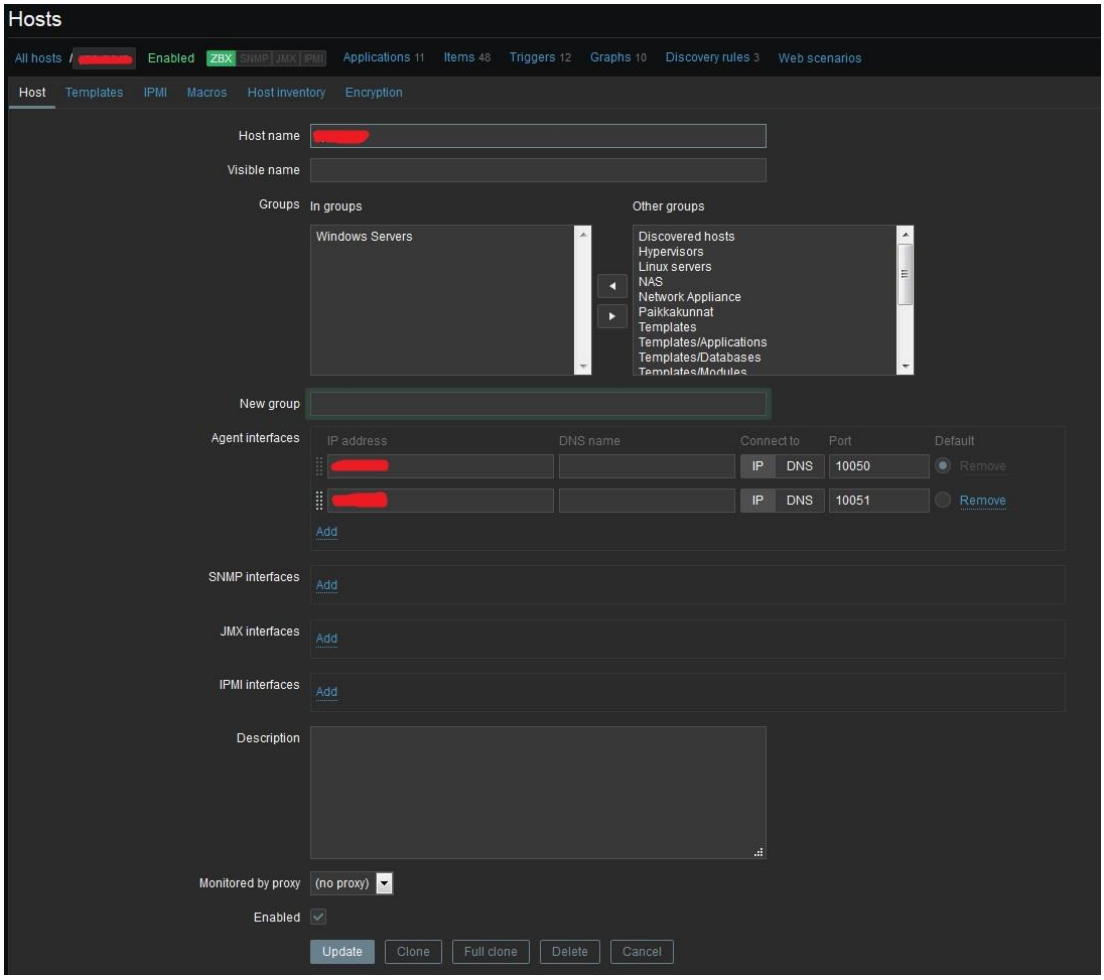
Simple check on nimensä mukaisesti vain yksinkertainen palvelimella ajettava testi, esim. ping-yhteystesti tai jonkin palvelun saatavuuden testi TCP- tai UDP-protokollalla. Simple check ei vaadi kohdelaitteelle mitään erityisasetuksia. Zabbix käyttää ping-testiin erillistä fping ohjelmaa, joka pitää asentaa palvelinkoneelle erikseen.

3.3 Toiminta

Zabbixin toiminta perustuu seuraaviin komponentteihin, joiden avulla varsinainen monitorointi tapahtuu.

3.3.1 Isännät

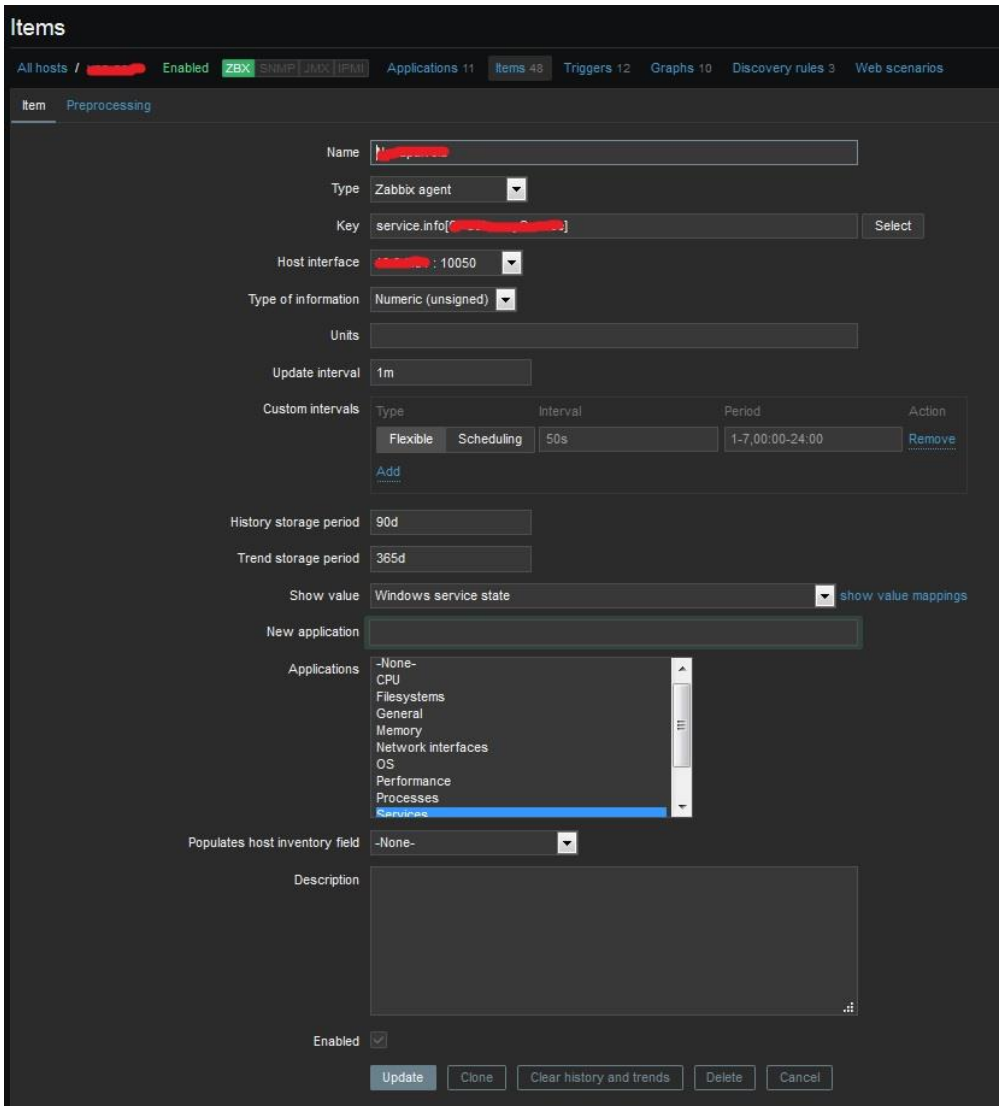
Isännät(hosts) ovat tyypillisesti monitoroitavia laitteita, joita varten luodaan objekti Zabbixiin ja jonka kautta Zabbix yhdistää kyseiseen laitteeseen. Yhdistämistä varten määritellään liitännät (interfaces), jotka laitteessa on käytössä (esim. Zabbix-agentti, SNMP jne.) ja näille IP-osoite tai DNS nimi ja portti. Isäntä myös nimetään kuvaavalla nimellä, jotta tiedetään mistä laitteesta on kyse. Yleensä on tapana nimetä isäntä samalla nimellä kuin mikä on sen isäntänimi, jolla se näkyy verkossa. Lisäksi isännät kategorioidaan ryhmiin (Host group), esim. ”Windows servers”. Jokaisen isännän pitää olla vähintään yhdessä ryhmässä (Kuva 3).



Kuva 3: Isännän luonti

3.3.2 Item

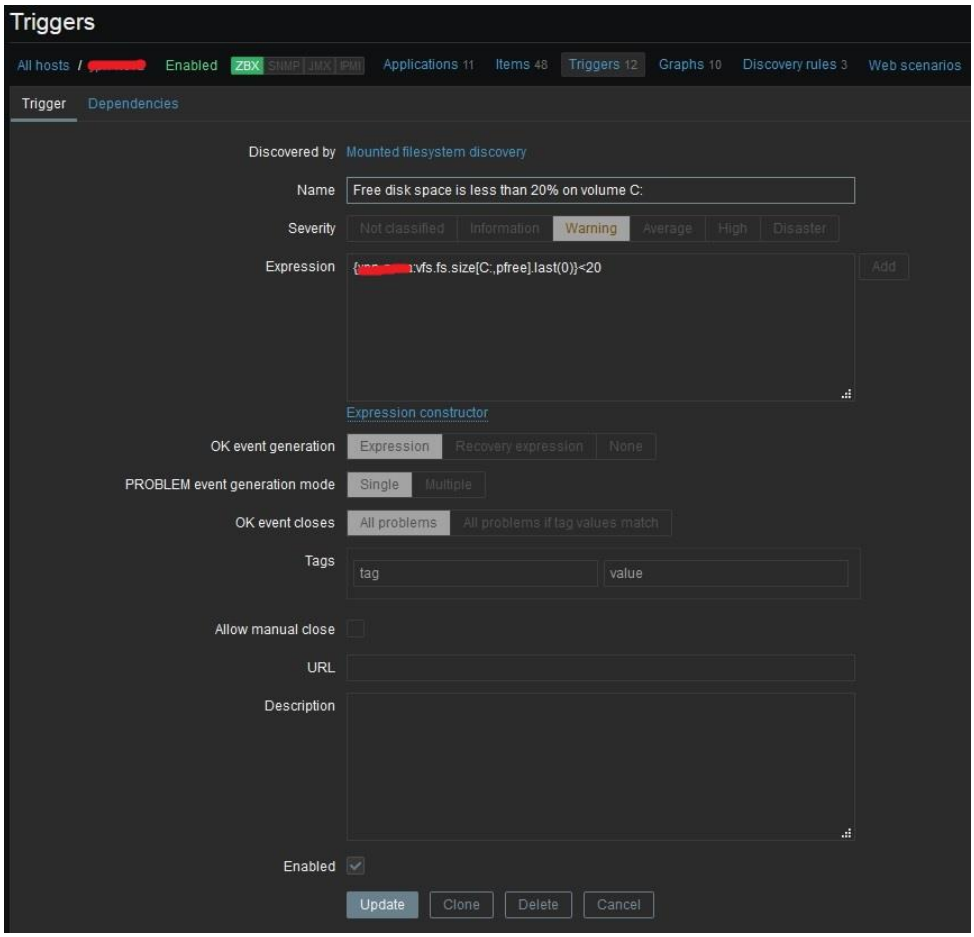
Itemit ovat objekteja, jotka luodaan isännille ja joiden tehtävänä on varsinainen datan keruu. Jokainen item hakee jonkun tietyn datapisteen tiedon isännältä. Itemille määritellään nimi, tyyppi (esim. Zabbix-agent, SNMP, jne.), avain (key), joka identifioi haettavan tiedon ja joka riippuu tyypistä. Eri tyypeille on eri asetukset, esim. SNMP:llä OID ja versio 3:n tapauksessa salausasetukset jne. Lisäksi kaikille itemeille voidaan määritellä mm. yksikkötyypit, päivitysaikavälit ja tietojen säilytysaika. Hyödyllinen toiminto on myös itemien kategorointi sovelluksiin (Applications). Esim. kaikki prosessorin suorituskykyyn liittyvät arvot voidaan laittaa ”CPU”-sovellukseen, muistin ”Memory” jne (Kuva 4).



Kuva 4: Itemin luonti

3.3.3 Trigger

Triggerit ovat loogisia lausekkeita, jotka tutkivat itemien arvoja ja joiden avulla voidaan luoda hälytyksiä tiettyjen ehtojen täyttyessä. Triggerin tilana on OK, kun ehto ei täyty ja PROBLEM, kun ehto täyttyy ja trigger ”laukeaa”. Triggerille voidaan asettaa vakavuusaste, jonka perusteella hälytystä voidaan muokata (Kuva 5).



Kuva 5: Triggerin luonti

3.3.4 Tapahtumat ja toimenpiteet

Triggerien laukeaminen tai palautuminen muodostaa tapahtumia (events), joiden avulla voidaan luoda toimenpide (action), esim. sähköpostin tai tekstiviestin lähettäminen tietyille henkilöille. Toimenpiteeseen määritellään olosuhteet, joiden pitää täyttyä ja toiminnot, jotka silloin suoritetaan. Viestien lähettämistä varten

määritetään vielä erikseen mediatyypit, esim. sähköposti, tekstiviestit jne. administrationissa.

3.4 Monitorointidatan tarkastelu ja visualisointi

Kaikki kerätty monitorointidata voidaan lukea *Monitoring/Latest data* –valikon kautta ja suodattaa isäntien, isäntäryhmien ja sovellusten mukaan. Käytännössä datan käytettävyyttä kuitenkin parannetaan eri visualisointikeinoilla, kuten kaaviot (graphs), näytöt (screens) ja kartat (maps). Lisäksi voidaan koota kokoelmaikkunoita (dashboards).

3.4.1 Kaaviot ja näytöt

Kaaviot luodaan isännille tai mallipohjille. Kaavioiden datalähteeksi liitetään itemit, joiden dataa halutaan kuvata. Kaaviotyypiksi voidaan valita ainakin viiva- ja ympyräkaaviot, jotka ovat Zabbixissa oletuksena.

Näytöt (screens) ovat kaavioista muodostettuja kokonaisuuksia, esim. tietyn palvelimen eri osien suorituskyvyt (Kuva 6). Näytöistä voidaan muodostaa diaesityksiä (slide show).

Kuva 6: Erään palvelimen suorituskyvystä koottu näyttö

3.4.2 Kartat

Isännistä ja näiden yhteyksistä voidaan luoda karttoja, joista nähdään kätevästi verkkotopologia ja mahdolliset ongelmakohdat. Karttoja voidaan visualisoida laajasti kuvien avulla.

3.4.3 Kokoelmaikkunat

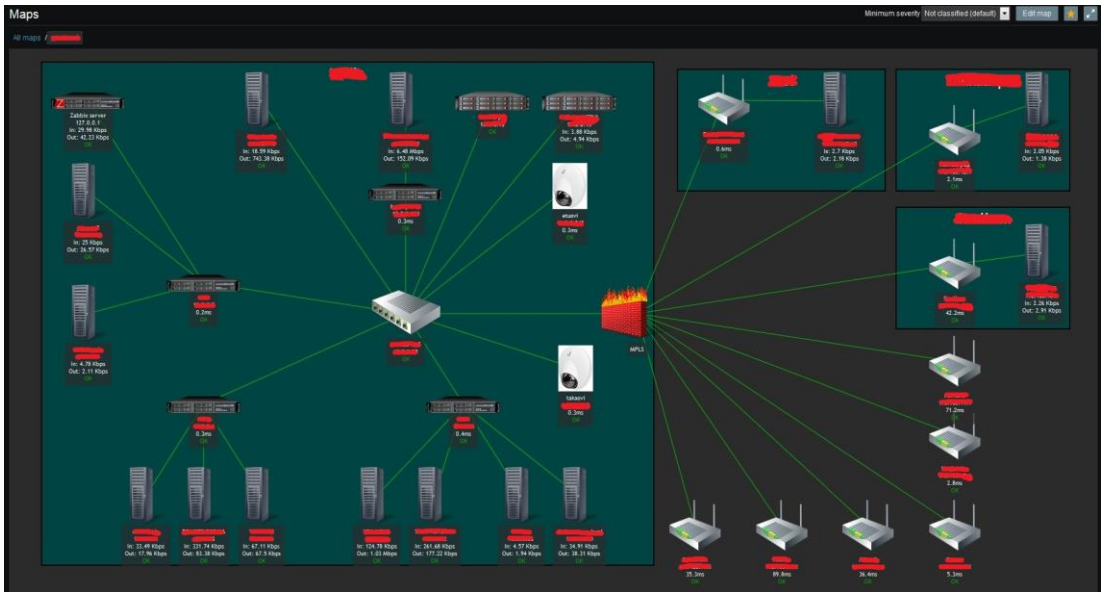
Kokoelmaikkunoihin voidaan koota laajasti eri elementtejä, kuten edellä mainitut kaaviot ja kartat ja lisäksi esim. lista kaikista tai tietyistä ongelmista ja näiden hälytyksistä.

3.5 Mallipohjat

Sen sijaan, että jokaiselle isännälle määritellään itemit, triggerit, kaaviot jne. erikseen, voidaan samantyyppisistä kokonaisuuksista luoda mallipohjia(templates), esim ”Template Windows servers”. Tämän jälkeen isäntiin voidaan liittää luotu mallipohja, jolloin se saa automaattisesti kaikki mallin objektit. Zabbixin mukana tulee laaja määrä erilaisia mallipohjia ja niitä voi myös ladata netistä ja tuoda Zabbixiin.

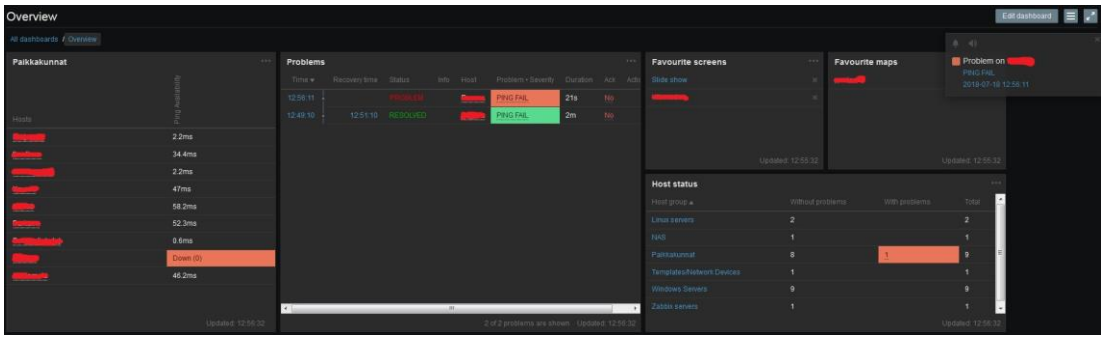
4 ZABBIX ASIAKASYRITYKSESSÄ

Yritysverkosta on luotu kartta, jossa näkyy kaikki palvelimet ja oleellisimmat verkkolaitteet, sekä yrityksen sivutoimipisteiden yhdyslaitteet. Yritys käyttää Internet-palveluntarjoajan yritysasiakasverkkoa, joka on toteutettu MPLS-tekniikalla. Kartassa oleva palomuuri kuvastaa palveluntarjoajan verkkoa, jonka kautta yhteydet kulkevat sivutoimipisteille. (Kuva 7).



Kuva 7: Verkkokartta

Yrityksen eri paikkakunnilla sijaitsevien sivutoimipisteiden nettiyhteyttä monitoroidaan käyttämällä simple checkiä, joka testaa pingillä toimipisteiden yhdyslaitteen saavutettavuutta minuutin välein ja trigger muodostaa hälytyksen jos yhteyttä ei saavuteta. Kuva 8 on havainnollistettu, millaisen hälytyksen yhteysongelma aiheuttaa ja ongelman ratketessa triggerin palautuminen *resolved*-tilaan. Ilmoituksista näkyy tapahtuman ajankohdat ja kesto. Tapahtumat tallentuvat myös historiatietoihin.



Kuva 8: Sivutoimipisteiden nettiyhteyksien monitorointi

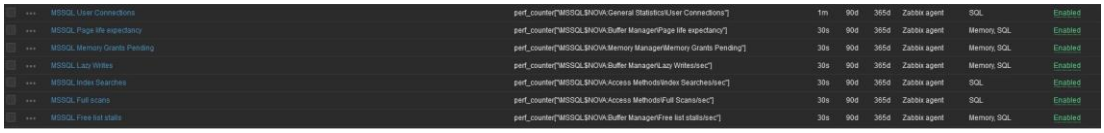
Päätoimipisteen yritysverkossa suurin osa palvelimista toimii virtuaalikoneina ESXi virtualisointialustoilla. Palvelimia monitoroidaan niihin asennetun Zabbix-agentin avulla. ESXi:tä monitoroidaan toistaiseksi vain simple checkillä, kuten myös valvontakameroita, sekä runkokytkintä SNMP:n avulla.

Palvelimien monitoroinnissa hyödynnetään laajalti valmiita Windows- ja Linux-mallipohjia ja kytkimessä yleistä HP:n kytkinten SNMP –mallipohjaa.

Palvelimista monitoroidaan ainakin laitetason suorituskykyä, esim. prosessorin käyttöaste, verkkoliikenteen määrä sisään ja ulos sekä muistin ja levytilan käyttöaste. Näistä on myös koottu palvelinkohtaiset näytöt kaavioineen (Kuva 6, s. 16).

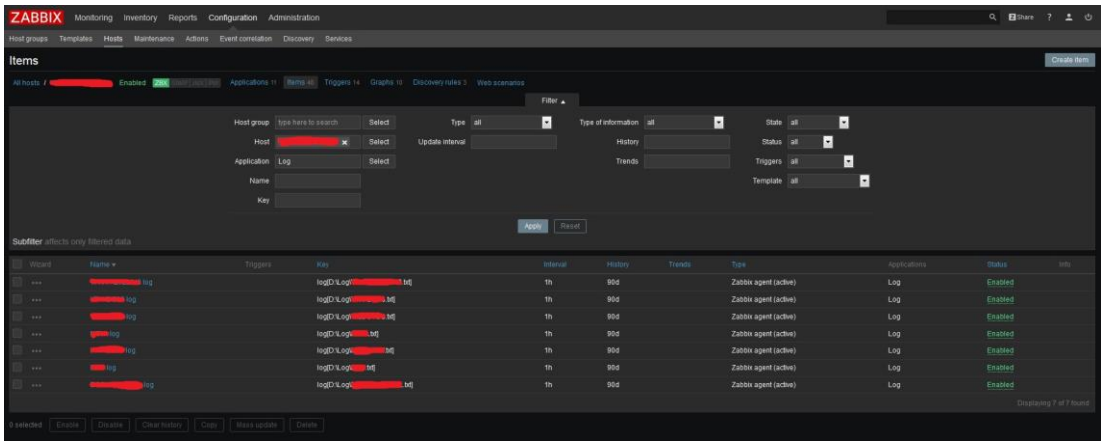
Yrityksen liiketoiminnan kannalta kriittisten ohjelmien toimintaa monitoroidaan tarkkailemalla Windows Server -palvelimella olevan palvelun tilaa, josta trigger muodostaa hälytyksen jos palvelu ei ole käynnissä.

Liiketoiminnan kannalta keskeisen MS SQL –tietokannan laskureita, kuten indeksihakujen määrä verrattuna koko tietokannan kattaviin hakuihin, monitoroidaan myös käyttämällä Windowsin Performance countereita.



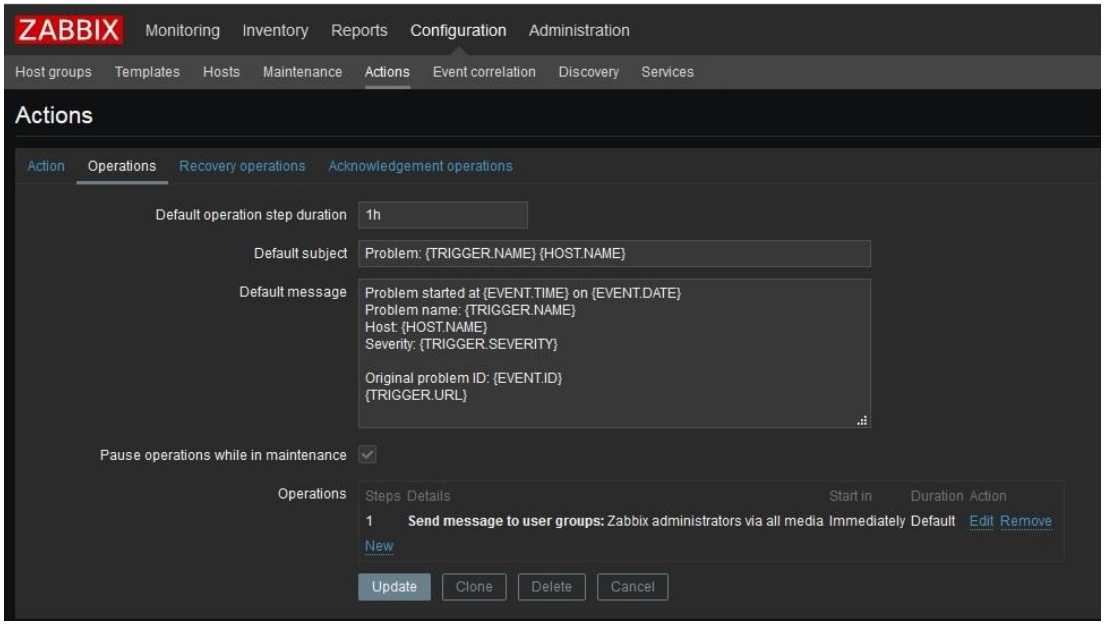
Kuva 9: MS SQL –tietokannan laskurit

Lokitiedostojen monitorointia käytetään varmuuskopiointipalvelimella. Palvelimelle otetaan määritettyinä ajankohtina varmuuskopiot muiden palvelimien datasta ja tästä toimenpiteestä kirjoitetaan lokitiedosto erikseen jokaisesta palvelimesta. Zabbix monitoroi näitä tiedostoja lokityyppisten itemien avulla (Kuva 10). Lokien sisältö on liitetty kyseisen palvelimen näyttöön, josta sitä voidaan tarkkailla muun palvelimen suorituskykydatan yhteydessä. Lisäksi esim. lokissa ilmenevän virhekoodin avulla voidaan luoda hälytyksiä.

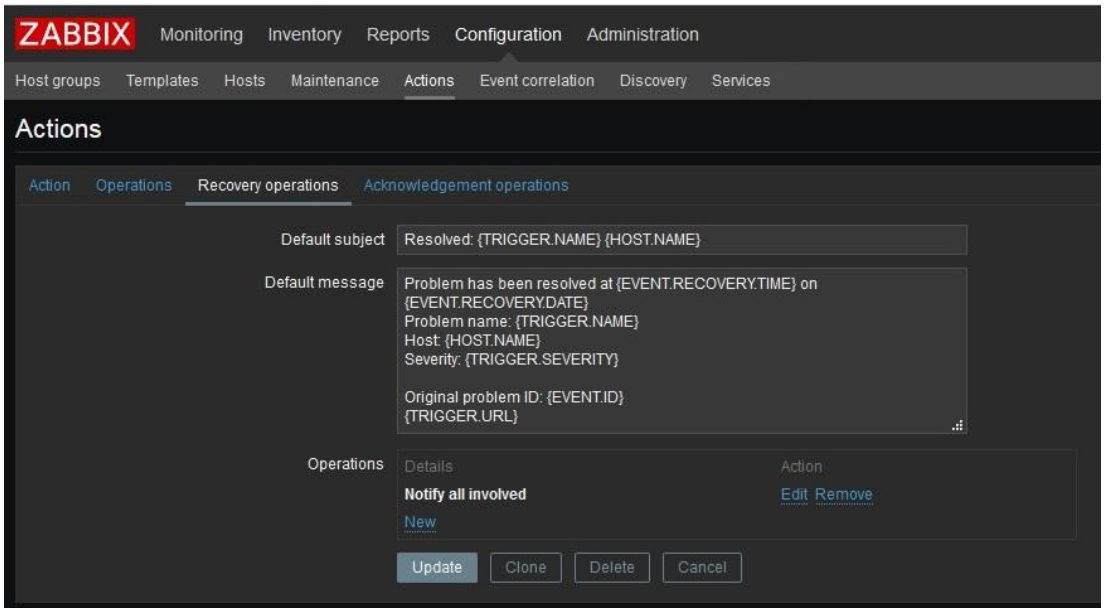


Kuva 10: Lokitiedostojen monitorointiin luodut itemit

Hälytyksistä on määritetty lähtemään sähköpostiviesti IT-vastaaville. Ilmoitukset lähtevät vikatilanteen tapahtuessa (Kuva 11) ja ratketessa (Kuva 12). Näihin on käytetty Zabbixissa oletuksena olevia toimintoja (*action*), jotka lähettävät kaikista hälytyksistä tiedon kaikille administrators-ryhmään kuuluville henkilöille. Toimintoja voidaan lisätä ja muokata vapaasti, esim. lähettää tietyistä tilanteista vain tietyille henkilöille ilmoitus.



Kuva 11: Vikailmoitusviesti



Kuva 12: Vikatilanteen ratkeamisesta lähetettävä viesti

5 YHTEENVETO

Itselläni ei entuudestaan ollut juuri kokemusta monitoroinnista ja vain rajallisesti kokemusta verkon ja järjestelmien ylläpidosta oppilaitokseni laboratorioympäristössä, joten projekti oli laaja ja haastava.

Yrityksen verkosta ei myöskään ollut saatavilla dokumentointia, joten verkkokarttaa luodessa muodostui hyvin kuva verkon rakenteesta ja siellä olevista palveluista. Mielestäni kriittisimmät laitetason ongelmat ja yhteysongelmat ovat hyvin havaittavissa ja hahmotettavissa verkkokartasta.

Aikaa vei myös Zabbixin toimintaan tutustuminen ohjelman dokumentaation, foorumien ja tutoriaalien avulla. Zabbix tarjoaa käytännössä puhtaan pöydän ja haastavaa oli miettiä, mitä ylipäätään monitoroidaan ja millaisesta informaatiosta on hyötyä. Tässä oli apuna yrityksen ICT-järjestelmäpäällikkö, joka tuntee järjestelmät parhaiten ja jolla oli paljon ideoita monitoroinnin suhteen.

Näen, että kehitettävää riittää varmasti valmiiden tai itse ohjelmoitavien lisäosien muodossa. Yksi toteuttamiskelpoinen idea olisi palvelimiin asennettavat lämpötilasensorit ja näiden monitorointi.

LÄHTEET

1. **Solarwinds.** Basics of Network Monitoring. [Viitattu: 3. 9 2018.] https://www.solarwinds.com/basics-of-network-monitoring.

2. **Solarwinds**. Network Monitoring Design Philosophy. [Viitattu: 18. 7 2018.] https://www.solarwinds.com/network-monitoring-design-philosophy.

3. **Cisco Systems.** Cisco Networking Academy. *CCNA4 Connecting Networks.* 2016. [Viitattu: 5. 9 2018.] https://www.netacad.com/.

4. **Zabbix LLC.** Zabbix Documentation 3.4. 2018. https://www.zabbix.com/documentation/3.4/manual/installation/requirements.

5. **Dalle Vacche, Andrea.** *Mastering Zabbix - Second Edition.* Birmingham: Packt Publishing, 2015.