



Osaamista  
ja oivallusta  
tulevaisuuden  
tekemiseen

Joni Kiiski

# Automaatioverkon valvonta Zabbix- ohjelmistolla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Automaatiotekniikka

Insinööriytyö

15.3.2020

Tekijä Otsikko	Joni Kiiski Automaatioverkon valvonta Zabbix-ohjelmistolla
Sivumäärä Aika	22 sivua 15.3.2020
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine	Automaatiotekniikka
Ohjaajat	Senior System Specialist Jukka-Pekka Vihmo Lehtori Kristian Junno
<p>Opinnäytetyössä tavoitteena oli käyttöönottaa asiakkaan automaatiojärjestelmässä Zabbix verkonvalvontaohjelmisto verkkolaitteissa, tärkeissä palvelimissa sekä virtuaaliklusterin osissa. Työ tehtiin Valmet Automationin Vantaan asiakaspalvelulle. Valmet Automation toimittaa, kehittää sekä uusii automaatiojärjestelmiä öljy-, energia- sekä prosessiteollisuudessa. Tarve opinnäytetyön aiheelle tuli Valmet Automationin uudeksi verkonvalvontajärjestelmäksi valikoituneesta Zabbixista, ja tarpeesta saada kokemusta siitä asiakaspalveluyksiköille</p> <p>Zabbix on avoimen lähdekoodin verkonvalvontaohjelmisto, joka asennettiin Linux -pohjaiselle käyttöjärjestelmälle omaksi virtuaaliseksi palvelimekseen. Zabbixia käytetään sekä operoidaan graafisen käyttöliittymän kautta, joka toimii verkkoselaimissa. Tässä työssä Zabbixin käyttämiä valvontaprotokollia ovat ICMP, SNMP sekä Zabbix Agent.</p> <p>Työhön kuului verkonvalvontaohjelmiston käyttöönotto, toiminnan ja operoinnin koulutus asiakkaan henkilökunnalle sekä turhien hälytyksien siivoaminen pois Zabbixista. Zabbix:ia käyttöönotettaessa asennettiin Zabbix Server ja tietokanta sekä määritettiin verkkolaitteiden valvonta- ja hälytysparametrit. Valvonta määritettiin toimimaan verkkolaitteilla ja virtuaaliklusterilla SNMP-pohjaisesti sekä Windows palvelimilla Zabbix Agentia käyttäen.</p> <p>Verkonvalvonnasta tulleiden hälytyksien avulla Zabbixin avulla säästettiin yli viisi tuntia työaikaa, kun huoltoa voitiin suorittaa ennakoivasti, jolloin siihen kului huomattavasti vähemmän aikaa. Työtä tehtäessä saatiinkin ensimmäinen Vantaan asiakaspalvelun alueelle tullut Zabbix -verkonvalvontajärjestelmä ainakin osittain tutuksi asiakaspalveluinsinööreille. Verkonvalvontajärjestelmä saatiin myös liitettyä vuoden 2020 alusta asiakkaan palvelusopimuksen osaksi, jolloin sekä käyttö että kehitystyöt jatkuvat myös tulevaisuudessa.</p>	
Avainsanat	Verkonvalvonta, Zabbix

Author Title Number of Pages Date	Joni Kiiski Automation Network Monitoring with Zabbix Software 22 pages 15 March 2020
Degree	Bachelor of Engineering
Degree Programme	Electrical and Automation Engineering
Professional Major	Automation Engineering
Instructors	Jukka-Pekka Vihmo, Senior System Specialist Kristian Junno, Senior Lecturer
<p>The aim of this thesis work was to implement Zabbix network monitoring software on network devices, important servers and virtual cluster components in the customer's automation system. The work was done for Valmet Automation's customer service in Vantaa. Valmet Automation supplies, develops and renews automation systems for the oil, energy and process industries. The need for this thesis topic came from Valmet Automation's new network management system, Zabbix, and the need to gain experience with it for customer service units.</p> <p>Zabbix is an open source network monitoring software that was installed on a Linux-based operating system as its own virtual server. Zabbix is accessed and operated through a graphical user interface that runs on web browsers. The monitoring protocols used by Zabbix in this work are ICMP, SNMP, and Zabbix Agent.</p> <p>The work included deploying network monitoring software, training functions and operating for the customer's staff, and cleaning up unnecessary alarms off Zabbix. When Zabbix was deployed, a Zabbix server and database were installed, and monitoring and alert parameters for network devices were configured. Supervision was configured to work on network devices and virtual cluster SNMP-based, and on Windows servers using Zabbix Agent.</p> <p>With network monitoring alarms, Zabbix saved more than five hours of work time, allowing for proactive maintenance, which took much less time. As a result, the first Zabbix network management system that came to Vantaa's customer service area was at least partially familiar to customer service engineers. The network monitoring system was also included as part of the customer service agreement from the beginning of 2020, so both operation and development work will continue in the future.</p>	
Keywords	Network monitoring, Zabbix

## Sisällys

### Lyhenteet

1	Johdanto	1
2	Valmet	2
2.1	Valmetin historia	2
2.2	Valmet Automation	2
3	Zabbix	3
4	Toimintaperiaate	4
4.1	Zabbixin toimintaperiaate	4
4.2	Valvontaprotokollat	5
4.2.1	Zabbix Agent	5
4.2.2	ICMP	5
4.2.3	SNMP	6
5	Zabbixin käyttöönotto	7
5.1	Zabbix Serverin käyttöönotto	7
5.2	Valvottavien kohteiden määrittäminen	8
6	Zabbixin käyttö	13
6.1	Hälytykset ja niihin reagoiminen	14
6.2	Valvonnassa olevien laitteiden ja datan seuranta	16
7	Zabbixista saatavat hyödyt	18
8	Yhteenveto	21
	Lähteet	22

## Lyhenteet

CPU	<i>Central Processing Unit.</i> Laitteen keskusyksikkö.
DNA	<i>Dynamic Network of Applications.</i> Valmetin DNA-niminen automaatiojärjestelmä.
ICMP	<i>Internet Control Message Protocol.</i> Tietoliikenteen kontrolliprotokolla, jolla lähetetään viestejä nopeasti laitteiden välillä.
IP	<i>Internet Protocol.</i> Tietoliikenneprotokolla, joka huolehtii tietoliikennepaketien toimittamisesta pakettikytkentäisessä verkossa.
LAN	<i>Local Area Network.</i> Paikallinen tietoverkko.
NTP	<i>Network Time Protocol.</i> Protokolla täsmällisen aikatiedon siirtämiseen tietokoneiden välillä.
TCP	<i>Transmission Control Protocol.</i> Tietoliikenneprotokolla yhteyksien luomiseen tietokoneiden välille.
RAM	<i>Random Access Memory.</i> Tietokoneohjelmien työmuisti, johon ladataan käyttöjärjestelmän sekä sovelluksien tarvitsemat tiedot.
SNMP	<i>Simple Network Management Protocol.</i> Tietoliikenneprotokolla, jonka avulla voidaan selvittää esimerkiksi verkossa olevan laitteen tilatietoja.
SMTP	Simple Mail Transfer Protocol. Protokolla, jonka avulla voidaan välittää viestejä sähköpostipalvelimien kesken.
VLAN	<i>Virtual LAN.</i> Virtuaalisesti toteutettu LAN.
VPN	<i>Virtual Private Network.</i> Virtuaalinen erillisverkko, jonka avulla useampi verkko voidaan yhdistää julkisen verkon yli.

## 1 Johdanto

Opinnäytetyö tehtiin Valmet Automationin Vantaalle sijaitsevalle Customer Service -yksikölle. Vantaan Customer Service -yksikössä palvelee Uudenmaan alueella sijaitsevia asiakasyrityksiä, ja kehitetään heillä jo olemassa olevia automaatiojärjestelmiä. Työtä aloittaessa Zabbix oli otettu käyttöön Valmetin toimesta muutamalla asiakkaalla Suomessa ja tässä työssä käsiteltävä käyttöönotto on Vantaan yksikön ensimmäinen.

Tarve opinnäytetyön aiheelle tuli Valmet Automationin uudeksi verkonvalvontajärjestelmäksi valikoituneen Zabbixin käyttöönotosta ja tarpeesta saada siitä kokemusta Vantaan asiakaspalveluyksikölle sekä saada Zabbix saatettua palvelutuotteeksi. Aikaisemmin Valmetilla oli ollut käytössä Nagioksen verkonvalvontajärjestelmä sekä muutamia verkkoanalysointilaitteita, mutta näiden vanhentuuksa tuli tarve saada selkeämpää ja keskittynyttä valvontaa asiakkaille. Tämän seurauksena Valmetilla on valittu Zabbix uudeksi verkonvalvontajärjestelmäksi.

Palvelutuotteena Zabbix toimii siten, että Valmet toimittaa asiakkaan automaatiojärjestelmän liitteeksi Zabbixin, josta molemmat osapuolet hyötyvät. Zabbix Serverin kautta voidaan tulevista hälytyksistä generoida sähköpostiviestit lähtemään määriteltyihin sähköpostiosoitteisiin. Tällöin saadaan tarkkaa tietoa hälytyksen alkuperästä sekä Valmetin palveluhenkilöstölle sekä asiakkaan omalle laitoshenkilökunnalle, jonka avulla ongelmanratkaisun nopeus voi nopeutua huomattavasti. Myöhemmin aiheena ollut Zabbix-järjestelmä saatiinkin liitettyä palvelusopimukseen asiakkaalle.

## 2 Valmet

### 2.1 Valmetin historia

Valmet on yksi maailman johtavista teknologian kehittäjistä ja toimittajista, jonka historia alkaa vuodesta 1797 Tampereen Verkatehtaalta kankaiden valmistuksesta. Nämä toiminnot ovat nykyään osa Valmetin Palvelut-liiketoimintalinjaa. Vuonna 1951 yrityksen nimeä Valmet käytettiin ensimmäistä kertaa Valtion Metallitehtaiden muuttaessa nimeään. Valmet toimitti ensimmäisen paperikoneensa vuonna 1953, ja kohosi 1960-luvulla johtavaksi toimittajaksi.

Vuonna 1999 syntyi Metso, kun Valmet ja Rauma fuusioituivat yhdeksi yhtiöksi. Vuonna 2013 Metso jakautui Metsoksi ja Valmetiksi, jolloin Metson Massa, paperi ja voimantuotanto -liiketoimintalinjat siirtyivät toimimaan Valmet nimen alla. Vuonna 2015 Valmet osti Metsolta prosessiautomaatiojärjestelmät liiketoiminnan. [1].

Nykyään Valmetilla on neljä liiketoimintalinjaa. Vuonna 2018 Valmetilla oli ollut liikevaihtoa 3325 miljoonaa euroa ja henkilöstöä 12528 henkilöä. Liiketoimilinjoista suurin on Palvelut, jonka osuus liikevaihdosta on 37 % koko Valmetin liikevaihdosta. Seuraavina ovat Paperi (28 %) sekä Sellu ja energia (26 %). Pienin Valmetin liiketoimintalinjoista on Automaatio, jonka liikevaihto on 9 % Valmetin kokonaisliikevaihdosta. [2, s. 9.]

### 2.2 Valmet Automation

Valmet Automationilla oli vuonna 2018 henkilöstöä noin 1750 henkilöä Valmetin kokonaishenkilöstöstä, eli noin 14 % [2, s. 9]. Automaatioliiketoimintalinjan pääasiallisia tuotteita ovat Valmet DNA -automaatiojärjestelmät sekä automaatiojärjestelmien ja -järjestelmiin liitettävät analysaattori- sekä mittalaitteet.

Automaation -liiketoimintalinjan asiakasryhmät koostuvat paperiteollisuudesta, energian tuotannosta, öljy- ja kaasuteollisuudesta sekä prosessiteollisuudesta. Valmetin DNA -automaatiojärjestelmiä käytetään myös valtamerilaivojen automatisoinnissa. Valmetin ensimmäinen automaatiojärjestelmä on toimitettu vuonna 1979, ja tämän jälkeen Valmet

on toimittanut toimintansa aikana yhteensä yli 4500 automaatiojärjestelmää maailmanlaajuisesti. [3.]

### 3 Zabbix

Zabbix on samannimisen yrityksen kehittämä avoimen lähdekoodin verkonvalvontaohjelmisto. Zabbixin kehitystyö on aloitettu vuonna 1998, ja ensimmäinen julkinen versio on julkaistu vuonna 2001. Ensimmäinen vakaa versio ohjelmasta on julkaistu vuonna 2004. Yrityksenä Zabbix SIA on perustettu vuonna 2005. [4.]

Zabbixin avulla voidaan verkossa valvoa jopa sataa tuhatta yksittäistä laitetta, joista voidaan kerätä yhteensä jopa kymmentä miljoonaa erilaista tilatietoa. Ohjelman avulla voidaan myös tehdä laitteille tuhansia tarkistuksia sekunnissa. Tilatietoja ohjelma kerää laitteilta pääasiassa SNMP:n, ICMP:n tai Zabbix Agentin avulla. Käytännössä tilatietojen kerääminen toimii siten, että Zabbixin palvelimelle on määritetty laitelistaus sekä ennalta määritetty millä tavalla tietoja kerätään laitteilta. [5.]

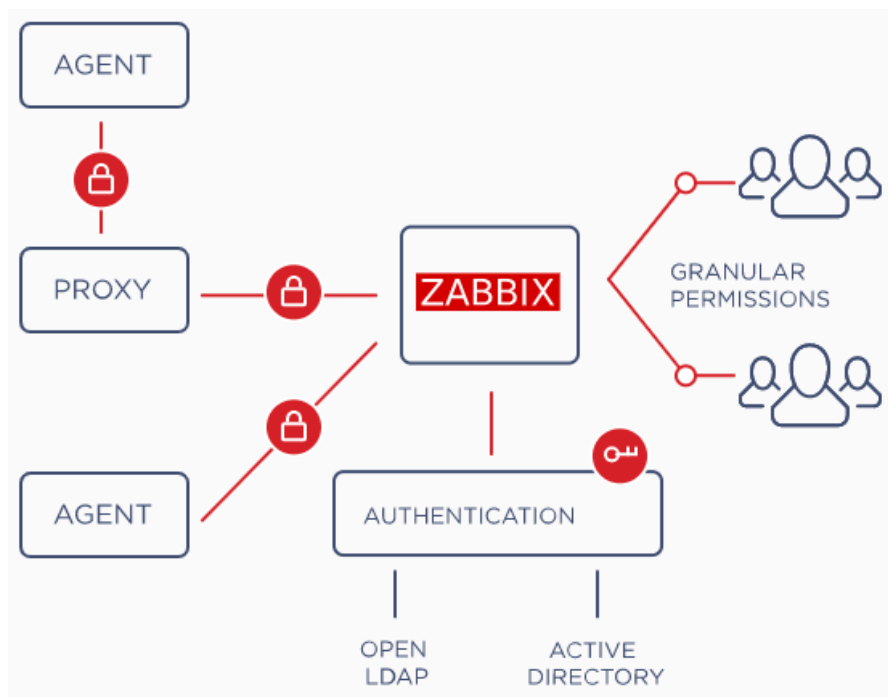
Zabbixin avulla voidaan valvoa esimerkiksi laitteiden prosessoriyksiköiden kuormituksen määrää, kovalevyjen täyttymisen astetta, sekä tuulettimien nopeuksia ja tuuletettävien kohteiden lämpötiloja, mikäli laite kykenee itse näitä tietoja antamaan. Zabbixilla voidaan myös valvoa laitteiden käynnissä olon tilaa sekä aikaa, sekä esimerkiksi kytkimistä uusien laitteiden kytkeytymistä verkkoon. Periaatteellisella tasolla Zabbixin avulla voidaan valvoa laitteen kaikkea antamaa diagnostiikkaa, kun valvontatyökalut ovat konfiguroitu tätä varten. Käytännössä tämä ei kuitenkaan ole tarpeellista, sillä laitteilla on myös paljon sellaista tietoa, jotka eivät ole tietyissä laiteympäristöissä tarpeellisia tietää. [5]

Zabbixia kuten muitakin verkonvalvontaohjelmistoja käytetään, jotta saadaan lisää tietoa verkosta ja sen kunnosta. Verkonvalvontaohjelmistot auttavat suunnittelemaan huolto- toimenpiteitä laitteille ennakoivasti, ja antavat dataa laitteista pitkältä ajalta. Verkonvalvontaohjelmistojen avulla voidaan myös diagnosoida ongelmia verkossa jopa laitteiden porttitasolta alkaen. Myös tietoturva paranee, sillä verkonvalvontaohjelmistojen avulla saadaan konfiguroitua hälytys tulemaan aina, kun aikaisemmin käyttämättömään porttiin liitetään uusi laite.

## 4 Toimintaperiaate

### 4.1 Zabbixin toimintaperiaate

Zabbix on avoimeen lähdekoodiin perustuva verkonvalvontaohjelmisto, joka voidaan asentaa Linux-pohjaisille käyttöjärjestelmille. Kuvassa 1 esitellään Zabbixin perustoimintaperiaate, ja se kuinka Zabbix Agentit voivat olla yhteydessä palvelimeen. Kuvassa oikealla puolella on esitelty eri käyttöoikeuksia vaativat käyttäjäryhmän, ja vasemmalla puolella Zabbix Agentin liitännäismahdollisuudet, eli joko suoraan palvelimelle, taikka välityspalvelimen kautta liittäminen. Tässä työssä Zabbix on asennettu Linux-käyttöjärjestelmälle, joka on asennettu virtuaaliklusteriin omaksi virtuaaliseksi palvelimekseen. Zabbix ohjelmana toimii siis keskitettynä palvelimena, joka kysyy tilatietoja valvomiltaan laitteilta erilaisien tekniikoiden avulla. Näitä tekniikoita ovat TCP/IP-pinosta ICMP ja SNMP sekä Zabbixin oma ohjelma Zabbix Agent, jota käytetään Windows -asemissa.



Kuva 1. Zabbixin toimintaperiaate [6].

Zabbixia käytetään graafisen käyttöliittymän kautta, joka toimii selaimessa. Käyttöliittymään voidaan erikseen määrittellä jokaiselle käyttäjälle tai käyttäjäryhmälle omat tunnukset eriarvoisilla käyttöoikeuksilla, jolloin voidaan seurata ja rajoittaa kunkin käyttäjän tekemiä toimia.

## 4.2 Valvontaprotokollat

### 4.2.1 Zabbix Agent

Zabbix Agent on Zabbixin luoma erikseen asennettava ohjelma laitteille, joilta ei voida tai haluta kysyä tilatietoja SNMP:n avulla. Tässä työssä Zabbix Agent on asennettu Windows-laitteille, ja niiden tilatietoja valvotaan Agentin avulla.

Zabbix Agent voi toimia joko passiivisessa tai aktiivisessa tilassa. Passiivisessa tilassa Zabbix Server kyselee ennalta määritetyn kyselyvälin mukaisesti tilatietoja Agentilta, ja Agent kertoo sen hetkiset tiedot. Aktiivisessa tilassa toimiessaan Agent pyytää palvelimelta listan valvottavista tiedoista ja lähettää tiedot eteenpäin. Aktiivisessa tilassa toimiessaan Zabbix Agent vaatii laitteelta, jolle se on asennettu hieman enemmän resursseja, mutta vähentää tarvittavia resursseja Zabbix -palvelimen puolelta. Agentin käyttö onkin suositeltavampaa aktiivisessa tilassa, kun valvottavia kohteita on paljon, jolloin vaadittavia resursseja saadaan jaoteltua useammille laitteille. [7.]

### 4.2.2 ICMP

ICMP:llä eli Internet Control Message Protocol on TCP/IP-pinossa verkkokerrokseen kuuluva protokolla, jota käytetään verkkolaitteiden kommunikaatio-ongelmien diagnosoinnissa. ICMP:n avulla tarkastetaan saavuttaako lähetetty viesti kohteensa, ja sen pääkäyttötarkoitukset ovat vikaraportointi sekä verkkodiagnostiikan suorittaminen. [8.]

Usein verkkodiagnostiikassa käytössä olevista komennoista traceroute ja ping komennot toimivat käyttäen ICMP:tä. Mikäli valvottava kohde ei tue SNMP:tä, Zabbixissa voidaan pingata sitä suoraan Zabbix -palvelimelta, jolloin kohteeseen ei tarvitse asentaa Zabbix Agentia. Tällöin kohteesta voidaan valvoa vain verkossaoloa, minkälaisella onnistumisprosentilla kohde vastaa takaisin sekä sitä, kuinka kauan vastauksen tuleminen kestää.

Mikäli valvottavasta kohteesta halutaan saada tätä enemmän tietoa, on käytettävä joko Zabbix Agentia tai SNMP:tä.

#### 4.2.3 SNMP

SNMP eli Simple Network Management Protocol on protokolla, jolla suoritetaan verkkohallintaan ja laitteiden tilatietoihin liittyviä kyselyitä. SNMP -protokollasta on olemassa kolme eri versiota, SNMPv1, SNMPv2 ja SNMPv3, joista tässä työssä oleva Zabbix Server käyttää tilatietojen kyselyihin SNMPv2 protokollaa.

Zabbix Server kysyy tilatietoja SNMP:n avulla laitteilta, jotka ovat konfiguroitu SNMP:llä valvottaviksi. Virtuaaliklusterin laitteistosta SNMP:llä valvotaan kaikkia fyysisiä komponentteja järjestelmässä. Verkkolaitteilta Valmetin konfiguroimalla Zabbixilla valvotaan SNMP:llä esimerkiksi seuraavia tietoja:

- CPU:n eli keskusprosessoriyksikön kuormitus
- yleiset laitteeseen liittyvät tiedot, esimerkiksi MAC numerot sekä versiotiedot
- verkkoliikennetiedot
- laitteen käynnissäoloaika.

SNMP:n avulla voidaan valvoa myös laitteita, joihin tässä tapauksessa on asennettu Zabbix Agent, mutta tällöin laitteilta ei saataisi yhtä laaja-alaisesti kerättyä tietoja. Tämä olisi kuitenkin hyvä vaihtoehto, jos valvottavalla laitteella olisi kuormitus jo valmiiksi korkea, jolloin vältettäisiin lisää kuormittavan ohjelmiston asentaminen.

## 5 Zabbixin käyttöönotto

### 5.1 Zabbix Serverin käyttöönotto

Zabbix Server asennetaan Valmetin sisäisen ohjeen mukaisesti virtuaaliklusteriin, josta sille varataan resursseja vähintään kaksi CPU -ydintä, 4 GB RAM -muistia sekä noin 40 GB kovalevytilaa. Virtuaaliklusteri on vähintään kahdesta eri tietokoneesta rakennettu palvelin, jossa pienellä määrällä tehokkaita tietokoneita käyttäen voidaan klusterin sisälle asentaa suurempi määrä virtuaalisia tehoisempia tietokoneita. Zabbixin kohdalla käyttöjärjestelmäksi on valittu Debian Linux, ja Zabbixista käytettävä versio on 4.0. Zabbix Server toimitetaan asiakkaalle virtuaaliklusteriin valmiiksi asennettuna ja konfiguroituna virtuaaliasemana, jonka jälkeen määritetään asemalle seuraavat asiat:

- Nimi
- Ip-osoitteisto ja Gateway-osoite
- NTP-palvelimen osoite, josta saadaan tarkka kellonaika asemalle
- SMTP-palvelimen osoite, jonka kautta Zabbix voi lähettää tulevat hälytykset sähköpostilla ennalta määritettyihin osoitteisiin.

Kun Zabbix Serverin perusasetukset on saatu kuntoon, on vuorossa Zabbixin tietokannan konfiguroinnin vuoro. Tietokantaa konfiguroidessa sille annetaan tietokannan skeema eli malli taulujen ja taulujen sarakkeiden rakenteesta, joka on ennalta määritelty tietynlaiseksi Valmetin toimittamissa asennuksissa.

Tietokannan konfiguroinnin jälkeen vuorossa on vielä verkon palomuurien sääntöjen muuttaminen, jotta Zabbix pystyy valvomaan myös laitteita muista verkoista kuin mihin se on asennettu. Palomuurin sääntöjä pitää muuttaa muun muassa seuraavilta kohdin:

DMZ-verkosta Valmet DNA-verkkoon

- ICMP
- SNMP
- Zabbix Agent
- NTP

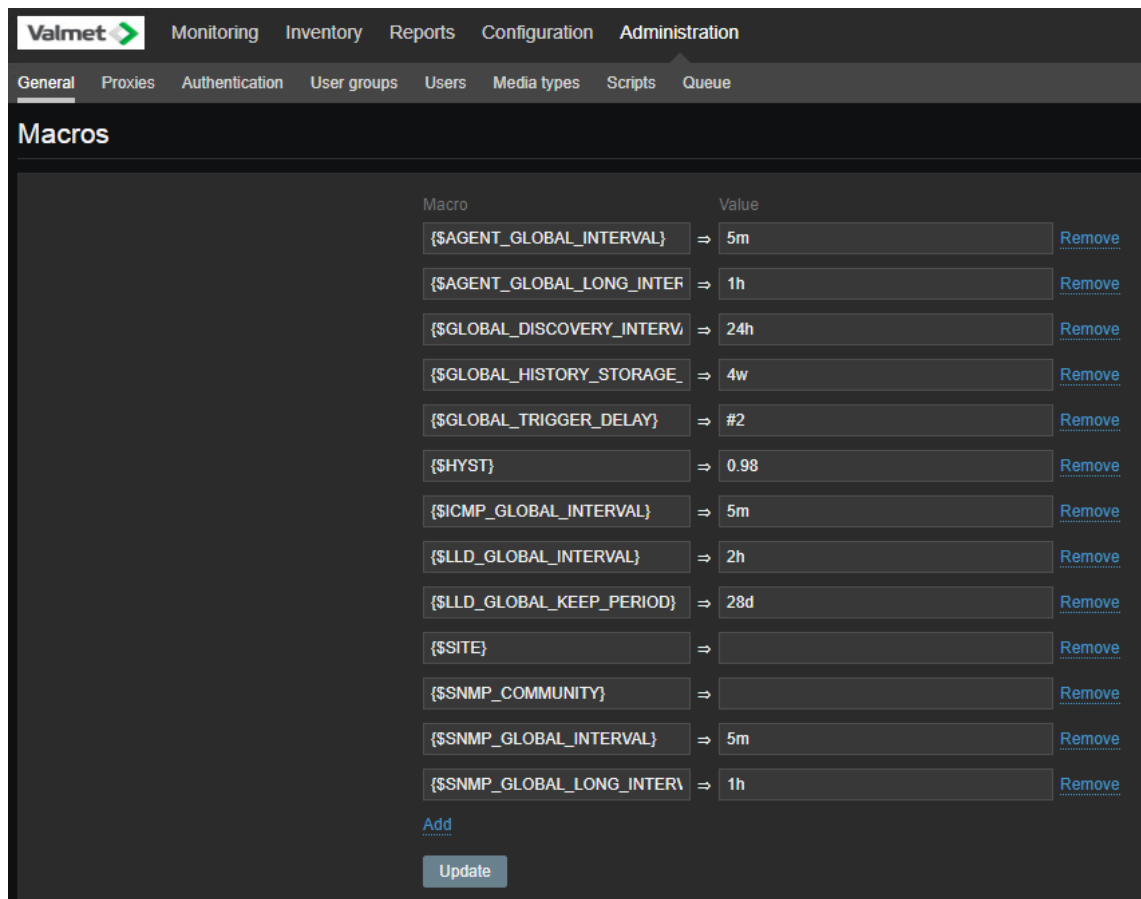
## Valmet DNA-verkosta DMZ-verkkoon

- SNMP-loukku, jonne kerätään valvottavien kohteiden SNMP -viestit
- Zabbix Agent active, jos käytössä aktiivinen agentti.

### 5.2 Valvottavien kohteiden määrittäminen

Kun Zabbix Server on saatu asennettua ja konfiguroitua, on aika alkaa konfiguroimaan Zabbixille valvottavia kohteita. Valvottavaksi kohteiksi valikoitiin verkkolaitteet, virtuaaliklusterin laitteisto sekä info- sekä tietoturvapalvelimet, jotka ovat Windows -pohjaisella käyttöjärjestelmällä toimivia. Windows -pohjaisille asemille asennettiin Zabbix Agent -ohjelmisto, jolloin niiltä voitiin valvoa dataa laajemmin ja tarkemmin kuin SNMP-pohjaisella valvonnalla. Verkkolaitteissa sekä virtuaaliklusterissa valvonta on SNMP-pohjaista, sillä kyseisiltä laitteilta saadaan riittävän laajat tiedot SNMP-kyselyillä.

Windows-asemille asennettava Zabbix Agent saadaan ladattua valmiiksi konfiguroituna Zabbix Serveriltä. Agentia asemalle asennettaessa ei tarvitse tehdä muuta kuin määrittää konfigurointitiedostolle Zabbix Serverin osoite, sekä asentaa ja käynnistää ohjelma komentoriviltä. Kun Agent on asennettu asemalle, pitää kyseinen asema saada liitettyä vielä Zabbix Serverin valvottavaksi. SNMP:llä valvottaville laitteille ei tarvitse tehdä muuta, kuin varmistaa että kyseisillä laitteilla on SNMP-valvonnan mahdollisuus kytketty päälle. Tämän jälkeen varmistetaan valvottavien kohteiden SNMP -yhteisö ja määritetään tämä Zabbix Serverin makroiin eli ennalta määriteltyihin muuttujiin. Kuvassa 2 on esitelty Valmetin konfiguroimalla Zabbix Serverillä tulevat oletusmakrot, joita muokataan tarvittaessa jokaiselle asiakkaalle sopiviksi.



Kuva 2. Zabbix Serverin makrot.

Päätelaitteita valvonnan piiriin määrittäessä aloitetaan lajittelemalla laitteet eri ryhmiin, jotka tämän työn tapauksessa ovat seuraavat:

- Network Devices (Verkkolaitteet)
- VM Hardware (Virtuaaliympäristön laitteet)
- Hosts (Windows-palvelimet)
- Zabbix Servers (Zabbix -palvelin)

Kun valvottavat kohteet on saatu lajiteltua sopiviin ryhmiin, aloitetaan kohteiden liittämisen Zabbixin valvonnan piiriin "Auto Discovery" -toiminnolla. Toiminnossa määritetään valvottavien kohteiden IP-osoitteisto, hakuvälin pituus sekä se, mitä tarkastuksia kohteille tehdään. Kuvassa 3 on esimerkkinä "Sample Agent Discovery", jossa tarkastuk-

sina käytetään ICMP -yhteyskokeilua sekä etsitään Zabbix Agentteja valmiiksi määritelystä IP-osoitteista. Hakuvälin pituudeksi esimerkissä on määritelty makro "{\$GLOBAL\_DISCOVERY\_INTERVAL}" joka on tässä tapauksessa kuvassa 2 esitelty 24 tuntia.

The screenshot shows the Zabbix Discovery rules configuration page. The form includes the following fields and options:

- Name:** Sample Agent Discovery
- Discovery by proxy:** No proxy
- IP range:** 192.168.0.30, 192.168.0.45, 192.168.0.50
- Update interval:** {\$GLOBAL\_DISCOVERY\_INTERVAL}
- Checks:**
  - ICMP ping (with Edit and Remove links)
  - Zabbix agent "system.uptime" (with Edit and Remove links)
  - New (with a plus icon)
- Device uniqueness criteria:**
  - IP address
  - Zabbix agent "system.uptime"
- Enabled:**
- Buttons:** Update, Clone, Delete, Cancel

Kuva 3. Valvottavien kohteiden haku Zabbix Serverille.

Kun valvottaville kohteille on määritelty sopivat hakutoiminnot, siirrytään varsinaiseen hakuun, jossa määritetään, minkälaiset suureet täyttäessään kohdetta aletaan valvomaan. Konfiguroinnin toiminnot -välilehdellä määritellään toiminnot, jolloin valvottaville kohteille tehdään toimenpiteitä. Kuvassa 4 on esitetty määriteltävät toiminnot, jotka ovat toimintoryhmän nimi, se missä tapauksissa kohteet hyväksytään valvottaviksi sekä miltä IP-osoite alueelta etsitään valvottavia kohteita.

Valmet Monitoring Inventory Reports Configuration Administration

Host groups Templates Hosts Maintenance Actions Event correlation Discovery Services

## Actions

Action Operations

\* Name

Type of calculation  A and (B or C)

Conditions	Label	Name	Action
A		Discovery rule equals <i>Sample Agent Discovery</i>	<a href="#">Remove</a>
B		Received value contains <i>Windows</i>	<a href="#">Remove</a>
C		Received value contains <i>windows</i>	<a href="#">Remove</a>

New condition

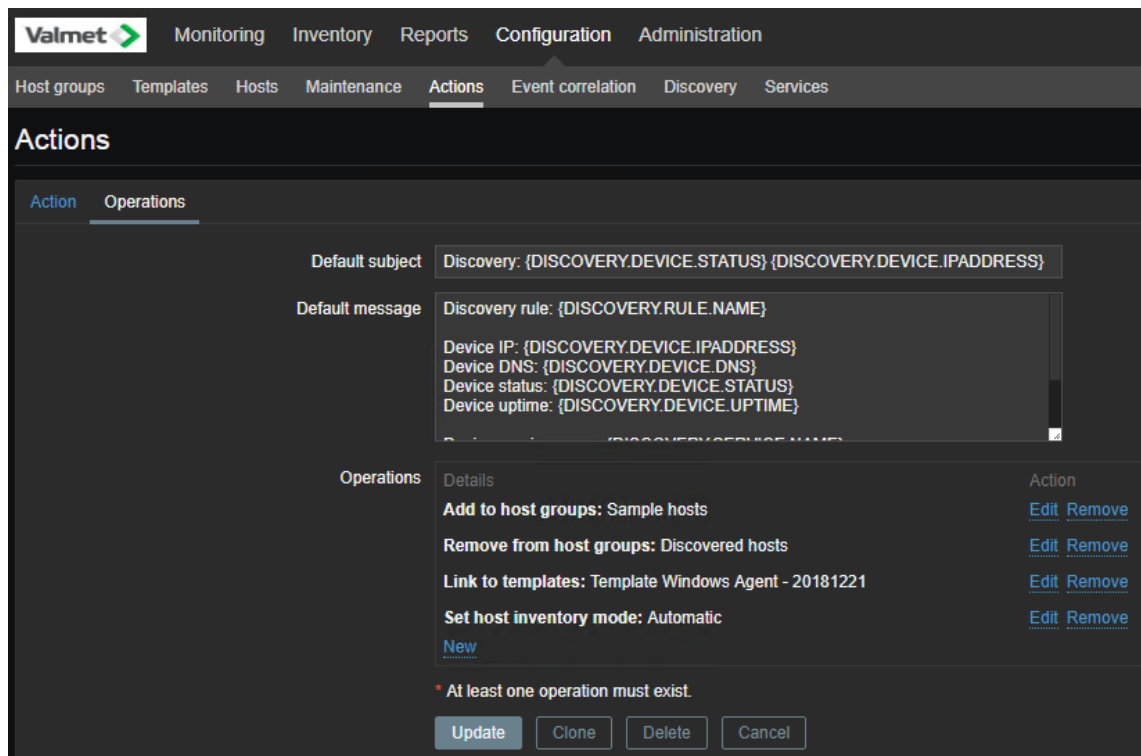
[Add](#)

Enabled

\* At least one operation must exist.

Kuva 4. Valvottavien kohteiden hakuparametrit.

Kun konfiguroinnin toimintaehdot on saatu määriteltyä, siirrytään operaatiot -välilehdelle, jossa määritetään kyseiselle ryhmälle tehtävät operaatiot, joista tärkeimpänä on oikeaan ryhmään siirtäminen sekä tälle ryhmälle kohdistettavan valvontamallin määrittäminen. Kuvissa 4 ja 5 esimerkkeinä ovat Windows Agenttien valvonnan määrittäminen IP-osoitealueilta 192.168.0.1-127 sekä 192.168.2.1, jossa valvottavat kohteet siirretään "Sample hosts" -ryhmään, poistetaan "Discovered hosts" -ryhmästä sekä määritetään valvontamalliksi "Template Windows Agent – 20181221".



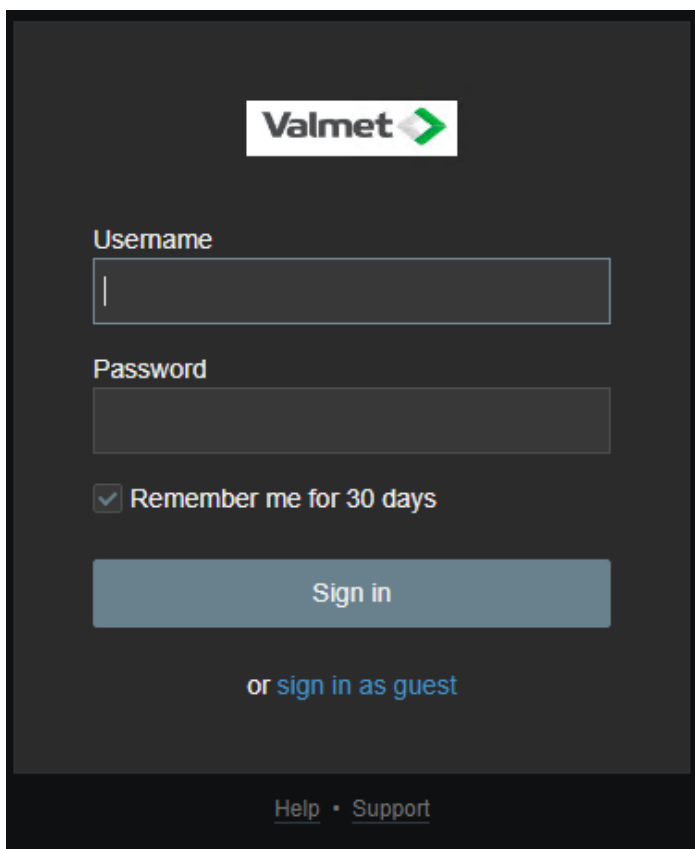
Kuva 5. Valvonnan operaatioiden määrittäminen.

Valvottavien kohteiden hälytykset sekä valvottavat asiat määritetään valvontamalleissa, ja näin saadaan samantyyppisille laitteille yhdellä kertaa samanlaiset hälytykset, jolloin voidaan välttää yhdeltä kohteelta yhdenlaisen valvottavan osion unohtuminen täysin. Valvontamalleja voi tehdä itse tai käyttää valmiiksi tehtyjä malleja. Valmiita valvontamalleja löytyy paljon Zabbixin omilta sivuilta sekä myös käyttäjien itse tekemiä sekä Zabbixin sivuilta, että muilta tietojen jakamiseen tarkoitetuilta sivuilta, esimerkiksi Githubista.

Itse tehtyjen valvontamallien etuna on se, että rajoitetun laiteympäristön järjestelmissä voidaan myös valvontamalleista karsia ylimääräiset ja kyseisessä ympäristössä turhat tiedonkeruut pois. Valvontamallien itse tekeminen vaatii kuitenkin aikaa sekä perehtymistä asiaan, jolloin turhien tietojen keruun oleminen Zabbix -palvelimella saattaa olla järkevämpi vaihtoehto kuin käyttää useita tunteja työtä muutamaaan turhaan tiedonkeruuseen. Tässä työssä käytetyt valvontamallit ovat Valmetin tuotekehityksen tuottamia valvontamalleja, jotka ovat kohdennettu juuri Valmetin automaatiojärjestelmiin.

## 6 Zabbixin käyttö

Kun Zabbix Server on saatu konfiguroitua Linuxin komentorivillä, Zabbixia operoidaan ja konfiguroidaan verkkoselaimella. Oletuksena osoite on <zabbix serverin ip-osoite>/zabbix, jolloin päästään kirjautumisikkunaan, joka on kuvassa 6. Kirjautumisikkunasta voidaan joko kirjautua määritellyillä käyttäjätunnuksilla, tai kirjautua vierailijakäyttäjällä, jolloin käyttöoikeudet rajoittuvat vain katseluoikeuksiin. Muita käytössä olevia käyttöoikeuksia ovat Zabbix admin sekä Zabbix super admin. Zabbix admin -käyttäjät voivat operoida Zabbixia sekä konfiguroida uusia valvottavia kohteita. Zabbix super admin -käyttäjät voivat lisäksi konfiguroida käyttöoikeuksiin liittyviä asetuksia.

The image shows a dark-themed login interface for Zabbix. At the top center is the Valmet logo, which consists of the word "Valmet" in white and a green arrow pointing to the right. Below the logo are two input fields: "Username" and "Password". Under the password field is a checked checkbox labeled "Remember me for 30 days". Below these fields is a large, light blue "Sign in" button. Underneath the button is the text "or sign in as guest" in a lighter blue color. At the bottom of the interface, there are two links: "Help" and "Support", separated by a small dot.

Kuva 6. Valmetisoitu Zabbix kirjautumisikkuna.

Sisään kirjautuessa ensimmäisenä aukeaa monitoroinnin perusnäkyvä, joka näyttää aktiiviset hälytykset, niiden vakavuuden sekä järjestelmään liittyvää informaatiota. Perusnäkyvää voi myös kustomoida haluamansa näköiseksi, jolloin saadaan juuri kyseisen laitoksen tärkeät näkymät esiin. Perusnäkyvästä voidaan siirtyä valikoissa eteenpäin

valitsemalla ensin päävalikko, eli kuvassa 7 Valmet -logon vieressä olevat viisi kohtaa, jonka jälkeen valitaan alavalikko, joka johtaa halutulle sivulle käyttöliittymässä.

The screenshot shows the Valmet monitoring interface. At the top, there are navigation tabs: Monitoring, Inventory, Reports, Configuration, and Administration. Below these are sub-tabs: Dashboard, Problems, Overview, Web, Latest data, Graphs, Screens, Maps, Discovery, and Services. The main content area is titled 'Global view' and contains two panels. The left panel, 'System information', displays a table of system parameters. The right panel, 'Problems by severity', shows a table with columns for Host group, Disaster, High, and Average. At the bottom, there is a 'Problems' section with filters for Time, Info, Host, Problem + Severity, Duration, and Ack.

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	162	40 / 0 / 122
Number of items (enabled/disabled/not supported)	7758	6817 / 394 / 547
Number of triggers (enabled/disabled [problem/ok])	5159	5054 / 105 [0 / 5054]
Number of users (online)	5	1
Required server performance, new values per second	22.67	

Kuva 7. Zabbixin perusnäkyvä.

## 6.1 Hälytykset ja niihin reagoiminen

Monitoroinnin perusnäkyvää katsottaessa nähdään vain aktiiviset hälytykset, mutta mikäli halutaan tarkkailla myös vanhoja hälytyksiä, voidaan valita päävalikosta "Monitoring" ja tämän jälkeen alavalikosta "Problems". Tällöin saadaan auki sivu, joka näyttää hälytyshistorian. Oikeassa reunassa olevasta valikosta voidaan myös vaihtaa hälytyshistorian ajanjaksoa pidemmäksi ja tarvittaessa voidaan hälytyksiä valvoa jopa kahden vuoden takaa.

Kuvassa 8 on esimerkki hälytyshistoriasta, jossa tarkkaillaan hälytyksiä viimeisen kolmen kuukauden ajalta. Kuvassa näkyvä hälytys on tullut uudesta kytkimen verkkoporttiin liitetystä prosessiasemasta. Kuvassa olevaan hälytykseen on reagoitu ja sen vakavuus on muutettu pienemmäksi, sillä kyseinen prosessiaseman lisäys oli suunniteltu, jolloin tulleella hälytyksellä ei ollut tarvetta olla vakava.

Kuva 8. Hälytyshistoria.

Hälytyksiin voidaan myös reagoida. Tällöin mikäli laitoksella on useampi henkilö, jotka tarkkailevat verkon tilaa Zabbixin kautta, tietävät he, kun hälytyksen aiheuttanut asia on otettu selvitykseen. Hälytykseen reagoinnin näkee hälytyslistalla hälytyksen kohdalta ”Ack”. Kuvassa 8 kyseisessä kohdassa lukee vihreällä ”Yes”, joka tarkoittaa, että hälytykseen on reagoitu. Mikäli hälytykseen ei ole reagoitu, kyseisessä kohdassa lukee punaisella ”No”. Hiirtä liikuttamalla hälytyksen reagoinnin päälle nähdään myös, milloin reagointi on tapahtunut ja onko hälytykseen reagoinut henkilö jättänyt viestin, joka antaa lisätietoja asiaan, kuten kuvassa 9 esitetään.

Kuva 9. Hälytykseen reagoitu.

## 6.2 Valvonnassa olevien laitteiden ja datan seuranta

Valvottavien laitteiden luettelo löytyy Zabbixista "Inventory" -päävalikon alta menemällä "Hosts" -alavalikkoon. Valvonnassa olevat laitteet voidaan joko listata kaikkien laitteiden mukaan tai yksittäistien laiteryhmiin mukaan. Tätä kautta voidaan valita haluttu laite ja muokata tarvittavia valvonta- sekä hälytysparametrejä laitekohtaisesti. Tämä voi olla tarpeen, mikäli yhden laitteen olosuhteet poikkeavat suuresti muista laitteista, joille on automaattisesti luotu valvonta- ja hälytysparametrit.

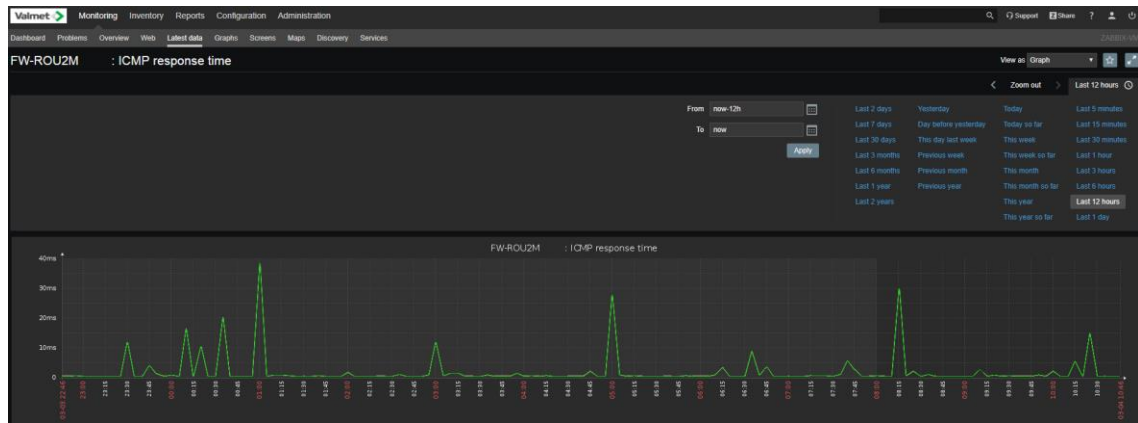
Valvonnanassa olevien laitteiden tilatietoja ja dataa voidaan Zabbixissa seurata reaaliaikaisesti "Monitoring" ja "Latest data" -välilehden alta. Laitteiden dataa voidaan valvoa joko ryhmäkohtaisesti tai laitekohtaisesti, kuten kuvassa 10 valvotaan. Valvottava kohde haetaan "Host groups" tai "Hosts" kenttän ryhmän tai laitteen nimeä kirjoittamalla, jolloin Zabbix osaa itse ehdottaa sopivia ryhmiä tai laitteita. Data päivittyy sivulle muutaman sekunnin välein, riippuen laitteiden valvontaa käyttöönotettaessa määritellyistä yleisistä tai laitekohtaisista makroista.

The screenshot shows the Valmet monitoring interface. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. Below this is a secondary navigation bar with 'Dashboard', 'Problems', 'Overview', 'Web', 'Latest data', 'Graphs', 'Screens', 'Maps', 'Discovery', and 'Services'. The 'Latest data' section is active, showing a filter section with 'Host groups', 'Hosts' (set to 'FW-ROU2M'), and 'Application'. Below the filter is a table of data for the host 'FW-ROU2M'.

Host	Name	Last check	Last value	Change
FW-ROU2M	CPU (1 Item)			
	CPU utilization	2020-03-04 10:25:53	19 %	
FW-ROU2M	General (7 Items)			
FW-ROU2M	Network Interfaces (dot3StatsTable) (60 Items)			
FW-ROU2M	Network Interfaces (ifTable) (72 Items)			
FW-ROU2M	Network Interfaces (ifxTable) (44 Items)			
FW-ROU2M	Status (5 Items)			
	Device uptime	2020-03-04 10:25:53	85 days, 10:53:50	+00:05:00
	ICMP loss	2020-03-04 10:25:53	0 %	
	ICMP ping	2020-03-04 10:25:53	Up (1)	
	ICMP response time	2020-03-04 10:25:53	14.7ms	+10ms
	SNMP availability	2020-03-04 10:29:45	available (1)	

Kuva 10. Valvottavan laitteen datan reaaliaikainen seuranta.

Dataa voidaan tarkastella myös käyrämuodossa, jolloin voidaan arvioida datassa tapahtuneita muutoksia jopa kahden vuoden ajalta helposti. Käyrän avaaminen tapahtuu valitsemalla "Graph" -kohta kuvassa 10 olevalta riviltä, jolloin siirrytään kyseisen rivin valvontapisteen graafiseen dataan, joka on esiteltynä kuvassa 11. Käyrän pituudeksi voidaan valita mikä vain arvo väliltä yhdestä minuutista kahteen vuoteen, joista kuvassa 11 on valittuna 12 tuntia. Kuvassa 11 näkyvän käyrä kuvaa reitittimen ICMP -pingin vastauksen pituutta viimeisen 12 tunnin ajalta.



Kuva 11. Datakuvaaja 12 tunnin ajalta.

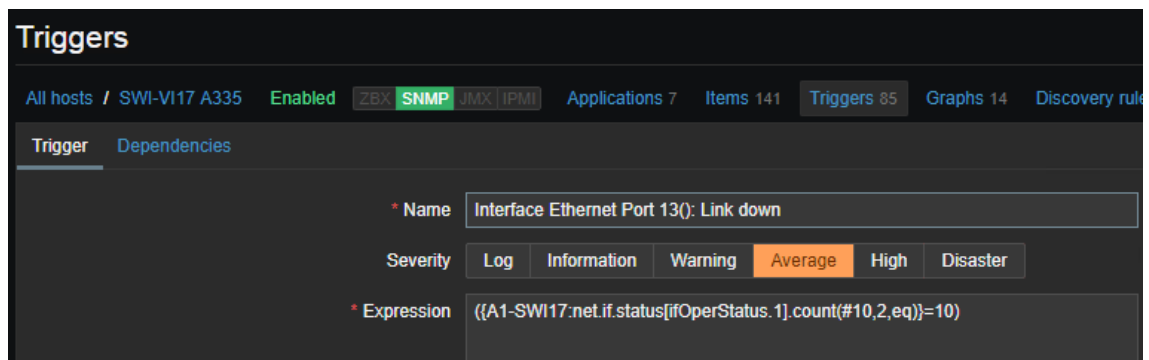
## 7 Zabbixista saatavat hyödyt

Automaatioverkon valvonnassa Zabbixista saatavat hyödyt voivat olla todella suuria, sillä verkkolaitteiden vikaantumiset saattavat aiheuttaa todella suuria tuotantomenetyksiä, jotka voivat johtaa suuriin taloudellisiin menetyksiin. Tästä syystä on tärkeää valvoa automaatioverkon kuntoa, joka on käytännössä koko laitoksen operoinnin selkäranka. Automaatiojärjestelmissä verkkolaitteet ovat yleensä kahdennetut, mutta mikäli laitteiden laiteohjelmistoissa on virheitä, saadaan Zabbixin avulla hälytykset verkosta hävinneestä laitteesta heti kun laitteen toiminta huononee, vaikka se ei kokonaan loppuisikaan.

Kuten kaikissa asioissa, myös Zabbixissa on sekä hyviä, että huonoja puolia. Huonoja puolia Zabbixin operoinnin kannalta ovat väärät hälytykset sekä niiden mahdollinen suuri määrä. Tämä lisää työkuormaa verkonvalvontaa käyttöönottaessa, sillä juuri valvonnan alkuvaiheiden aikaan nähdään turhat hälytykset, jotka tulevat valmiista valvonta- ja hälytyspohjista. Turhien hälytyksien poistaminen on myös hyvä tehdä vasta muutaman kuukauden kuluttua Zabbixin käyttöönotosta, jolloin voidaan tarkastella kyseisen hälytyksen vanhaa dataa, joka antaa lisää tietoja onko hälytys sittenkään turha, vai pitääkö jossakin muualla tehdä muutoksia, jotta kyseistä hälytystä ei tulisi. Turhien hälytyksien tuleamista voidaan välttää edelleen kehittämällä valvonta- sekä hälytyspohjia.

Suurimpana turhien hälytyksien aiheuttajana tämän työn aikana oli yhden kytkimen yhdestä portista lähtevä langaton yhteys toiselle kytkimelle, joka kulki pitkän matkan suuren

tien ylitse. Kyseinen langaton yhteys katkesi useasti päivässä ja generoikin noin 90 hälytystä kolmen päivän aikana. Tällöin hälytys tuli aina kun yhteys katkesi ja oli päällä viisi minuuttia, jonka aikana yhteys tuli takaisin. Yhteyden tilaa tarkasteltaessa huomattiin, että pisimmillään yhteys oli poikki 45 minuuttia, ja kun hälytysviivettä kasvatettiin 50 minuuttiin, ei turhia hälytyksiä katkeilevasta yhteydestä enää tullut. Kuvassa 12 esitellään hälytysviiveen kasvattaminen Expression -kohdassa. Kyseisessä kohdassa hälytys laukaistaan vasta, kun edellisellä kymmenellä tilatietojen kyselykerralla portti on ollut pois käytöstä. Tilatietojen kyselyväli on aikaisempien makrojen mukaisesti viisi minuuttia, joten hälytys tulee voimaan vasta kun portti on ollut pois päältä 50 minuuttia.



Kuva 12. Hälytysviiveen muokkaaminen hälytyslaukaisimelle.


Zabbixin avulla voidaan myös ennustaa mahdollisia tulevia ongelmia järjestelmässä, jolloin niihin voidaan puuttua hyvissä ajoin ja täten välttää taloudellisia tappioita. Kuvassa 13 on esimerkki, kuinka Zabbix Server ilmoittaa uudesta hälytyksestä sähköpostitse esiasetettuihin sähköpostiosoitteisiin. Kun sähköpostiviesti ongelmista saadaan liikkeelle heti ongelman tultua sekä Valmetin huoltohenkilökunnalle että laitoksen omalle henkilökunnalle, päästään vian korjaaminen aloittamaan nopeasti ja tehokkaasti oikeassa paikassa. Zabbix parantaa myös tietoturvaa laitoksella, jossa se on asennettuna, sillä verkkolaitteiden hälytyspohja määrittää hälytykset myös sille, kun uusi laite liitetään verkkoon tai kun laite liitetään verkkoporttiin, joka on aikaisemmin ollut tyhjänä.

## Average: SWI : Interface Ethernet Port 13(): Link down



-zabbix@ .fi  
Vastaanottaja Joni M Kiiski



 Viestistä poistettiin ylimääräiset rivinvaihdot.

Problem started at 08:10:30 on 2019.05.29 Problem name: Interface Ethernet Port 13(): Link down

Host: SWI-

Severity: Average

Sender: SITE-FIXX -VM

Problem description:

Original problem ID: 164922

Kuva 13. Zabbixin lähettämä sähköposti hälytyksestä.

Tässä työssä käyttöön otetun Zabbix Serverin avulla kyettiin myös kyseisellä laitoksella välttämään ongelma, joka olisi tulevaisuudessa voinut olla työläämpi korjata. Kyseisessä tapauksessa laitoksen tietoturvapalvelimelta oli kovalevytila vähissä, ja tällöin Zabbix hälytti kovalevytilan vähenemisestä. Mikäli kovalevytila olisi kokonaan loppunut palvelimelta, ei laitokselle olisi tietoturvapäivitykset saapuneet automaattisesti, jolloin ne olisi pitänyt päivittää manuaalisesti palvelimelle. Kun kovalevytilaa lisättiin, kului työaika vain noin kymmenen minuuttia sen sijaan, että tietoturvapäivitykset olisi manuaalisesti päivitetty, jolloin aikaa olisi kulunut noin kuusi tuntia.

Ohjelman käyttöönotto sekä konfiguroiminen oli asiaan perehtymisen sekä neuvojen kysymisen jälkeen helppoa. Zabbixin verkkosivuilta saatavissa oleva manuaali on selkeä ja erittäin paljon informaatiota sisältävä. Ohjelman graafinen käyttöliittymä on hyvin käytäjäystävällinen ja moderni, ja se toimii kaikilla yleisimmillä verkkoselaimilla. Nykyaikaisuutta Zabbixin käyttöliittymässä kuvastaa myös vaalean sekä tumman tilan mahdollisuudet. Tällä hetkellä Zabbixin käyttöliittymä on käännetty täysin 11 eri kielelle, ja myös käännösprojekti suomeksi on käynnissä vapaaehtoisvoimin. [9.]

## 8 Yhteenveto

Tavoitteena opinnäytetyössä oli saada kokemusta Vantaan asiakaspalvelulle Zabbix verkonvalvontaohjelmistosta, saada Zabbix toimintaan asiakkaan järjestelmään sekä liittää se osaksi asiakkaan palvelusopimusta. Työtä tehtäessä saatiinkin ensimmäinen Vantaan asiakaspalvelun alueelle tullut Zabbix -verkonvalvontajärjestelmä ainakin osittain tutuksi asiakaspalveluinsinööreille. Verkonvalvonnan käyttöönottoon liittyi myös operoinnin koulutus kyseisen laitoksen henkilökunnalle sekä turhien hälytyksien siivoaminen pois verkonvalvontaohjelmistosta.

Käyttökokemukset Zabbixista ovat hyvät, ja tarve keskitetylle modernille verkonvalvonnalle on olemassa Valmetin asiakaskunnassa. Tämän työn myötä Vantaan asiakaspalvelulle on saatu hyvin kokemusta Zabbixista, ja tässä työssä olevaa järjestelmää voidaan käyttää mahdollisesti referenssinä myös tuleville Zabbix -verkonvalvontajärjestelmille. Verkonvalvontajärjestelmä saatiin myös liitettyä vuoden 2020 alusta asiakkaan palvelusopimuksen osaksi, jolloin sekä käyttö että kehitystyöt jatkuvat myös tulevaisuudessa.

## Lähteet

- 1 Valmetin historia. 2019. Verkkoaineisto. Valmet Oyj. <<https://www.valmet.com/fi/valmet-yrityksena/valmet-lyhyesti/historia/>>. Luettu 12.4.2019.
- 2 Vuosikatsaus 2018. 2019. Verkkoaineisto. Valmet Oyj. <[https://www.valmet.com/globalassets/investors/reports--presentations/annual-reports/2018/valmet\\_vsk\\_2018\\_fi\\_secured.pdf](https://www.valmet.com/globalassets/investors/reports--presentations/annual-reports/2018/valmet_vsk_2018_fi_secured.pdf)>. Luettu 12.4.2019.
- 3 Valmetin liiketoiminnat, automaatio. 2019. Verkkoaineisto. Valmet Oyj. <<https://www.valmet.com/fi/valmet-yrityksena/valmet-lyhyesti/liiketoiminnat/automaatio/>>. Luettu 12.4.2019.
- 4 Open Source Enterprise Monitoring with Zabbix. 2012. Verkkoaineisto. Vladishev Alexei. <[https://web.archive.org/web/20120226220044/http://www.netways.de/uploads/media/Alexei\\_Vladishev\\_Open\\_Source\\_Monitoring\\_with\\_Zabbix.pdf](https://web.archive.org/web/20120226220044/http://www.netways.de/uploads/media/Alexei_Vladishev_Open_Source_Monitoring_with_Zabbix.pdf)>. Luettu 23.4.2019.
- 5 General Brochure. 2019. Verkkoaineisto. Zabbix LCC. <[https://assets.zabbix.com/files/Brochures/General\\_Brochure\\_3.2.pdf](https://assets.zabbix.com/files/Brochures/General_Brochure_3.2.pdf)>. Luettu 26.4.2019
- 6 Zabbixin ominaisuudet. 2019. Verkkoaineisto. Zabbix LCC. <<https://www.zabbix.com/features>>. Luettu 4.9.2019
- 7 Zabbix Agent. 2019. Verkkoaineisto. Zabbix LCC. <[https://www.zabbix.com/zabbix\\_agent](https://www.zabbix.com/zabbix_agent)>. Luettu 5.9.2019
- 8 What is the ICMP?. 2020. Verkkoaineisto. Cloudflare, Inc. <<https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/>>. Luettu 23.11.2019
- 9 List of localizations. 2020. Verkkoaineisto. Zabbix LCC. <<https://www.zabbix.org/pootle/>> Luettu 6.3.2020