Toni Korpi

Zabbix verkkovalvonta yrityskäytössä

Tradenomi,
Tietojenkäsittely

Syksy / Kevät 2015

KAJAANIN
AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

TIIVISTELMÄ

Tekijä: Korpi, Toni

Työn nimi: Zabbix verkkovalvonta yrityskäytössä

Tutkintonimike: Tradenomi (AMK), tietojenkäsittely

Asiasanat: Zabbix, Nagios

Tämän opinnäytetyön tarkoituksena on selvittää Zabbix verkkovalvontaohjelmiston toiminta yrityskäytössä. Lisäksi Zabbixia verrataan toiseen verkkovalvontaohjelmistoon, Nagois XI:hin, tarkoituksena arvioida, onko Zabbix toimiva vaihtoehto kaupalliselle tuotteelle.

Opinnäytetyö toteutettiin pystyttämällä testiympäristö Kajaanin AMK:n tietojärjestelmälaboratorioon ja perehtymällä kumpaankin ohjelmistoon. Työn kirjallinen osio muodostuu sekä kummankin ohjelmiston dokumentaatioista ja käyttöoppaista kootusta tiedosta sekä projektin aikana opituista asioista. Työ keskittyy kuvailemaan vain Zabbixin keskeisiä osa-alueita ja toimintoja ja lopuksi esittelee projektin aikaisten kokemusten perusteella arvion siitä, onko Zabbix toimiva vaihtoehto Nagios XI:lle.

Lopputuloksena voidaan todeta Zabbixin ja Nagios XI:n olevan toiminnoiltaan lähes samanlaiset. Kumpikin ohjelmisto kykenee samaan, eriävin menetelmin. Pääasiallinen ero on käyttöliittymässä ja aloittelijaystävällisyydessä.

ABSTRACT

Author: Korpi, Toni

Title of the Publication: Zabbix network monitoring in enterprise environment

Degree Title: Bachelor of Business Administration,

Keywords: Zabbix, Nagios

Purpose of this thesis is to determine effectiveness Zabbix network monitoring software in company usage. In addition to that, Zabbix is compared with another network monitoring software, Nagios XI, with intention of determining if Zabbix is valid alternative to commercial product.

Thesis was made by setting up test environment datacenter lab at Kajaani University of applied sciences and testing out both software. Literal portion of this thesis is formed from information gathered by reading documentation and user guides of both software and experiences gained during the project. Thesis focuses on describing integral part of Zabbix only and in the end, based on experiences gained during project, presents evaluation if Zabbix is valid alternative for Nagios XI.

In the end it can be determined that both Zabbix and Nagios XI are almost identical on their functionalities. Both software are capable of doing the same with slightly different methods. Main difference can be found in user interface and beginner friendliness.

ALKUSANAT

Opinnäytetyö sai aiheensa ollessani työharjoittelussa. Yksi tehtävistäni harjoittelun aikana oli Zabbix SNMP valvontaan tutustuminen, asennus ja kehittäminen. Harjoittelun kesto ei ollut riittävä Zabbix:n syvällisempään tutustumiseen, mutta ohjelma vaikutti lupaavalta käyttöympäristössä. Asiasta keskusteltiin, ja sovittiin että jatkaisin Zabbix:n tutkimista opinnäytetyön merkeissä.

Sisällysluettelo

SYMBOLILUETTELO

API: Application Programming Interface

CPU: Central Processing Unit

DBMS: DataBase Management Systems

FTP: File Transfer Protocol

HTTP: Hypertext Transfer Protocol

IAB: Internet Architecture Board

IPMI: Intelligent Platform Management Interface

JCP: Java Community Process

JMX: Java Management eXtension

JSON: JavaScript Object Notation

LDAP: Lightweight Directory Access Protocol

MIB: Management Interface Base

ODBC: Open DataBase Connectivity

OID: Object Identifier

PHP: PHP Hypertext Preprocessor

RegExp: Regular Expression

SNMP: Simple Network Management Protocol

SOAP: Simple Object Access Protocol

SQL: Structured Query Language

SSH: Secure Shell

TCP/IP: Transmission Control Protocol/Internet Protocol

1 JOHDANTO

Tämä opinnäytetyö on toteutettu Kajaanin ammattikorkeakoulussa kesällä 2015. Työn tarkoituksena on tutustua Zabbix verkkovalvontaohjelmistoon yritystason näkokulmasta, selvittäen sen ulottuvuudet ja rajat sekä tutustua Zabbix:n toimintoihin ja selvittää, kuinka toimivia ne ovat keskisuuren yrityksen ympäristössä. Zabbixia myös verrataan toiseen verkkovalvontaohjelmisto Nagios XI:hin. Tämän vertailun tavoitteena on selvittää, kykeneekö ilmainen, avoimen lähdekoodin Zabbix kilpailemaan kaupallisen tuotteen kanssa. Vertailtavaksi valittiin Nagios XI, koska se on listattu korkealla useissa verkkovalvontaohjelmistojen arvioissa ja testiversion saaminen oli yksinkertaista. Vertailussa ei ole tarkoitus mennä yksityiskohtiin Nagios XI:n käytöstä ja toiminnasta, vaan kuvata lyhyesti opinnäytetyöprosessin aikana saatuja vaikutelmia Nagios XI:stä Zabbixin toimintaan.

Tämän opinnäytetyön tarkoituksena ei ole ollä käyttöohje Zabbixin käyttöön, vaan esitellä Zabbixissa olevat verkkovalvontatyökalut ja pohtia niiden käyttömahdollisuuksia. Opinnäytetyö käyttää useissa tilanteissa englanninkielisiä nimiä ja termejä Zabbixin osa-alueista ja toiminnoista, sillä vaikka kyseinen yhdistelmä englannin ja suomen kieltä saattaa näyttää oudolta, suomennokset kyseisistä termeistä aiheuttaisivat todennäköisesti sekaannusta ja vaikeuttaisivat ymmärrystä, mitä Zabbixin kohdetta kyseisessä tilanteessa käsitellään.

2 ZABBIX

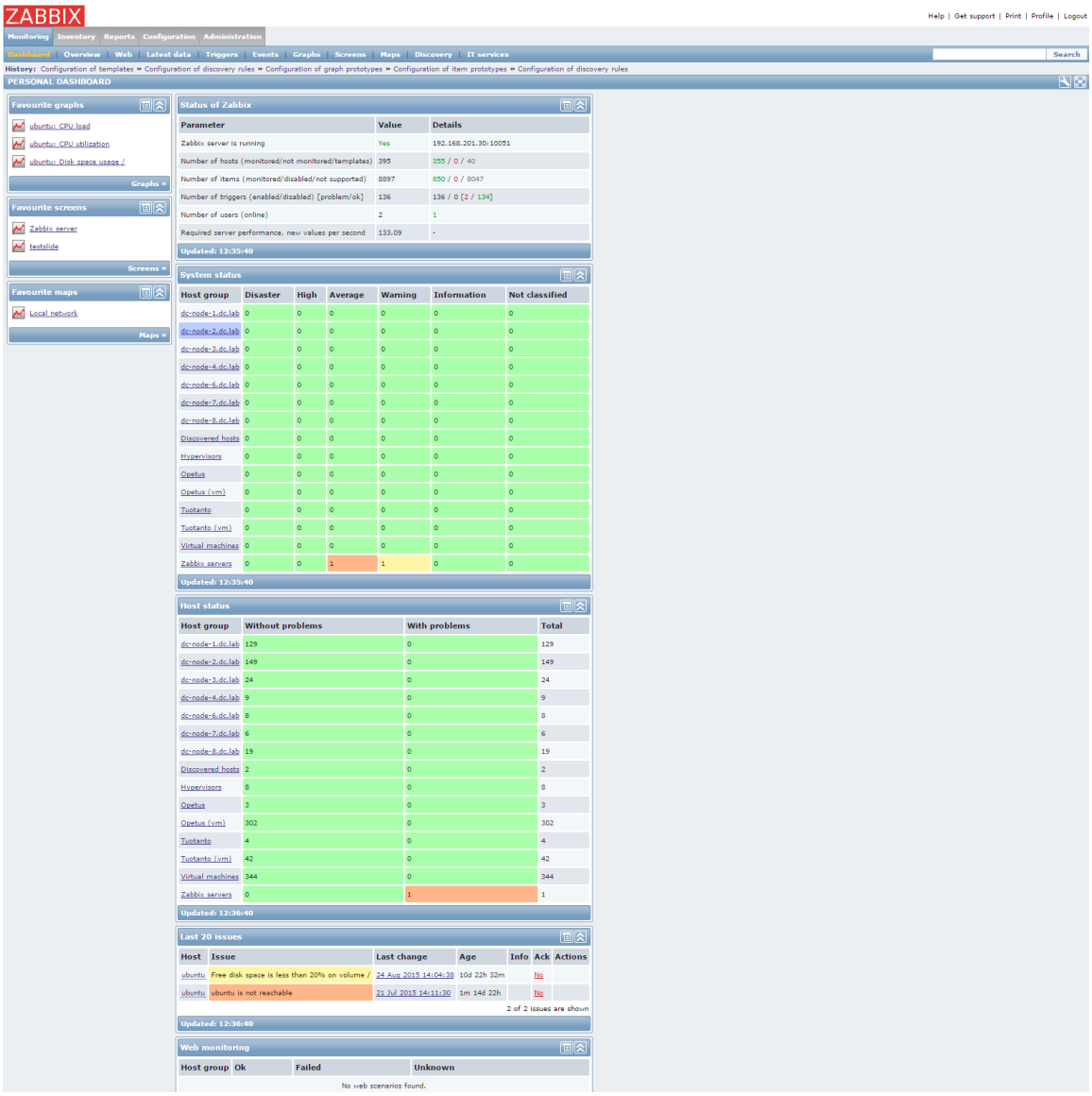
Zabbix on ilmainen, avoimen lähdekoodin ratkaisu yritysten IT infrastruktuurin valvontaan. Ohjelmisto tarjoaa mahdollisuuden lähes rajattomaan datan keräämiseen yrityksen verkkolaitteista ja –ympäristöstä. Lisäksi kerattyä dataa voidaan tallentaa ja seurata reaaliaikaisesti visuaalisessa muodossa. Kaikki Zabbix:n toimiakseen vaatimat ohjelmistot ovat myös ilmaisia avoimen lähdekoodin ratkaisuja. (What is Zabbix.)

2.1 Käyttöliittymä

Zabbix:n ainoa käyttöliittymä on PHP:llä ohjelmoitu, useita selaimia tukeva verkkokäyttöliittymä joka on nähtävillä kuvassa 1. Tästä käyttöliittymästä voidaan hallita, seurata ja konfiguroida keskitetysti kaikkia Zabbix:n toimintoja. Pääikkuna tarjoaa käyttäjälle vapaasti muokattavan näkymän, johon voidaan keskittää käyttäjälle olennaiset tiedot ja näkymät sekä asettaa suorat linkit tärkeisiin valvontakohteisiin. (Zabbix visualization.)

Verkkokäyttöliittymä tarjoaa kaikki työkalut Zabbix:n hallitsemiseen ja konfigurointiin. Muita lähestymistapoja, kuten asetusten muuttamista suoraan palvelimen tiedostoista ei tarvita. Kaikki Zabbix ympäristön kattamat kohteet ovat näkyvillä eri muodoissa (hälytykset, kohteet, kaaviot jne.) käyttöliittymän eri välilehtien alla ja uusia valvottavia kohteita voidaan lisätä samaa kautta.

Käyttöliittymän ongelma on sisäänrakennetun opastuksen puute. Kaikki toiminnot, erityisesti uusien kohteiden lisääminen, eivät ole yksinkertaisia ja uudella käyttäjällä on todennäköisesti vaikeuksia käyttöliittymän ymmärtämiseen ilman opastusta.

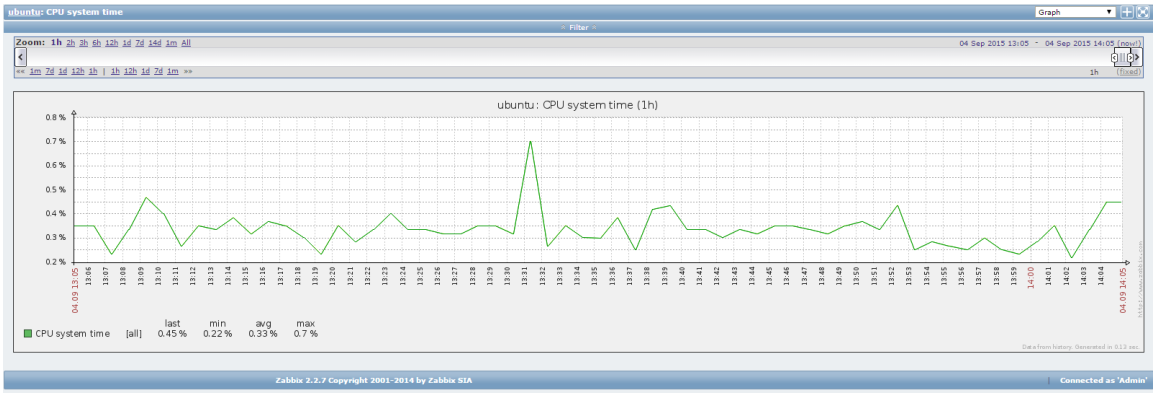


Kuva 1 Zabbix käyttöliittymä yleiskuva

2.1.1 Kaaviot

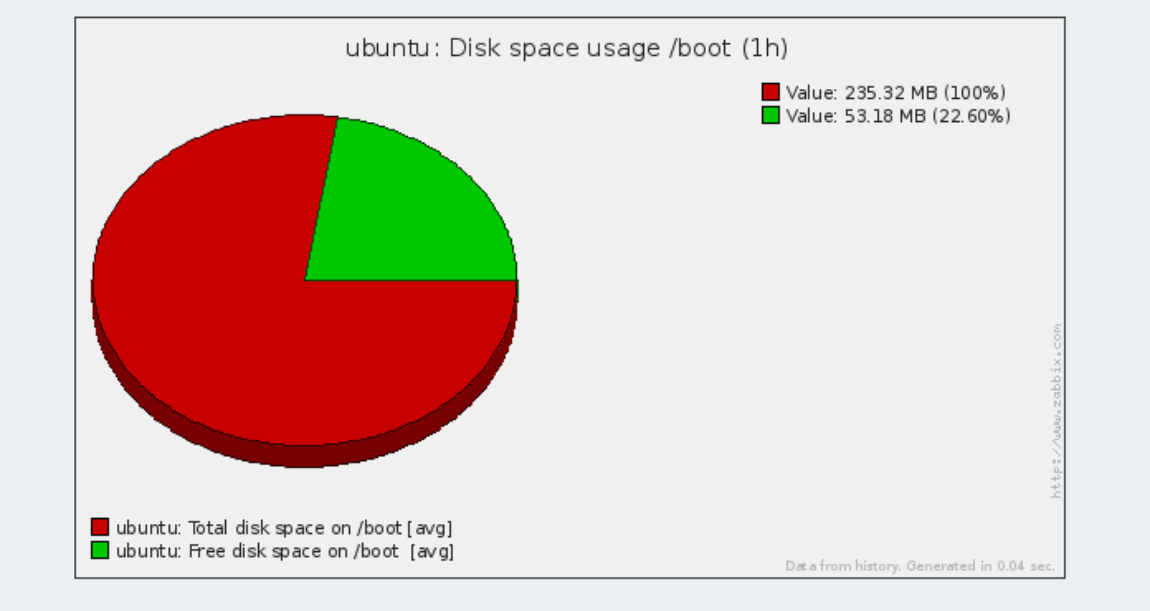
Zabbix tarjoaa mahdollisuuden kaavioiden (graphs) luomiseen valvottavista kohteista. Tämä sallii valvottavan datan muutosten seuraamisen visuaalisesti käyttöliittymän kautta. Käytön yksinkertaistamiseksi Zabbix käyttää neljää eri kaaviomallia: automatic, custom, ad-hoc ja bar report. (Graphs.)

Automatic, joista Zabbix käyttää myös nimeä simple, kaaviot ovat Zabbixin automaattisesti luomia kaavioita, jotka muodostetaan kaikille valvontakohteille, jotka seuraavat numeerisia arvoja. Esimerkki tällaisesta kaaviosta näkyy kuvassa 2. Nämä kaaviot ovat aina saatavalli käyttöliittymän Latest data välilehdeltä. Automatic kaaviot säilyttävät kerätyn datan Zabbix konfiguraation mukaisen ajan ja kaavio sisältää mahdollisuuden säätää näytettävän datan aikaväliä tunnista kaavion elinaikaan. Pidemmällä aikavälillä Zabbix näyttää myäs kaavion korkeimman, pienimmän ja keskiarvon. (Simple graphs.)



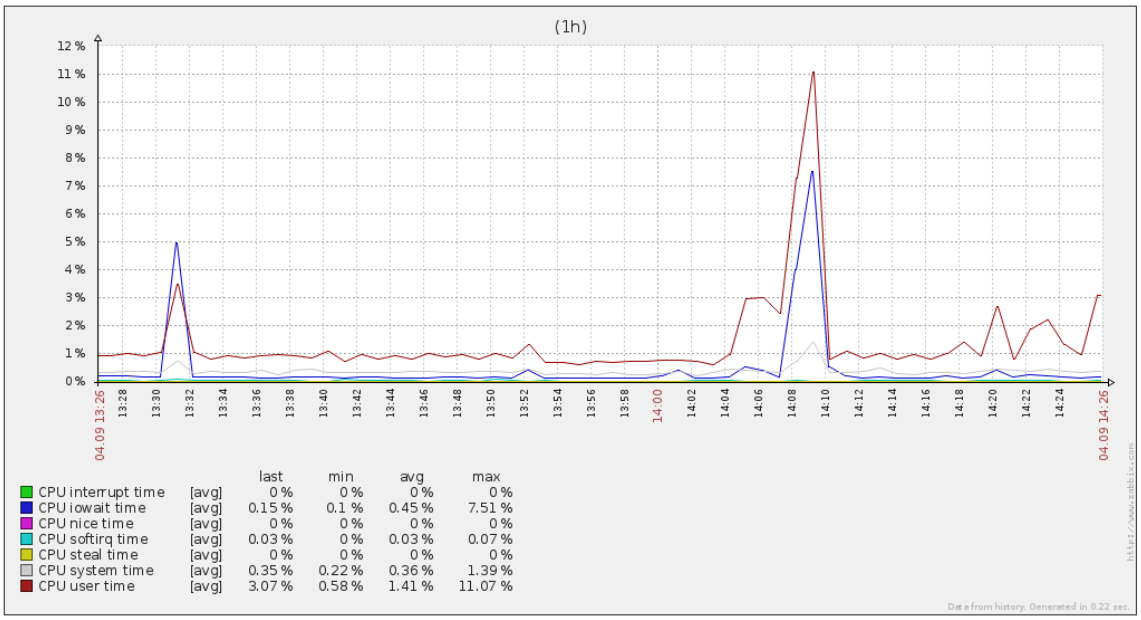
Kuva 2 Zabbixin automaattisesti luoma simple graph

Custom kaaviot ovat Zabbixissa käyttäjän luomia ja konfiguroimia kaavioita, joissa on mahdollista muokata kaavion tyyliä, luotavien viivojen näyttöä tai seurata useita kohteita yhtäaikaisesti Esimerkki tästä on kuvassa 3 esiintyvä pitsamallin kaavio. Custom kaaviot voidaan luoda suoraan valvottavalle laitteelle, yhdistämään useita valvottavia laitteita, tai mille tahansa yhden templaten sisältämille kohteille. Custom kaavioiden luontia ei voi automatisoida, vaan ne on konfiguroitava manuaalisesti.(Custom graphs.)



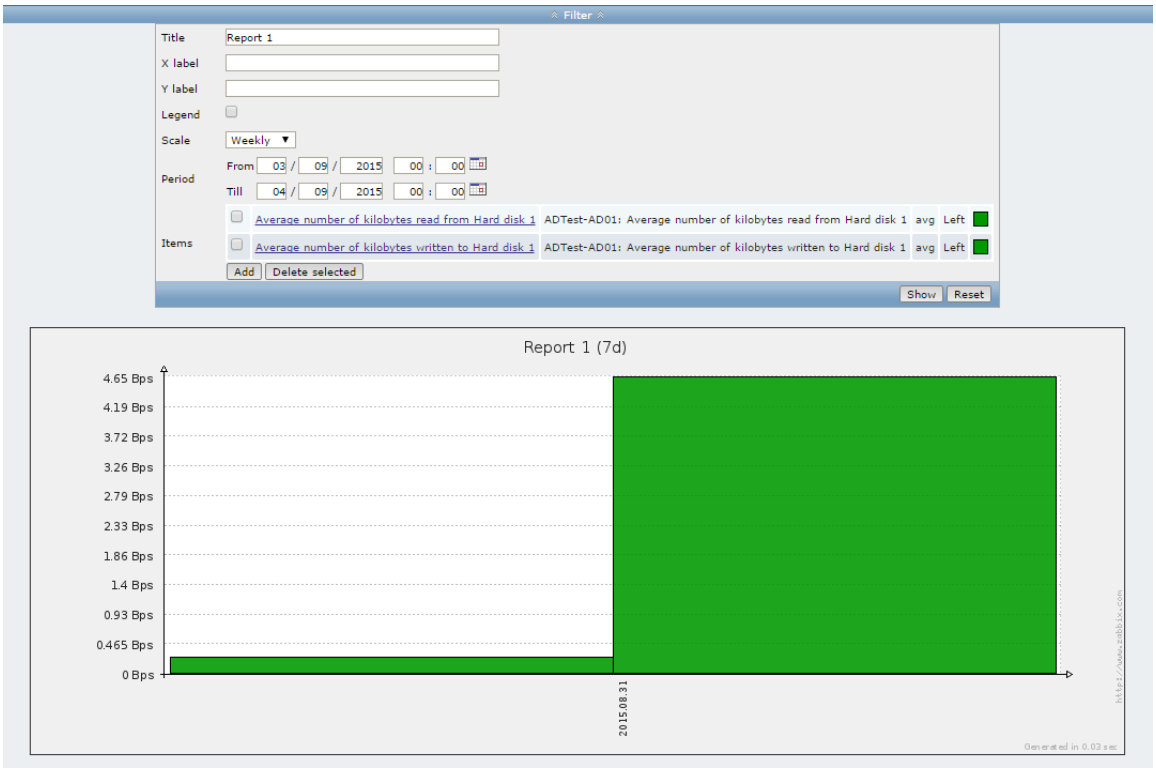
Kuva 3 Custom graph toiminnolla luotu pitsamalli

Ad-hoc kaavio on väliaikainen, useamman olemassa olevan kaavion vertailuun tarkoitettu ratkaisu joka lisättiin Zabbix 2.4 versiossa. Ad-hoc kaavio voidaan luoda valitsemalla vertailtavat kaaviot Zabbixin käyttöliittymästä ja valitsemalla Display stacked graph tai Display graph. Ad-hoc kaaviota ei voi konfiguroida, sillä ne ovat väliaikainen ratkaisu usean eri kaavion näyttämiseen yhdessä kaaviossa. Kuva 4 näyttää Ad-hoc kaavion joka on muodostettu valvottavan laitteen CPU tilastoista. Ad-hoc kaaviot eivät näytä vertailtavien kaavioiden korkeimpia ja pienimpiä arvoja, vaan ainoastaan keskiarvon. Muita alkuperäisiin kaavioihin liitettyjä tietoja, kuten triggereitä, ei näytetä. (Ad-hoc graphs.)



Kuva 4 Eri CPU tilastoista luotu ad-hoc kaavio

Bar reports kaaviot ovat Zabbixin tarjoama mahdollisuus luoda pylväsdiagrammeja lennossa olemassa olevasta datasta. Zabbix tarjoaa vaihtoehtoina kolme eri tyyppistä bar reportia. Bar reports kaavioita voidaan luoda ja katsella pikaisesti, mutta niitä ei ole mahdollista tallentaa. Kuvassa 5 on nähtävillä esimerkki. (Bar reports.)



Kuva 5 Bar report levyn luetusta ja kirjoitetusta datasta

2.1.2 Tapahtumat

Zabbixissa tapahtumat (events) ovat osa valvontajärjestelmää. Tietyissä tilanteissa Zabbix palvelin kirjaa ylös aikaleimalla varustetun tapahtuman, jotka ovat nähtävillä Zabbixin verkkokäyttöliittymän kautta. Tilanteita, joissa palvelin kirjaa tapahtuman, ovat:

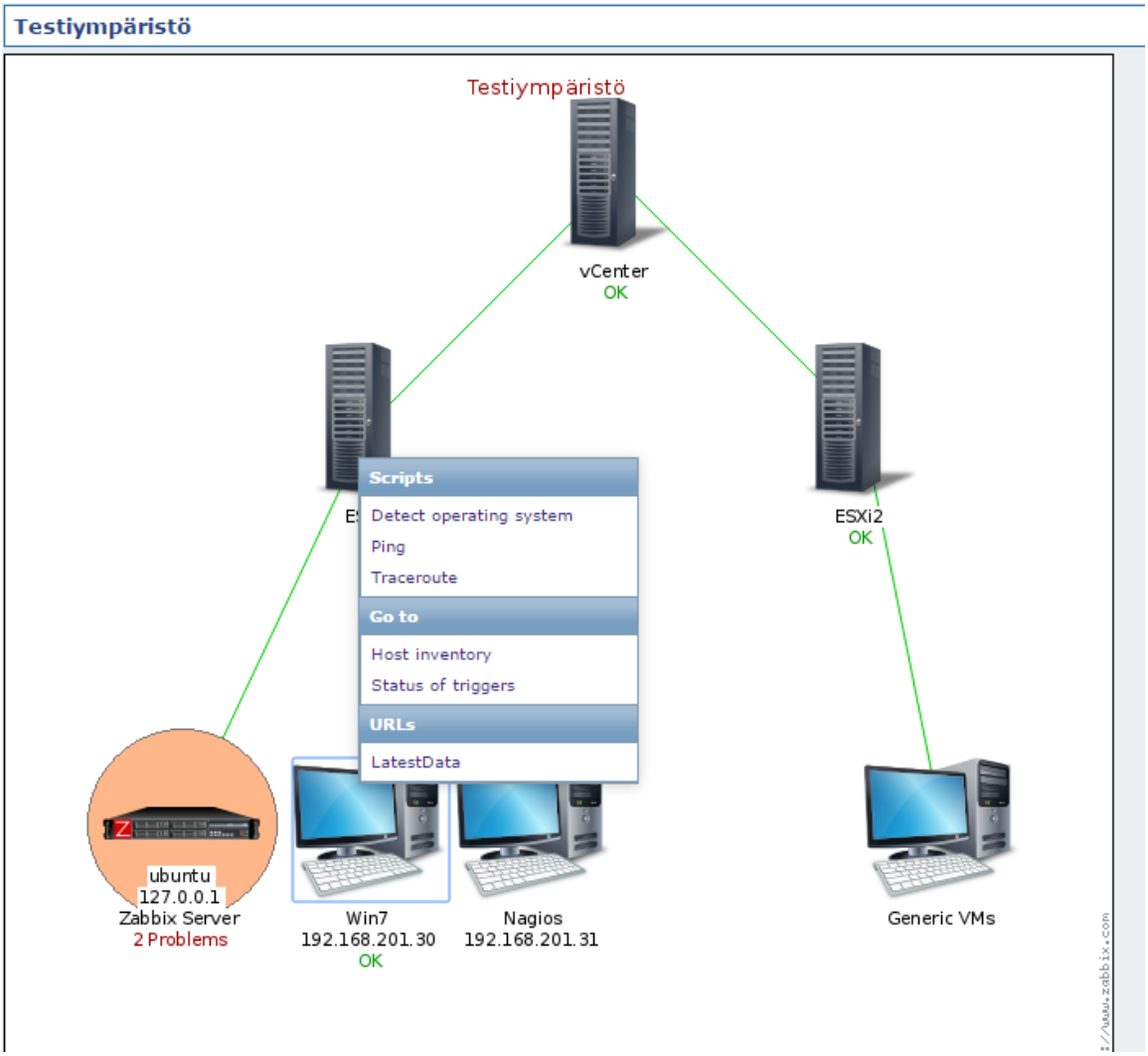
- Valvottava laite tai palvelu on aktiivinen ajastetun skannauksen aikana.
- Valvottava laite tai palvelu ei ole aktiivinen ajastetun skannauksen aikana.
- Laite tai palvelu havaitaan ensimmäisen kerran tai pitkän käyttökatkon jälkeen.
- Laite tai palvelu katoaa valvontajärjestelmästä.
- Aktiivinen agentti rekisteröi kohteen valvontaan automaattisesti.

- Itemin, low-level discovery rulentaitriggerintilaksivaihtuu normal, un-known tai unsupported.

Zabbixissa näiden tapahtumien tarkoituksena on sekä ilmoittaa ympäristössä tapahtuneesta muutoksesta joka voi vaikuttaa valvonnan toimintaan, sekä toimia laukaisimina ennalta määritetyille toiminnoille. Näitä toimintoja voivat olla mm. tapahtuman tietojen lähettäminen valvojalle sähköpostin välityksellä tai tarpeettomien valvontakohteiden automaattinen poisto. (Event sources.)

2.1.3 Kartat

Zabbix sisältää mahdollisuuden luoda verkkokarttoja (network maps) valvottavasta ympäristöstä vapaasti valittavalle taustalle, tarkoituksena tarjota käyttäjäystävällinen näkymä valvottavasta ympäristöstä. Kuvassa 6 on nähtävillä esimerkki Zabbix kartasta. Jokainen kartalla esiintyvä kohde voidaan liittää laitteeseen, laiteryhmään, triggeriin, kuvaan tai erilliseen karttaan. Kartan kohteet voivat linkittää suoraan olemassa olevaan kohteeseen, jolloin kartalta kyetään seuraamaan valitun kohteen tilaa ja toimintoja. Esimerkiksi, jos kartalla oleva kohde saa problem statuksen, kohteen ympärille ilmestyy ongelman tason värinen ympyrä. Valitsemalla kohteen kartalta Zabbix tarjoaa pääsyn tiettyihin ennalta määriteltyihin ja itse luotuihin skripteihin jotka liittyvät valittuun kohteeseen. (Maps.)



Kuva 6 Zabbix kartta testiympäristöstä

2.1.4 Turvallisuus ja autentikointi

Zabbixin autentikointi on mahdollista toteuttaa kolmella eri tavalla: Zabbixin sisäinen(internal), LDAP tai HTTP. Sisäinen autentikointi on alustavasti käytössä oleva ratkaisu, jossa järjestelmä käyttää Zabbixin sisäisiä käyttäjätunnuksia, joita voidaan hallita web-käyttöliittymän kautta. (Authentication.)

LDAP ja HTTP autentikointi toimivat samalla menetelmällä, käyttäen ulkoista käyttäjätietokantaa kirjautumisen varmistamiseen. LDAP autentikointi on tuettu Microsoft Active Directoryn ja openLDAP:n kanssa, muut LDAP ratkaisut voivat

olla mahdollisia. Vastaavasti HTTP ratkaisu tukee Apache pohjaista autentikointia. Sekä LDAP että HTTP ratkaisuissa olemassa olevaa käyttäjätietokantaa käytetään vain vertailukohteena. Jokainen haluttu käyttäjä on lisättävä Zabbixiin erikseen, jonka jälkeen kirjautumisen yhteydessä annettua käyttäjää verrataan LDAP:n kautta saatuun käyttäjälistaan. Tässä tilanteessa kyseisen käyttäjän Zabbixiin kirjattua salasanaa ei käytetä, vaan kirjautuminen vaatii LDAP:n kautta saadun salasanan. Joka tapauksessa Zabbixiin ei kyetä kirjautumaan LDAP:n kautta olemassa olevilla käyttäjätunnuksilla ellei niitä ole myös lisätty Zabbixin sisäiseen käyttäjälistaan. (Authentication.)

Testeissä havaittiin, että vaikka Zabbixin käyttäjätunnukset ovat tavanomaisesti kryptattu Zabbix serverin tiedoissa, on Zabbixissa puutteita tietyissä tilanteissa ulkoisten käyttäjätunnusten suojaamisen suhteen. Virtualisointiympäristön valvontaa varten Zabbix vaatii pääsyn valvottavaan hypervisoriin. Tässä tilanteessa Zabbix käyttää käyttäjätunnus- ja salasanamacroja, jotka käyttäjän on syötettevä web-käyttöliittymään. Tässä tilanteessä hypervisorin käyttäjätunnus sekä salasana esiintyvät plain text muodossa Zabbixin käyttöliittymässä.

2.2 Tietokanta

Zabbix vaatii toimiakseen erillisen tietokannan, joka on luotava joko Zabbix palvelimen tai proxyn asennuksen yhteydessä. Zabbix proxyt käyttävät palvelimesta ja toisistaan erillisiä tietokantoja tietojen tallentamiseen ennen niiden lähettämistä palvelimelle itselleen. Tästä syystä proxy-tietokanta on puutteellinen palvelimen tietokantaan verrattuna, eikä ole kelvollinen palvelimen tietokannaksi itsessään. Zabbix tarjoaa valmiit skriptit tuettujen tietokantojen asentamiseen. Tuettuja tietokantoja ovat MySQL, PostgreSQL, Oracle, IBM DB2 sekä SQLite. (Database creation scripts.)

3 VALVONTA

Zabbix on työkalu verkkoympäristön valvontaan ja tarjoaa useita vaihtoehtoja ja ratkaisuja valvoa kaikkia verkossa olevia laitteita. Tässä kappaleessa tutustun Zabbix:n tarjoamiin eri valvontaratkaisuihin Kuvassa 7 on nähtävillä Zabbixin näkymä kerätystä datasta.

Host	Name	Last check	Last value	Change	
Win7-2	**Classes** (3 Items)				
	cl Loaded Class Count	04 Sep 2015 15:41:05	3375	-	Graph
	cl Total Loaded Class Count	04 Sep 2015 15:41:05	3375	-	Graph
	cl Unloaded Class Count	04 Sep 2015 15:41:05	0	-	Graph
Win7-2	**Compilation** (2 Items)				
	comp Accumulated time spent in compilation	04 Sep 2015 15:41:05	28s 92ms	+40ms	Graph
	comp Name of the current JIT compiler	04 Sep 2015 15:00:06	HotSpot 64-Bit Tiered Compilers	-	History
ubuntu	**CPU** (13 Items)				
	Context switches per second	04 Sep 2015 15:41:18	198 sps	-26 sps	Graph
	CPU idle time	04 Sep 2015 15:41:19	98.85 %	+0.78 %	Graph
	CPU interrupt time	04 Sep 2015 15:41:20	0 %	-	Graph
	CPU iowait time	04 Sep 2015 15:41:21	0.13 %	-0.11 %	Graph
	CPU nice time	04 Sep 2015 15:41:22	0 %	-	Graph
	CPU softirq time	04 Sep 2015 15:41:23	0.03 %	-	Graph
	CPU steal time	04 Sep 2015 15:41:24	0 %	-	Graph
	CPU system time	04 Sep 2015 15:40:25	0.3 %	-0.03 %	Graph
	CPU user time	04 Sep 2015 15:40:26	1.32 %	+0.66 %	Graph
	Interrupts per second	04 Sep 2015 15:41:14	77 ips	-8 ips	Graph
	Processor load (1 min average per core)	04 Sep 2015 15:41:16	0	-	Graph
	Processor load (5 min average per core)	04 Sep 2015 15:41:17	0.01	-0.01	Graph
	Processor load (15 min average per core)	04 Sep 2015 15:41:15	0.05	-	Graph
Win7-2	**CPU** (3 Items)				
ubuntu	**Filesystems** (10 Items)				
	Free disk space on /	04 Sep 2015 15:40:36	44 MB	-8 KB	Graph
	Free disk space on / (percentage)	04 Sep 2015 15:40:38	0.32 %	-	Graph
	Free disk space on /boot	04 Sep 2015 15:40:37	53.18 MB	-	Graph
	Free disk space on /boot (percentage)	04 Sep 2015 15:40:39	23.83 %	-	Graph

Kuva 7 Käyttöliittymän latest data välilehti, valvottavat kohteet

3.1 Zabbix agentti

Zabbix agentti on Linux, UNIX, Windows ja OS X käyttöjärjestelmien valvontaan tarkoitettu, laitteelle asennettava ohjelma, jota ajetaan käyttöjärjestelmän prosessina, joka kerää kohteesta sille määriteltyjä tietoja ja lähettää ne eteenpäin Zabbix palvelimelle. Palvelin käyttää JSON pohjaista protokollaa agenttien kanssa kommunikointiin. Agenttia voidaan käyttää valvomaan:

- Verkkoliikennettä.
- CPU käyttöä.
- Muistin käyttöä.

- Levykapasiteettia.
- Prosessien ja palveluiden tilaa (kuten Windows servicet) ja resurssikäyttöä.
- DNS ja TCP yhteyttä.
- Tiedostokokoa ja olemassaoloa + RegExp hakuja.
- Tekstilokeja ja Windows event lokia.
- Järjestelmän käytettävyysaikaa.
- Käyttäjätunnuksien kirjautumisaikaa ja toimintoja.

Zabbix agentti toimii käyttöjärjestelmässä itsenäisesti, eikä vaadi erillisiä ohjelmistoja toimiakseen. (Monitor everything. Agent.)

Zabbix agentteja on kahdenlaisia, passiivisia ja aktiivisia. Passiivinen agentti on rekisteröitävä aina manuaalisesti valvontaan käyttöliittymän kautta. Passiivinen agentti toimii odottamalla palvelimelta saapuvaa pyyntöä ennen datan lähettämistä takaisin palvelimelle. Palvelin lähettää datapyynnön valvottaville kohteille ennalta määritellyin väliajoin. Passiivisia agentteja kannattaa käyttää tilanteissa, joissa valvottava data muuttuu jatkuvasti, kuten CPU:n käyttö. Tässä tilanteessa uusi data saadaan määrätyin väliajoin sen sijaan, että agentti lähettäisi tiedon joka kerta tilanteen muuttuessa, säästäen näin verkkoliikennettä.

Aktiivinen Zabbix agentti toimii päinvastoin passiivisesta. Tämän lisäksi palvelin voidaan asettaa automaattisesti rekisteröimään kaikki aktiiviset agentit valvottavaksi, sen sijaan että ne täytyisi manuaalisesti lisätä käyttöliittymän kautta. Aktiivinen agentti lähettää dataa palvelimelle aina tarkkailtavan kohteen muuttuessa. Aktiivista agenttia kannattaa käyttää kohteissa, joiden tilanne muuttuu vain harvoin, kuten tallennuskapasiteetissa. Tämä vähentää verkkoliikennettä poistaen turhia kyselyitä, joita passiivinen agentti lähettäisi palvelimelle datan tilasta riippumatta.

3.2 SNMP

SNMP on IAB:n määrittelemä, sovellustason protokolla verkkolaitteiden väliseen hallintatietojen vaihtamiseen. Se on osa TCP/IP protokollajoukkoa ja yksi laajalti hyväksytyistä protokollista verkkoelementtien hallintaan ja valvontaan. Suurimmassa osassa yritystason verkkolaitteista on sisäänrakennettu SNMP agentti, joka on konfiguroitu kommunikoimaan verkkovalvontajärjestelmien kanssa. (SNMP tutorial.)

Zabbix tukee SNMP agenttien valvomista, jotka ovat pääasiallinen ratkaisu verkkolaitteiden, kuten kytkinten ja reitittimien sekä muiden laitteiden kuten tulostimien, valvontaan. SNMP valvonta toteutetaan UDP protokollalla ja perustuu OID (Object Identifier) ja MIB:hin (Manangement Information Base). OID on kohteen yksilötunnus jonka avulla kaikki SNMP valvonta kohdistetaan. MIB tietokannan avulla OID:t voidaan muuttaa ymmärrettävään muotoon. Esimerkiksi OID 1.3.6.1.2.1.1.3 muuttuu MIB tietokannan kautta muotoon sysUpTime. (Dalle Vache & Lee 2012, 145-146; Monitor everything.)

Tilanteissa joissa SNMP valvonta on mahdollista, sen käyttö on usein suositeltavaa Zabbix agentin sijasta. Jos tarkoituksena on valvoa yksinkertaisempia tilastoja kuten CPU kuormaa, muistin käyttöä ja vastaavia resursseja, ei valvonnan käyttöönotosta ja agenttien asentamisesta tarvitse huolehtia, vaan Zabbix palvelin voi ottaa suoraan yhteyden laitteiden SNMP agentteihin. Lähes kaikki tuotteet myös tunnistavat SNMP protokollan ja UDP portit 161 ja 162. Tämä helpottaa valvontaliikenteen kulkua ilman erityisiä oikeuksia, toisin kuin Zabbix agentti. Kaikki kolme SNMP versiota ovat tuettuja Zabbixissa, mutta on suositeltavaa käyttää SNMPv3:sta sen sisäänrakennetun autentikoinnin ja turva-asetusten vuoksi. Versiot 1 ja 2 eivät tarjoa SNMP viestien autentikointia ja vain minimaaliset turva-asetukset. . (Dalle Vache & Lee 2012, 147.)

Zabbix:ssa SNMP valvonnan käyttöönotto on periaatteessa yksinkertaista, mutta vaatii jonkin verran totuttelua.Kohteet otetaan valvontaan viittaamalla suoraan

laitteen OID:hen tai niiden MIB käännöksiin, jos vaaditut MIB tietokannat ovat asennettuna. Käyttäjän on siis tunnettava halutut arvot kyetäkseen lisäämään ne valvontaan. Palvelin voidaan myös konfiguroida ottamaan tietyt SNMP kohteet valvontaan automaattisesti palvelimen muodostettua yhteyden laitteeseen, mutta tämä vaatii ymmärrystä OID:den arvoista sekä niiden rajaamisesta vain haluttuihin kohteisiin. Rajaaminen on suositeltavaa, sillä verkkolaitteessa saattaa olla satoja arvoja tietylle OID:lle, joista vain rajattua määrää halutaan valvoa. SNMP valvonta Zabbix:ssa on tehokas mutta totuttelua vaativa menetelmä verkkolaitteiden valvontaan. SNMP valvonta on kuitenkin rajoittunut vain kohteisiin, jotka sallivat SNMP-valvonnan, joten se ei kykene korvaamaan muita valvontamenetelmiä.

3.3 Virtuaaliympäristön valvonta

Versiosta 2.2.0 alkaen Zabbix on tukenut VMware ympäristöjen valvontaa. Tuettuna ovat VMware vCenter ja vSphere versiosta 4.1 ylöspäin. VMware ympäristöjen valvonta sisältää hypervisoreiden ja virtuaalikoneiden automaattisen havaitsemisen sekä vSphere ja vCenter asennuksessa hypervisoreiden ja virtuaalikoneiden tilastojen ja ominaisuuksien tarkkailun. Hypervisoreiden ja virtuaalikoneiden automaattiseen löytämiseen Zabbix käyttää low-level discoveryä. Valvottavien tietojen kerääminen tapahtuu Zabbix:n VMware collector prosessien avulla, jotka käyttävät SOAP protokollaa tiedonkeruuseen VMware web palveluilta ja tallettavat sen palvelimelle. Täältä palvelin hakee halutut tiedot konfiguroitujen kyselyiden perusteella. Versiosta 2.4.4 alkaen Zabbix jakaa VMwaren kohteilta kerätyt tiedot kahteen kategoriaan, konfiguraatiodataan ja performanssidataan, jotka kerätään palvelimelle toisistaan riippumatta. (Virtual machine monitoring.)

Perusasennuksessa Zabbix ei tue VMware valvontaa, vaan VMware collector on otettava käyttöön konfiguraatiotiedoston kautta asennuksen jälkeen. Valvottava vCenter palvelin tai hypervisor voidaan lisätävalvottavaksi manuaalisesti tai low-

level discoveryä käyttäen automaattisesti. VMware valvonta Zabbixissa vaatii käyttäjätunnuksen jolla on pääsy valvottavaan kohteeseen toimiakseen. Koska kyseinen käyttäjä ja salasana on lisättävä valvottavaan laitteeseen Zabbixin webkäyttöliittymästä selkokielisessä muodossa, joka on nähtävissä kaikille Zabbixia administrator-oikeuksilla käyttäville, on suositeltavaa käyttää tähän tarkoitukseen erikseen luotua käyttäjää joka kykenee ainoastaan tarkkailuun.

Kun Zabbix:lla on pääsy valvottavaan VMware laitteeseen, se kykenee luomaan erilliset valvottavat kohteet kaikille vCenterin tai ESX hypervisorin alla toimiville kohteille käytössä olevien templatejen mukaisesti. Zabbix tarjoaa valmiit templatet yleisen tason valvontaan, joita voidaan käyttää mm. olemassa olevien virtuaalikoneiden automaattiseen tarkkailuun. Nämä templatet suositellaan otettavaksi käyttöön manuaalisesti jokaiselle valvottavalle kohteelle. (Virtual machine monitoring.)

3.4 JMX valvonta

Versiosta 2.0 eteenpäin Zabbix tukee sisänrakennettuna sovellusten valvontaa Java Management Extensionien (JMX) avulla. JMX on JCP:n kautta kehitetty API joka on tarkoitettu sovellusten, laitteiden, palveluiden ja Java virtuaalikoneiden valvontaan ja hallintaan. Tyypillisiä käyttökohteita JMX:lle ovat sovellusasetusten seuranta ja muuttaminen, tilastojen kerääminen sovellusten toiminnasta sekä vikatilanteiden ja muutosten raportointi. (Java Management Extensions.)

Zabbix:ssa JMX valvonta toteutetaan Zabbix Java gateway taustaprosessin avulla. Kun palvelin haluaa tietoja valvottavasta JMX:stä, se lähettää kyselyn Zabbix Java Gatewaylle. Tämän seurauksena gateway lähettää kyselyn kyseiselle JMX:lle, käyttäen Oraclen JMX Management API:a. JMX valvonnan käyttöönotto on yksinkertaista ja toteutetaan syöttämällä tietyt parametrit Java sovellukselle, mutta tää ratkaisu on mahdollinen tietoturvariski yritykselle. Sovelluspalvelimille listättynä JMX konsoli mahdollistaa sovellusten tarkkailun

lisäksi myös sovellusten sijoittamisen, käynnistämisen ja sammuttamisen. Jos väärät tahot saavat yhteyden JMX konsoliin, voivat ne lisätä omia sovelluksiaan tai aiheuttaa ongelmia olemassa olevien sovellusten toiminnassa mm. verkkosivujen skriptauksen kautta. Sovelluspalvelimen saastuminen voi vaarantaa koko infrastruktuurin, joten JMX:n käyttöönoton lisäksi on toteutettava lisätoimenpiteitä ympäristön turvaamiseksi.(Dalle Vache & Lee 2012, 137-138.)

JMX valvonnan käyttöönottossa on havaittavissa tiettyjä puutteita. Koska Zabbix Java gateway toimii vain linkkinä Zabbixin ja JMX:n välillä, on kummatkin konfiguroitava erikseen toimimaan yhdessä. Zabbix käyttää aina vain sille konfiguroituja portteja lähettääkseen kyselyitä ja vastaanottaakseen vastauksia, mutta JMX toimii valitsemalla sattumanvaraisen vapaan portin senhetkiseen tarpeeseen. Tässä tilanteessa kummatkin on saatava käyttämään aina samaa porttia tai Zabbix ja JMX eivät kykene keskustelemaan keskenään. Kun kumpikin saadaan keskustelemaan keskenään luotettavasti, ei Java sovellusten valvomisessa ole vaikeuksia.

3.5 Tietokantojen valvonta

Zabbixissa tietokantojen valvonta toteutetaan ODBC valvonnalla. ODBC on C ohjelmointikielellä toteutettu API jonka tarkoituksena on päästä käsiksi DBMS:än. Zabbix voi lähettää kyselyjä mille tahansa ODBC:tä tukevalle tietokannalle. Tämä sallii useiden erilaisten tietokantojen valvonnan yhtenevällä menetelmällä ja tehostaa eri tietokantojen valvontaa useisiin tarkoituksiin. Zabbix tukee unixODBC:tä. (ODBC monitoring.)

Tietokannan valvontaa varten Zabbix palvelimelle on asennettava unixODBC ja valvottavalle tietokannalle on asennettava unixODBC tietokanta-ajauri. Zabbixissa ODBC on reitti jota tietokantavalvonta käyttää, mutta datan keräämiseen tietokannoista Zabbix käyttää SQL kyselyjä. Täten valvottavista tietokannoista on mahdollista saada kaikki tieto, jotka voidaan hakea tietokannasta SQL kyselyillä manuaalisesti. (Zabbix database monitor.)

3.6 IPMI

Zabbixissa on mahdollista valvoa IPMI tuettujen laitteiden tilaa ja saatavuutta. Tätä varten Zabbix palvelin on erikseen konfiguroitava kyseista toimintoa varten. IPMI on standardisoitu liittymä tietokonejärjestelmienetänä toteutettuun ”lights-out” ja ”out-of-band” hallintaan. IPMI sallii laitteiston suoravalvontaa ”out-of-band” hallintakorteilla, itsenäisesti käyttöjärjestelmistä riippumatta tai laitteen ollessa pois päältä. (IPMI checks.)

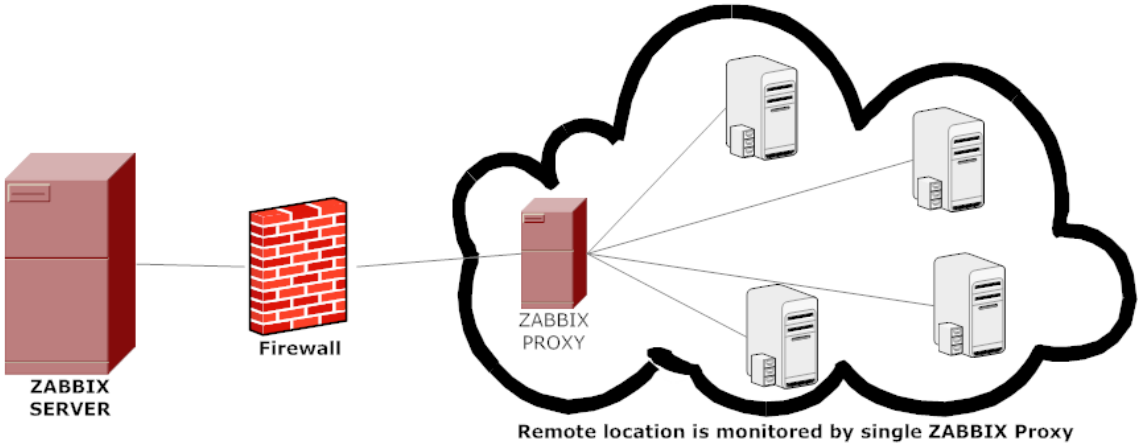
Zabbix IPMI valvonta käyttää IPMI laitteen IP:tä valvottavan kohteen löytämiseksi. IPMI valvonnan käyttöönotossa kohteen IP, portti, käyttäjätunnus ja salasana on konfiguroitava manuaalisesti, sillä tällä hetkellä Zabbix network discovery ei tue IPMI kyselyjä. Valvonta perustuu laitteissa oleviin IPM sensor arvoihin, jotka ovat valmistaja- tai laitekohtaisia kohteesta riippuen. IPMI valvontaan lisätyille laitteille on mahdollista lähettää etäkomentoja, kuten käynnistys tai sammutus, Zabbixin käyttöliittymän kautta. (Monitoring of IPMI devices. IPMI checks.)

3.7 Proxy

Zabbix proxy on prosessi jonka tarkoituksena on kerätä valvontadataa yhdeltä tai useammalta valvottavalta kohteelta ja lähettää saadut tiedot Zabbix palvelimelle.Kerätty data käsitellään proxyssä ja valmis informaatio lähetetään edelleen palvelimelle. Proxy on Zabbixin ratkaisu keskitetyn ja hajautetun valvonnan toteuttamiseen.Kuvassa 8 on kuvattu Zabbix proxyn toiminta. Zabbix proxyä voidaan käyttää:

- Etäkohteiden, kuten sivutoimistojen, valvontaan.
- Sijaintien, joilla on epäluotettava yhteys palvelimeen, valvontaan.
- Palvelimen kuormituksen vähentämiseen laajan skaalan valvonnassa.

- Hajautetun valvonnan hallinnan yksinkertaistamiseen.



Kuva 8 Zabbix proxyn toiminta (Proxies.)

Zabbix proxyn käyttöönotto on samanlainen kuin palvelimen. Proxy asennetaan taustaprosessinalaitteelle valvottavassa ympäristössä ja vaatii erillisen tietokannan Zabbix palvelimesta. Yhteyden muodostamiseksi palvelimeen proxy vaatii yhden TCP yhteyden. Valvontaa toteuttaessa proxy toimii kuten Zabbix palvelin, kaikki kerätty data tallennetaan paikallisesti proxyn tietokantaan konfíguraatiossa määritellyksi ajaksi ja käsitellään ennen lopullisen informaation lähettämistä palvelimelle. Tämä estää informaation katoamisen tilanteessa, jossa proxyn ja palvelimen yhteydessä on ongelmia. Zabbix proxy on puhtaasti datan kerääjä. Se ei käsittele triggereitä, tapahtumia tai lähetä hälytyksiä. (Proxy. Proxies.)

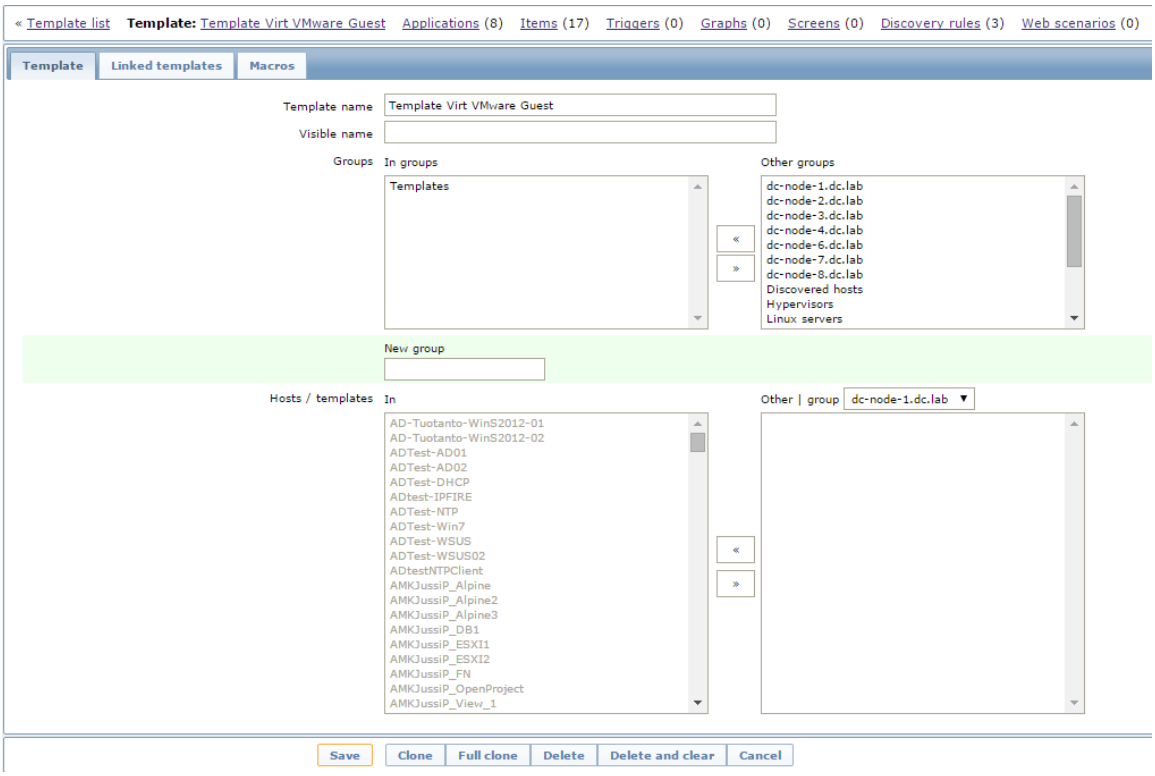
3.8 Template

Template on Zabbixin käyttämä pohja laajan tason valvontaan. Zabbix template on joukko yksiköitä jotka voidaan ottaa käyttöön useassa eri laitteessa. Kuvassa 9 on nähtävissä Zabbix templaten hallintanäkymä.Yksi templateen kuuluva yksikkö voi olla:

- item: Yksittäinen, tiettyä asiaa tietyssä kohteessa valvova toiminto (Items).

- trigger: Zabbixin hälytys, joka lähettää ilmoituksen määriteltyihin kohteisiin tietyn tilanteen tapahtuessa (Triggers).
- graph: Zabbixin luoma kaavio, joka voi näyttää graafisesti joko yhden tai useamman kohteen tilan tietyin kriteerein (Custom graphs).
- application: Joukko loogisiin ryhmiin kerättyjä itemejä tai web scenarioita (Applications).
- screen: Usean kohteen näkymä kerättynä yhteen seurannan nopeuttamiseksi (Screens).
- low-level discovery: Menetelmä itemien, triggereiden ja graphien automaattiseen luontiin erillisille kohteille (Low-level discovery).
- web scenario: Yksi tai useampi määritetty HTTP pyyntö joita palvelin käyttää verkkosivujen valvontaan (Web monitoring).

Zabbix valvonnassa templatejen käyttö on lähes välttämätöntä laajemman ympäristön tehokkaaseen monitorointiin. Koska samat ja samankaltaiset, kuten saman valmistajan, laitteet ja ohjelmistot vastaavat samoihin kyselyihin, on mahdollista luoda yksi template joka kykenee valvomaan kaikkia tietyntyyppisiä laitteita, sen sijaan että jokaiselle laitteelle muodostettaisiin oma joukko valvontatoimintoja. Templatet toimivat myös valvonta-asetusten tallennusmuotona, esimerkiksi tilanteessa jossa valvottava laite poistuu ympäristöstä. Tällöin valmis template voidaan ottaa uudelleen käyttöön tarpeen vaatiessa, sen sijaan että asetukset katoaisivat valvottavan laitteen mukana.



Kuva 9 Zabbix templaten hallinta

3.9 Discovery ja prototype

Zabbix tarjoaa ratkaisuja laajojen ympäristöjen valvonnan käyttäänottoon valvottavien kohteiden automaattisen löytämisen ja lisäämisen avulla. Aktiivisen agentin kohteen valvonnan automaattisen käyttöönoton lisäksi Zabbix tarjoaa kaksi toimintoa, network discovery ja low-level discovery. Kumpikin toiminto on tarkoitettu eri kohteiden valvontaan joiden tarkoituksena on lisätä ja hallita valvottavia kohteita niiden tullessa tai poistuessa ympäristöstä. (Auto Discovery.)

Network discovery on Zabbixin ratkaisu valvottavien laitteiden ja palveluiden löytämiseen. Network discovery pohjautuu neljään kriteeriin: IP-avaruuteen, ulkoisten palveluiden kuten FTP:n tai SSH:n saatavuuteen sekä Zabbix että SNMP agenteilta saatavaan tietoon. Network discoveryn toimintaa varten Zabbixille on luotava network discovery rule, jolle määritetään etsittävien

kohteiden rajat edellämainittujen neljän kriteerin avulla. Discovery rulea määritellessä ei ole tarpeellista käyttää kaikkia neljää kriteeriä vaan käytettävien kriteerien määrää voidaan rajoittaa halutun tarkkuuden mukaan. Esimerkiksi jos tietyltä IP-avaruudelta haetaan vain laitteita joilla on Zabbix agent, voidaan käyttää vain IP-avaruutta ja Zabbix agenteilta saatavaa tietoa. Lisäksi on mahdollista määrittää löydetyille kohteille toteutettavat toiminnot. Network discoveryn avulla toteutettavat mahdolliset toiminnot ovat seuraavat:

- Huomautuksen luominen käyttäjälle.
- Kohteen poistaminen tai lisääminen ryhmästä tai valvonnasta.
- Valvonnan kytkeminen päälle tai pois päältä.
- Templaten liittäminen tai poistaminen kohteesta.
- Skriptien suorittaminen.

Halutut toiminnot voidaan määrittää toteutuviksi asetettujen kriteerien pohjalta, kuten laitteen poistaminen valvonnasta jos siihen ei saada yhteyttä yli 24 tuntiin. (Discovery.)

Zabbixissa low-level discoveryä käytetään tiettyjen valvontakokonaisuuksien (item, trigger, graph) automaattiseen havaitsemiseen valvottaville kohteille. Zabbix voi näin asettaa laitteen tiedostojärjestelmän tai verkkoportit valvontaan automaattisesti, ilman että jokaiselle olisi luotava oma kokonaisuus manuaalisesti. Lisäksi on mahdollista asettaa Zabbix poistamaan automaattisesti käyttämättömät valvontakokonaisuudet. Zabbix tukee low-level discoveryllä neljää eri kohdetyyppiä:

- Tiedostojärjestelmät
- Verkkoliitännät.
- CPU:t ja CPU ytimet.

- SNMP OID:t.

Tätä toimintoa varten on Zabbixiin luotava low-level discovery rule, joka luodaan joko suoraan valvottavaan laitteeseen tai useimmin valvonnassa käytettävään templateen. Low-level discovery rule koostuu kahdesta kokonaisuudesta. Ensimmäistä käytetään haluttujen kohteiden etsimiseen valvottavalta laitteelta ja toinen muodostuu lisättävien kokonaisuuksien prototypeistä.(Low-level discovery.)

Prototype on zabbixissa osa low-level discoveryn automaattista valvontaa. Prototype on discovery rulen osa, joka luo itsestään kopion jokaiselle löydetylle kohteelle.Tämä kopio toimii valvontakokonaisuutena kyseiselle kohteelle. Prototypet on luotava erkiseen jokaiselle halutulle kokonaisuudelle joita discovery rule käyttää (item, graph, trigger). Prototypen tarkoituksena on poistaa tarve luoda erillinen ominaisuus jokaiselle löydetylle kohteelle, joita voi olla satoja yhdessä laitteessa.

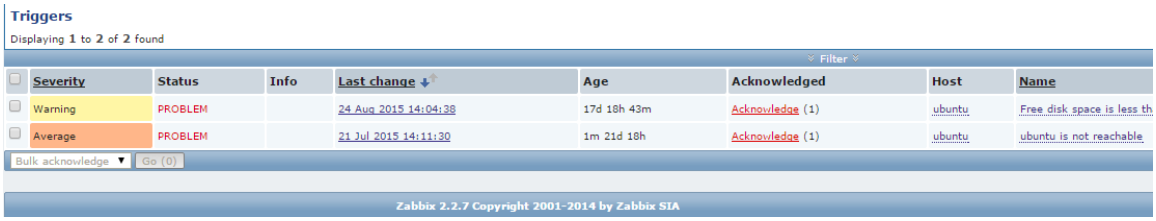
Discovery on olennainen osa Zabbix valvontaa, sillä discovery on ainoa Zabbixissa oleva ratkaisu valvottavien kohteiden automaattiseen havaitsemiseen. Kaikki Zabbixissa valmiina olevat templatet käyttävät discovery ruleja valvonnan automatisointiin ja toteuttamiseen. On suositeltavaa tutustua discovery rulejen luomiseen valmiisiin templateihin luottamisen lisäksi, erityisesti discoveryn rajaaminen vain halutuihin kohteisiin voi olla haastavaa mm. SNMP valvonnassa, jossa laitteessa voi olla tuhansia OID:tä joista vain rajattua osaa halutaan valvoa.

3.10 Trigger

Zabbixissa triggerit ovat loogisia määritelmiä joiden tarkoitus on arvioida palvelimelle kerättyä dataa ja tätä kautta kuvata järjestelmän tilaa. Käytännössä triggereiden tarkoituksena on helpottaa kerätyn datan valvontaa, sillä valvottavassa ympäristössä on helposti satoja tai tuhansia valvottavia kohteita.

Tässä tilanteessa kaiken olemassa olevan datan jatkuva seuraaminen ongelmien löytämiseksi on epäkäytännöllistä ja vaivalloista. Triggerin tarkoituksena on poistaa tarve jatkuvaan seuraamiseen. Sen sijaan ylläpitäjä voi asettaa triggereitä valvomaan Zabbixin keräämää dataa ja asettaa näille rajat jolloin kerätyt arvot ovat hyväksyttävässä tilassa. Jos valvottavat arvot ylittävät määritellyn rajan, trigger havaitsee tämän ja statukseksi vaihtuu PROBLEM. (Triggers.)

Missä tahansa Zabbix ympäristössä trigger valvonta tulee olemaan tärkeässä asemassa, sillä Zabbixissa triggerit ovat ainoa käytettävä vaihtoehto automaattisiin hälytyksiin. Ilman triggerien käyttöä ainoa vaihtoehto ongelmallisien tilanteiden tunnistamiseen valvottavassa ympäristössä on datan manuaalinen seuranta verkkokäyttöliittymän kautta tilanteessa, jossa kaikki seurattavat voivat uusiutua automaattisesti useita kertoja minuutissa. Triggerit taas toimivat automaattisesti ja huomautus tapahtuneesta ongelmasta on nähtävänä lokissa, vaikka tilanne korjautuisi itsestään. Tästä on nähtävillä esimerkki kuvassa 10. Zabbix voidaan myös asettaa lähettämään hälytys sähköpostilla tai hakulaitteella ylläpitäjälle tärkeissä tilanteissa.



Kuva 10triggerit PROBLEM tilassa

4 VERTAILU

Tässä osiossa Zabbixia verrataan toiseen yrityskäyttöön keskittyneeseen verkkovalvontaohjelmistoon. Vertailukohteeksi valittiin kaupallinen Nagios XI. Valinta tehtiin pohjautuen olemassa oleviin luokituksiin eri verkkovalvontaohjelmistoista, joissa Nagios XI oli usein sijoitettu korkealle. Lisäksi Nagios XI:n testiversion saaminen oli yksinkertaista. Vertailun tavoitteena ei ole selvittää, kumpi käytettävistä ohjelmistoista on tehokkaampi tai parempi. Tarkoituksena on selvittää, kykeneekö ilmainen Zabbix kilpailemaan kaupallisen tuotteen kanssa.

4.1 Testiympäristö

Opinnäytetyön toteutuksessa käytettiin sekä Zabbixin että Nagioksen testaamiseen Kajaanin AMK:n tietojärjestelmälaboratoriota. Käytössä oleva testiympäristä koostui seuraavista:

- Zabbix palvelin, Ubuntu virtuaalikone
- Nagios palvelin, CentOS virtuaalikone
- vCenter server
- 2 ESXi hostia
- 351 Linux ja Windows pohjaista virtuaalikonetta

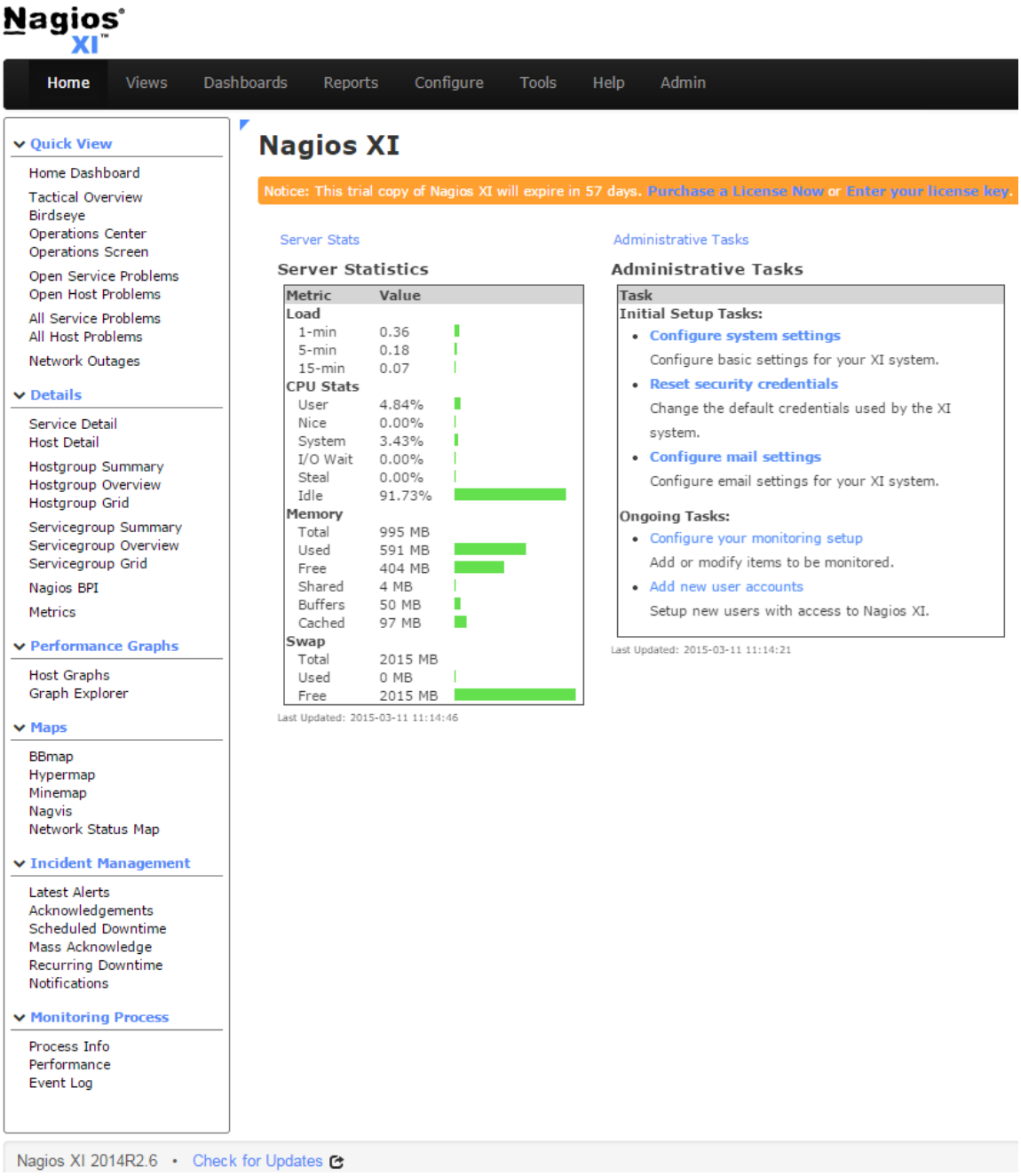
Testiympäristö toteutettiin asentamalla sekä Zabbix että Nagios palvelimet olemassa olevaan virtuaaliympäristöön, jonka jälkeen kyseinen virtuaaliympäristö lisättiin kokonaisuudessaan valvontaan.

4.2 Nagios

Nagios XI on kaupallinen, yrityskäyttöön tarkoitettu IT-standardi ratkaisu yritysten infrastruktuurin valvontaan. Nagios XI on kehitetty versio ilmaisesta Nagios Core:sta ja tarjoaa valvonnan kaikille infrastruktuurin kriittisille kohteille kuten kytkimille, käyttöjärjestelmille, ohjelmistoille sekä palveluille. Lisäksi Nagios XI tarjoaa laajan käsityksen yrityksen IT infrastruktuurista ongelmien ehkäisemiseksi ennen vaikutusta yrityksen toimintaan. (Nagios XI.)

4.3 Käytettävyys

Zabbix:n käyttöliittymästä poiketen Nagios XI ei tarjoa yhtä standardisoitua käyttöliittymää. Valmiiksi asennettuna Nagios XI tarjoaa Nagios Corelle kehitettyä verkkokäyttöliittymää, mutta Nagios XI tukee käyttäjien itse kehittämiä käyttöliittymiä, kuten puhelimelle tai varta vasten eri käyttöjärjestelmille kehitettyjä ratkaisuja. Zabbix taas tukee vain yhtä verkkokäyttöliittymää. Nagios-XI:nperuskäyttöliittymä on nähtävilläkuvassa 11. (Gutherie 2013, 13-14; Nagios XI administrator guide, Monitoring configuration.)



Kuva 11 Nagios XI:N peruskäyttöliittymä.

Valvontaohjelmiston päivittäminen on havaittavasti helpompaa Nagioksen kuin Zabbixin kanssa. Nagios XI sisältää toiminnon ohjelmiston automaattiseen päivittämiseen uuden version tullessa saataville. Tämä toiminto voidaan ottaa käyttöön tai poistaa käytöstä vapaasti. Zabbixin tilanteessa päivitys on tehtävä manuaalisesti, joka vaatii mm. Zabbix tietokannan ja PHP tiedostojen

varmuuskopioinnin ja manuaalisen siirron uuteen ympäristöön. (Upgrade procedure. Nagios XI – How to upgrade using the web UI.)

Nagios XI:n peruskäyttöliittymä on Zabbix:iin verrattuna käyttäjäystävällisempi. Tuetuille valvontakohteille on olemassa ohjatut asennustoiminnot, jotka opastavat käyttäjää valvonnan käyttöönotossa. Jos kohteen valvontaa ei tueta alunperin, on mahdollista etsiä Nagioksen ylläpitämästä tietokannasta käyttäjien luomia ohjattuja asennustoimintoja. Toisaalta, jos ohjattua toimintoa ei ole tai käyttäjä haluaa kustomoida valvontakohdetta ohjatun asennuksen sallimien vaihtoehtojen ulkopuolella, ainoa vaihtoehto tämän toteuttamiseen on konfiguroida muutokset suoraan Nagios XI palvelimen tiedostoihin palvelimen kautta, sillä verkkokäyttöliittymä ei tue ohjatun asennuksen ulkopuolisia toimintoja.

4.4 Valvontakohteet

Käytännössä Zabbixin ja Nagios XI:n välillä ei ole havaittavissa eroa valvottavien kohteiden määrän välillä. Tavanomaisessa yrityksessä kumpikin ratkaisu kykenee valvomaan kaikkia tarvittavia laitteita ilman erityisvaatimuksia. Kumpikin ohjelmisto kykenee pohjimmiltaan valvomaan:

- Virtuaaliympäristöjä
- Java sovelluksia
- Fyysisiä tietokoneita
- Verkkolaitteita (kytkimet, reitittimet jne.)
- Tietokantoja
- Verkkosivuja
- Laitekomponentteja (CPU, lämpötila jne.)

Kumpikin ohjelmisto käyttää hieman toisistaan poikkeavia ratkaisuja, kuten Zabbix ja Nagios agentit sekä Zabbix Java Gateway ja Nagios JMX plugin, mutta lopputulos on sama. Pääasiallinen ero Nagios ja Zabbix valvonnassa ilmenee kohteissa, joiden valvontaa kumpikaan ohjelma ei suoraan tue. Tässä tilanteessa Nagios tarjoaa paremman tuen käyttäjien kehittämien valvontaratkaisujen jakamiseen, joten Nagios XI:n tilanteessa harvinaisempien valvontakohteiden lisääminen ympäristöön on usein helpompaa. Zabbix kuitenkin tarjoaa käyttäjille mahdollisuuden kehittää omia ratkaisuja useilla täysin tuetuilla ohjelmointikielillä. (monitoring configuration. Monitor everything.)

5 POHDINTA JA YHTEENVETO

Opinnäytetyön aihe oli luonnollinen jatke harjoittelun aikana toteutetuille tehtäville. Tämän seurauksena Zabbixin käytöstä oli kokemusta huomattavasti enemmän kuin vertailtavan Nagios XI:n käytöstä. Työn tarkoituksena kuitenkin oli pääasiassa selvittää Zabbixin käyttömahdollisuudet ja hyödyllisyys keskisuurelle yritykselle. Nagioksen osa opinnäytetyöstä oli vain selvittää kykeneekö Zabbix samaan kuin kaupallinen sovellus.

Itse opinnäytetyöprosessin aikana Zabbixin käyttöön ei tarvinnut keskittyä erityisemmin, sillä harjoittelun aikana Zabbixin käyttö ja asennus tuli tutuksi, minkä lisäksi työn tarkoituksena ei ollut ohjeistus Zabbixin käyttöön. Tämän huomioon ottaen ja oman kokemuksen perusteella siitä, että Zabbixin peruskäytön opettelu ei vaadi huomattavasti aikaa, työ toteutettiin oletuksella että lukija joko ymmärtää keskeiset termit ja toiminnot tai on valmis opettelemaan ne itsenäisesti.

Vaikka pohjana oli useamman kuukauden kokemus Zabbixin käytöstä, projektin aikana esiin tulleiden käyttökohteiden määrä oli silti yllättävä. Aiempi kokemus oli keskittynyt lähinnä SNMP valvontaan, joten projekti vaati enemmän tutkimustyötä ja tutustumista muihin Zabbix valvonnan ratkaisuihin kuin oli alunperin oletettu. Erityisesti oudommat ratkaisut, kuten JMX vaativat enemmän tutustumista ennen valvonnan käyttöönottoa. Lopputulos oli kuitenkin huomattavan avartava kokemus, joka laajensi omaa tietämystä sekä Zabbixista että verkkoympäristöistä.

Kun ottaa huomioon kokemuksen puutteen suurimman osan valvontaratkaisujen ja prokollien kanssa, projektin aikana ilmeni yllättävän vähän ongelmia. Suurin ongelmia aiheuttanut tilanne oli Zabbix java gatewayn ja JMX:n väliset erot porttikäytännöissä. Koska Zabbixin ratkaisu JMX valvontaan on eräänlaisena adapterina Zabbix palvelimen ja JMX:n välillä toimiva Zabbix Java gateway, käyttää gateway Zabbixin verkkoasetuksia. Ongelma ilmeni siinä, että JMX ei

käytä tiettyjä määriteltyjä portteja datan siirtoon kuten Zabbix, vaan valitsee randomilla vapaan portin jota se käyttää datan lähettämiseen vastaanottavalle palvelimelle. Tämä taas aiheutti ongelman siinä mielessä, että Zabbix suostui vastaanottamaan dataa vain itselleen käyttöön määritellyn portin kautta. Tämä ongelma esti koko JMX valvonnan käytön totaalisesti useamman viikon ajan. Loppujen lopuksi ongelma saatiin ratkaistua. Selvitysprosessin aikana kuitenkin selvisi, että tämä vaikuttaa olevan yleinen ongelma Zabbixin JMX valvonnan kanssa. Tosin kun JMX valvonta saadaan toimimaan, sen toiminta ja käyttö itsessään on ongelmatonta. Käyttöönotto on kuitenkin mahdollisesti haastavaa. Muita suuremman tason ongelmia projektin aikana ei ilmennyt, muutamat pienet ongelmat olivat yleensä muutamassa minuutissa korjattavia käyttäjävirheitä.

Yrityskäytön näkökulmasta Zabbix kykenee täyttämään alustavasti kaikki tavanomaisen yrityksen verkkovalvontavaatimukset. Tietyt tilanteet kuten JMX vaativat hienosäätöä käyttöönoton aikana, mutta valvonnan toimivuuden puolesta ei projektin aikana havaittu mitään huomattavia ongelmia. Zabbix ei ole täydellinen ratkaisu verkkovalvontaan, mutta täydellistä ratkaisua ei todennäköisesti edes ole olemassa. Projektin perusteella Zabbix on täysin toimiva ratkaisu suurempienkin yrityksien verkkovalvontaan, joka tukee alustavasti kaikkia tavanomaisessa tilanteessa esiin tulevia valvontakohteita, ja erittäin harvoissa tapauksissa että valvottava laite ei ole suoraan tuettu, on Zabbixille mahdollista ohjelmoida kyseistä laitetta valvova ratkaisu.

Zabbix agentti tulee todennäköisesti olemaan käytössä lähes jokaisessa yrityksessä joka käyttää Zabbix valvontaa. Agentti on Zabbixin pääasiallinen ratkaisu fyysisten työpisteiden ja palvelimien valvontaan. Koska agentin kautta on mahdollista valvoa huomattavaa määrää kohteita, useimmissa tilanteissa Zabbix agentti tulee todennäköisesti olemaan ainoa tarvittava valvontaratkaisu fyysisissä tietokoneissa ja palvelimissa. Zabbix agenttia on tosin myös mahdollista käyttää virtuaalikoneissa, jos virtuaaliympäristön valvonta koetaan riittämättömäksi. Ongelmana agentin käyttöönotossa on, että Zabbix ei tarjoa automaattista ratkaisua levittää agenttia kohdelaitteille, joten tämä on toteutettava manuaalisesti tai kehitettävä erillinen levitysratkaisu.

Zabbixin käyttämä SNMP valvonta tulee todennäköisesti olemaan käytössä jos yrityksen tarkoituksena on valvoa verkkoliikennettä.Kunnollisten triggereiden käyttö helpottaa huomattavasti verkko-ongelmien lähteen paikantamista, jos esimerkiksi verkon katketessa tietystä työpisteestä Zabbix hälyttää ylläpitäjän kytkimen irronneesta johdosta. Muissa tilanteissa SNMP valvonnalle ei ole erityisemmin käyttöä.

Virtuaaliympäristöjen valvonnassa Zabbix tukee vain Vmwarea. Tämä voi aiheuttaa ongelmia yrityksille, jotka käyttävä muita virtualisointiratkaisuja, kuten Hyper-V:tä. Vmwaren tilanteessa Zabbix valvonta on kuitenkin yksinkertaista ja tehokasta. Erityisesti virtuaalikoneiden automaattinen lisääminen valvontaan toimii testien perusteella moitteetta, joskin se vaatii aikaa. Projektin aikana Vmware valvonnan käyttöönoton jälkeen kaikki 351 virtuaalikonetta olivat listattuna seuraavana aamuna. Muiden virtuaaliympäristöjen valvontaa varten käyttäjät ovat kehittämässä ja jakamassa omia ratkaisujaan, mutta täysin luotettavaa ratkaisua tähän ei ole, Zabbix agentin asentamisen kaikille virtuaalikoneille lisäksi.

Kuten aiemmin mainittiin, Java sovellusten valvonnan käyttöönotossa on tiettyjä vaikeuksia. Javasovellusten valvonta on myös rajoitettu tilanne, joka ei välttämättä tule esiin kaikilla yrityksillä. Java sovelluksilla on mahdollista valvoa laitteiden resurssikäyttöä, mutta Zabbix kykenee siihen myös muilla keinoin. Täten java valvonta Zabbixilla on tilanne, jota kannattaa harkita vain jos haluttava valvontadata on mahdollista saada vain java sovelluksen avulla. Tosin kun valvonta saadaan toimimaan kunnolla, ei siinä projektin aikana havaittu ongelmia.

Kuten java valvonta, IPMI valvonta on tilanne joka voi olla hyödyllinen, mutta IPMI:n kautta valvottavia rautatason tilastoja on usein mahdollista valvoa myös muilla lähestymistavoilla. Jos IPMI valvontaa tarvitaan, Zabbix kuitenkin tukee täysin tietyissä laitteissa sisäänrakennettuja IPMI agentteja.

Suurempien valvontaprosessien lisäksi projektin aikana tutustuttiin myös Zabbixin tarjoamiin pienempiin valvontakohteisiin, kuten verkkosivujen ja tietokantojen valvontaan. Verkkosivujen valvonnassa Zabbix ei tarjoa paljoa vaihtoehtoa, vaan keskittyy olennaiseen. Siis onko sivusto ylhäällä vai ei. Tämä voi varmasti olla tietyille yrityksille hyödyllinen toiminta, erityisesti jos yrityksen oman tai asiakkaiden verkkosivun ylläpito on tärkeää. Tietokantojen valvonta rajoittuu SQL kyselyiden automaattiseen suorittamiseen SQL tietokannoissa. Siis tietokantojen valvontaa varten on opeteltava myös SQL kyselyiden käyttö.

Zabbixia ja Nagiosta vertaillessa lähtökohta oli tietyssä määrin ongelmallinen, sillä Nagios XI:n käyttöönoton aikana oli jo useiden kuukausien kokemus Zabbixin käytöstä, jolla oli mahdollisuus värittää mielipiteitä Nagioksen käytöstä. Kuitenkin projektin aikana voitiin todeta, että teknisesti Zabbix ja Nagios XI kykenevät suorittamaan samat tehtävät, joskin välillä eriävillä ratkaisuilla. Pääpiirteisesti teknisessä mielessä projektin aikan ei voitu kummankaan todeta olevan selkeästi parempi yrityksen käyttöön. Pääasiallinen ero ilmeni käyttöliittymässä sekä käyttöönoton helppoudessa. Projektin aikana saatujen kokemusten perusteella Nagios on huomattavasti helpompi aloittelevalle käyttäjälle, johtuen lähinnä käyttöliittymään kuuluvien ohjeistettujen toimintojen määrästä. Zabbixin toimiva käyttö vaati useamman päivän totuttelun ennen valvonnan toimivaa käyttöönottoa, mutta Nagiksen tilanteessa ensimmäisten kohteiden toimivaan valvontaan saantiin kului alta päivä. Tähän saattoi tietysti vaikuttaa Zabbixista saatu kokemus termistöstä ja tietyistä yhtenevistä toiminnoista. Nagioksen käytön helppous tosin aiheutti ongelman pitemmällä tasolla, sillä valvonnan kustomointi oli havaittavasti vaikeampaa kuin Zabbixissa. Tämän arvioitiin johtuvan siitä, että Nagioksen ohjatut toiminnot rajoittivat tiettyjä vaihtoehtoja Zabbixin vapaampaa, mutta opettelua vaativaa käyttöä enemmän.

Projektin tuloksena voitiin kuitenkin todeta, että Zabbix on tehokas ja täysin toimiva ratkaisu eri kokoisten yritysten verkkovalvontaan. Avoimen lähdekoodin tilastaan riippumatta se kykenee samaan kuin Nagios XI:n kaltaiset kaupalliset tuotteet. Se kuitenkin oli selvää, että Zabbixin käyttöön on nähtävä enemmän vaivaa, erityisesti koska olemassa oleva dokumentaatio on heikompaa kuin

kaupallisella vastikeella. Jos yritys on valmis ottamaan aikaa valvontajärjestelmän opetteluun ja satunnaiseen trial-and-error lähestymistapaan, voidaan tämän projektin kokemusten perusteella Zabbixia suositella valvontajärjestelmänä.

6 LÄHTEET

6.1 Verkkolähteet

Ad-hoc graphs, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/2.4/manual/config/visualisation/graphs/adhoc

Agent, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 11.9.2015. https://www.zabbix.com/documentation/2.4/manual/concepts/agent

Applications, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 30.8.2015. https://www.zabbix.com/documentation/2.0/manual/config/visualisation/screens

Authentication, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 26.8.2015. https://www.zabbix.com/documentation/2.4/manual/web_interface/frontend_sections/administration/authentication

Auto Discovery, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 3.9.2015. http://www.zabbix.com/auto_discovery.php

Bar reports, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/2.4/manual/web_interface/frontend_sections/reports/bar_reports

Custom graphs, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/2.4/manual/config/visualisation/graphs/custom

Database creation scripts, n.d.Verkkodokumentti, Zabbixinsivusto. Viitattu 26.8.2015.
https://www.zabbix.com/documentation/2.4/manual/appendix/install/db_scripts

Discovery, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 3.9.2015. https://www.zabbix.com/documentation/1.8/manual/auto-discovery

Event sources, n.d. Verkkodokumentti, Zabbixin sivust. Viitattu 8.9.2015. https://www.zabbix.com/documentation/2.4/manual/config/events/sources

IPMI checks, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/2.4/manual/config/items/itemtypes/ipmi

Items, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 30.8.2015. https://www.zabbix.com/documentation/2.4/manual/config/items

Java Management Extensions. n.d. Verkkodokumentti. Oraclen sivusto. Viitattu 31.5.2015. https://docs.oracle.com/javase/7/docs/technotes/guides/jmx/

Low-level discovery, n.d.Verkkodokumentti, Zabbixinsivusto. Viitattu 3.9.2015. https://www.zabbix.com/documentation/2.4/manual/discovery/low_level_discovery

Maps, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. http://www.zabbix.com/maps.php

Monitor everything. n.d.Verkkodokumentti. Zabbixin sivusto. Viitattu 13.3.2015. http://www.zabbix.com/monitor_everything.php

Monitoring Configuration, n.d. Verkkodokumentti, Nagioksen sivusto. Viitattu 11.9.2015. https://assets.nagios.com/downloads/nagiosxi/guides/administrator/monitoringconfig.php

Monitoring of IPMI devices, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/1.8/manual/ipmi

Nagios XI. n.d.Nagioksen sivusto. Viitattu 13.3.2015.http://www.nagios.com/products/nagiosxi

Nagios XI administrator guide. n.d.Verkkodokumentti. Nagioksen sivusto. Viitattu 13.3.2015. http://assets.nagios.com/downloads/nagiosxi/guides/administrator/

Nagios XI – How to upgrade using the web UI, n.d.Verkkodokumentti, Nagioksensivusto. Viitattu 11.9.2015. https://assets.nagios.com/downloads/nagiosxi/docs/Upgrading-Nagios-XI-Using-the-Web-UI.pdf

ODCB monitoring, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015.https://www.zabbix.com/documentation/2.4/manual/config/items/itemtypes/odbc_checks

Proxies, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/2.4/manual/distributed_monitoring/proxies

Proxy, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/2.4/manual/concepts/proxy

Screens, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 30.8.2015. https://www.zabbix.com/documentation/2.0/manual/config/visualisation/screens

Simple graphs, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 4.9.2015. https://www.zabbix.com/documentation/2.4/manual/config/visualisation/graphs/simple

SNMP tutorial. n.d. Verkkodokumentti. ManageEnginen sivusto. Viitattu 30.5.2015. https://www.manageengine.com/network-monitoring/what-is-snmp.html

Templates, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 30.8.2015. https://www.zabbix.com/documentation/2.4/manual/config/templates

Triggers, n.d. Verkkodokumenti, Zabbixin sivusto. Viitattu 11.9.2015. https://www.zabbix.com/documentation/2.4/manual/config/triggers

Upgrade procedure, n.d. Verkkodukomentti, Zabbixin sivusto. Viitattu 11.9.2015.https://www.zabbix.com/documentation/2.4/manual/installation/upgrade

Virtual machine monitoring. n.d.Verkkodokumentti. Zabbixin sivusto. Viitattu 31.5.2015. https://www.zabbix.com/documentation/3.0/manual/vm_monitoring/

Web monitoring, n.d. Verkkodokumentti, Zabbixin sivusto. Viitattu 30.8.2015. https://www.zabbix.com/documentation/2.4/manual/web_monitoring

What is Zabbix.n.d.Verkkodokumentti. Zabbixin sivusto.Viitattu 13.3.2015. http://www.zabbix.com/product.php

Zabbix database monitor, n.d. Verkkodokumentti, lab4 sivusto. Viitattu 4.9.2015. http://lab4.org/wiki/Zabbix_Database_Monitor_English

Zabbix visualization. n.d. Verkkodokumentti. Zabbixin sivusto.Viitattu 13.3.2015. http://www.zabbix.com/visualization.php

6.2 Kirjalähteet

DalleVacche, A. and Lee, S.K., 2012. *Mastering Zabbix.* Olton, Birmingham, GBR: Packt Publishing Ltd.

Gutherie, M., 2013. Instant Nagios Starter. Olton, Birmingham, GBR: Packt Publishing Ltd.