VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Joonas Lindell

ZABBIX-VERKONVALVONTAOHJELMISTON KÄYTTÖÖNOTTO ASIAKASYRITYKSESSÄ

Liiketalous
2023

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittelyn koulutusohjelma

TIIVISTELMÄ

Tekijä	Joonas Lindell
Opinnäytetyön nimi	Zabbix-verkonvalvontaohjelmiston käyttöönotto asiakasyrityksessä
Vuosi	2023
Kieli	suomi
Sivumäärä	32
Ohjaaja	Antti Mäkitalo

Zabbix on verkonvalvontaohjelmisto, jonka avulla on mahdollista valvoa verkkoon kuuluvia laitteita, palvelimia ja ohjelmia. Tässä opinnäytetyössä kuvataan Zabbixin asennustyö pääpiirteissään sekä esitellään lyhyesti verkonvalvontaa ja asiakasyrityksen tarpeita sen suhteen.

Teoreettisena viitekehyksenä opinnäytetyössä esitellään verkonvalvontaa TCP-IP-pinon avulla. Lisäksi luodaan lyhyt katsaus muutamiin muihin verkonvalvontaohjelmistoihin. Zabbixin asennustyön esittely perustuu kevään ja kesän 2022 aikana toteutetun asennustyön dokumentointiin ja Zabbixin omaan käyttöohjeeseen.

Zabbixin asentaminen on monivaiheinen työ, joka vaatii ymmärrystä niin tietoverkoista, protokollista, palvelimista ja käyttöjärjestelmistä kuin perehtymistä Zabbixin dokumentaatioon. Aiheen käsittelyä olisi mahdollista syventää paneutumalla teknisemmin johonkin osa-alueeseen tai laajentamalla valvonnan kohteiden kirjoa esimerkiksi laitteiden suuntaan.

Avainsanat	tietoverkot, TCP/IP, tietoturva, yritystoiminta, asennus

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittelyn koulutusohjelma

ABSTRACT

Author	Joonas Lindell
Title	Setting up Zabbix Network Monitoring Tool in Customer Company
Year	2023
Language	Finnish
Pages	32
Name of Supervisor	Antti Mäkitalo

Zabbix is a network monitoring tool which can be used to monitor devices, servers, and programs. This thesis describes the basic steps of the installation process of Zabbix and gives a short presentation about network monitoring and what the customer company's needs for it are.

The theoretical background of this thesis is network monitoring described by TCP-IP model. In addition, this thesis gives a short presentation of few other network monitoring tools. The installation process of Zabbix described in this thesis is based on documentation of installation of Zabbix in spring 2022 and also on Zabbix's own documentation.

The installation process of Zabbix includes several steps and requires understanding of networks, protocols, servers, and operating systems but also studying Zabbix's documentation. This research could be extended to a more technical aspect or by broadening the variety of devices to some other direction.

Keywords network, TCP/IP, information security, business, installation

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

LYHENTEET JA KÄSITTEET

admin	järjestelmän pääkäyttäjä, josta käytetään myös nimityksiä sysadmin, administrator tai system administrator
API	eli rajapinta, jonka kautta kaksi eri ohjelmistoa voivat keskustella keskenään
CPU	suoritin tai prosessori (Central prosessing unit), joka vastaa tietokoneen prosessien suorittamisesta
docker	tuoteperhe, jonka avulla on mahdollista jakaa ohjelmisto käyttäjälle yhtenä kokonaisuutena ns. kontissa (container)
GPL	avoimen lähdekoodin ohjelmistoissa käytetty lisenssi.
host	tietokone tai muu laite, joka kommunikoi toisten kanssa tietoverkon välityksellä
IP	protokolla (Internet protocol), jota käytetään laitteiden tunnistamiseen internetissä tai lähiverkossa
item	valvottava datan osa Zabbixissa (tässä yhteydessä)
skripti	komentosarja
SLA	(Service level agreement) eli palvelutasosopimus, jossa asiakas ja palveluntarjoaja määrittelevät mitä palveluita palveluntarjoaja toimittaa ja millä standardeilla
TCP	protokolla (Transmission control protocol), jonka avulla voidaan lähettää dataa luotettavasti laitteiden tai ohjelmien välillä

trigger	looginen väite, joka määrittelee raja-arvon, jolla arvioidaan vastaanotettua dataa
template	valmiiksi määritelty asetusten kokonaisuus, jonka voi asettaa hostille
proxy	prosessi, joka kerää dataa Zabbix-palvelimen puolesta dataa vähentäen näin sen kuormitusta

1 JOHDANTO

Lähtölaukaus tälle opinnäytetyölle laukaistiin tammikuussa 2022 istuessani silloisen työpaikkani ruokalassa. Kokeneempi kollega tiedusteli, olisinko kiinnostunut asentamaan asiakasyrityksen ympäristöön erään verkonvalvontaohjelmiston, joka oli siihen asti toiminut yhteistyökumppanin ympäristössä. Joitakin kuukausia myöhemmin olimmekin jo työn touhussa, ja samalla sovin tekeväni opinnäytetyön tämän Zabbix-nimisen ohjelmiston asennustyöstä.

Aiheena tietoturva ja verkonvalvonta on merkittävä, sillä elämme tietoyhteiskunnassa, jossa digitalisaatio koskee isoa osaa yhteiskuntaa. Samalla tietoturvan merkitys niin yritysten kuin yksityishenkilöiden toiminnassa korostuu entisestään, sillä Suomeen kohdistuvien kyberhyökkäysten määrä on ollut kasvussa (Kyberturvallisuuskeskus 12.9. 2022). Samalla Ukrainassa käynnistynyt sota saattaa OP:n tietoturva-asiantuntija Catharina Candolinin mukaan lisätä Venäjältä Suomeen suuntautuvaa kyberrikollisuutta (Candolin, luento 14.10. 2022).

Aihetta lähestytään verkonvalvonnan näkökulmasta ja työssä etsitään vastauksia seuraaviin kysymyksiin:

1. Millaisia vaatimuksia verkonvalvontaohjelmistolle asetetaan asiakasyrityksessä?
2. Millainen Zabbix-verkonvalvontaohjelmisto on?
3. Miten Zabbix-verkonvalvontaohjelmisto asennetaan?

Esitettyihin kysymyksiin vastataan opinnäytetyön luvuissa 2 ja 3. Luvussa 2 esitellään verkkoa ja verkonvalvontaa sekä erilaisia verkonvalvontaohjelmistoja. Luvussa 3 puolestaan esitellään yrityksen tarpeita verkonvalvonnalle sekä eri työvaiheet, joita Zabbixin asentamiseen kuuluu.

Työ on pyritty kirjoittamaan niin, että henkilö, jolla on IT-alan perustiedot, pystyisi ymmärtämään tekstin. Yksityiskohtaisia teknisiä kuvauksia on pyritty välttämään, jotta teksti olisi sujuvasti luettavissa ja kokonaiskuvan muodostaminen olisi helpompaa.

2 VERKONVALVONTA

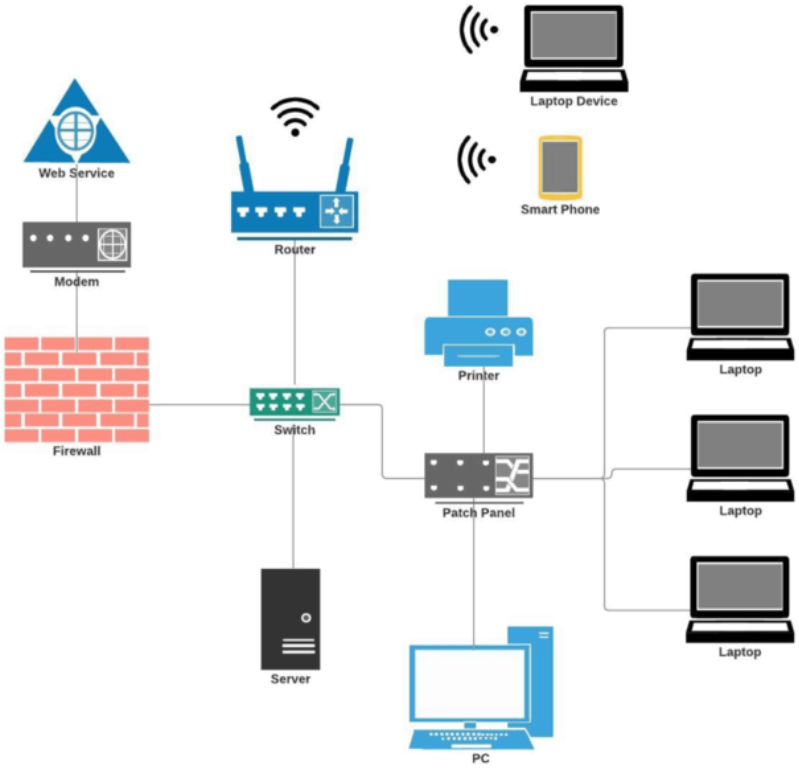
Ajateltaessa melkein minkä tahansa yrityksen toimintaa, on sen tietoverkkoon kuuluvien laitteiden toiminta lähes poikkeuksetta varsin kriittistä itse yrityksen toiminnalle. Varsin monen yrityksen kohdalla tietoliikenneyhteyksien ja verkkopalveluiden kaatuminen tai hidastuminen haittaa merkittävästi toimintaa, puhumattakaan sellaisista yrityksistä, joiden toiminnasta suurin osa on verkossa tapahtuvaa. Verkonvalvonnan avulla on mahdollista pyrkiä muodostamaan kuva siitä, mitä yrityksen tietoverkossa tapahtuu.

2.1 Mitä on verkonvalvonta?

Verkonvalvonta on verkon ylläpitäjän suorittamaa monitorointia, jolla tämä pyrkii saamaan kokonaiskuvan verkkoon kuuluvien osien toimintakyvystä ja mahdollisista häiriöistä. Tässä valvonnassa tukeudutaan usein verkonvalvontajärjestelmään, jonka tehtävänä on ilmoittaa ylläpitäjälle häiriöiden ilmaantumisesta. Verkonvalvontajärjestelmän tehtävänä on valvoa niin yhteyksien muodostumista kuin valvonnan piiriin kuuluvien järjestelmien suorituskykyä. (Jethva 2022.)

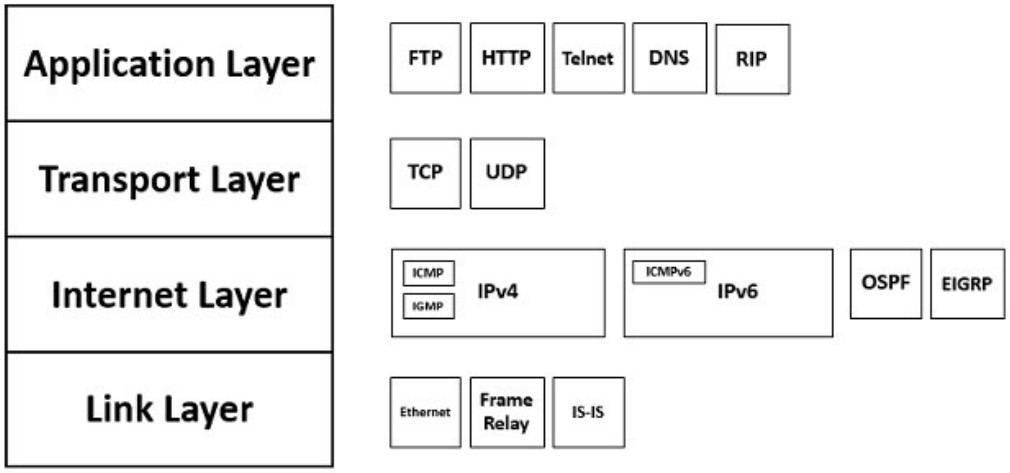
Valvonnan piiriin kuuluvien verkon osien kirjo on hyvin laaja: WAN- ja LAN-verkot, pilvipalvelut, IoT-laitteet, etäkäyttäjät, VPN-yhteydet, mobiililaitteet, palvelimet, palomuurit, palvelimet ja clientit jne. Yhteistä näille kaikille on niiden siirtämä tieto jotakin tietoliikenneprotokollaa käyttäen. (DNS Stuff.)

Kuvassa 1 on esimerkki pienen yrityksen verkosta. Karkeasti kuvassa näkyvä verkko voidaan jakaa kahteen osaa: sisäverkkoon ja ulkoverkkoon. Näistä ensimmäiseen on rajattu pääsy ja jälkimmäinen puolestaan on julkinen internet-verkko. Sisäverkko on reititetty kytkinten kautta eri laitteille, kuten palvelimille, tietokoneille ja Wifi-reitittimille. Internet-yhteys puolestaan kulkee palomuurin kautta, joka rajaa pääsyn sisäverkkoon. Isommassa yrityksessä verkko toimii mahdollisesti hyvin samalla tavalla, mutta IP-verkko on esimerkiksi voitu jakaa eri IP-alueisiin turvallisuuden lisäämiseksi. Lisäksi verkkoon voi kuulua muitakin laitteita, kuten lisää palvelimia, IoT-teknologiaa, pilvipalveluita tai sisäverkon palomuuri. (Jones IT.)



Kuva 1. Pienen yrityksen verkko (Jones IT)

Yksi mahdollinen keino havainnollistaa tietoliikenneyhteyksiä on TCP-IP-pino, joka kuvaa verkkolaitteiden yhteyksiä neljän pinossa olevan kerroksen avulla (kuva 2). Malli koskee muitakin protokollia kuin TCP ja IP, mutta ne ovat keskiössä, koska suurin osa yhteyksistä toteutetaan niillä. TCP-protokolla määrittää sovellusten välisiä yhteyksiä ja sen avulla luodaan pienempiä paketteja, jotka lähetetään internetin välityksellä. IP-protokolla puolestaan määrittää näiden pakettien reittejä ja osoitteita. (Techtarget.)



Kuva 2. TCP-IP-pino (Techtarget, The Ultimate Guide to TCP/IP)

IP-protokolla on käytössä mallin toiseksi alimmalla kerroksella, verkkokerroksella. TCP puolestaan sijoittuu malliin toiseksi ylimmälle kerrokselle, kuljetuskerrokselle. Mallin ylimmällä kerrokselle, sovelluskerroksella, käytössä olevia protokollia ovat mm. internet-selaimissa tiedonsiirrossa käytetty HTTP sekä sähköpostien välittämisessä käytetty SMTP. Alimpana kerroksena mallissa on nk. peruskerros, joka välittää IP-paketteja eteenpäin mm. Ethernet- tai DSL-tekniikoiden avulla. (Techtarget.)

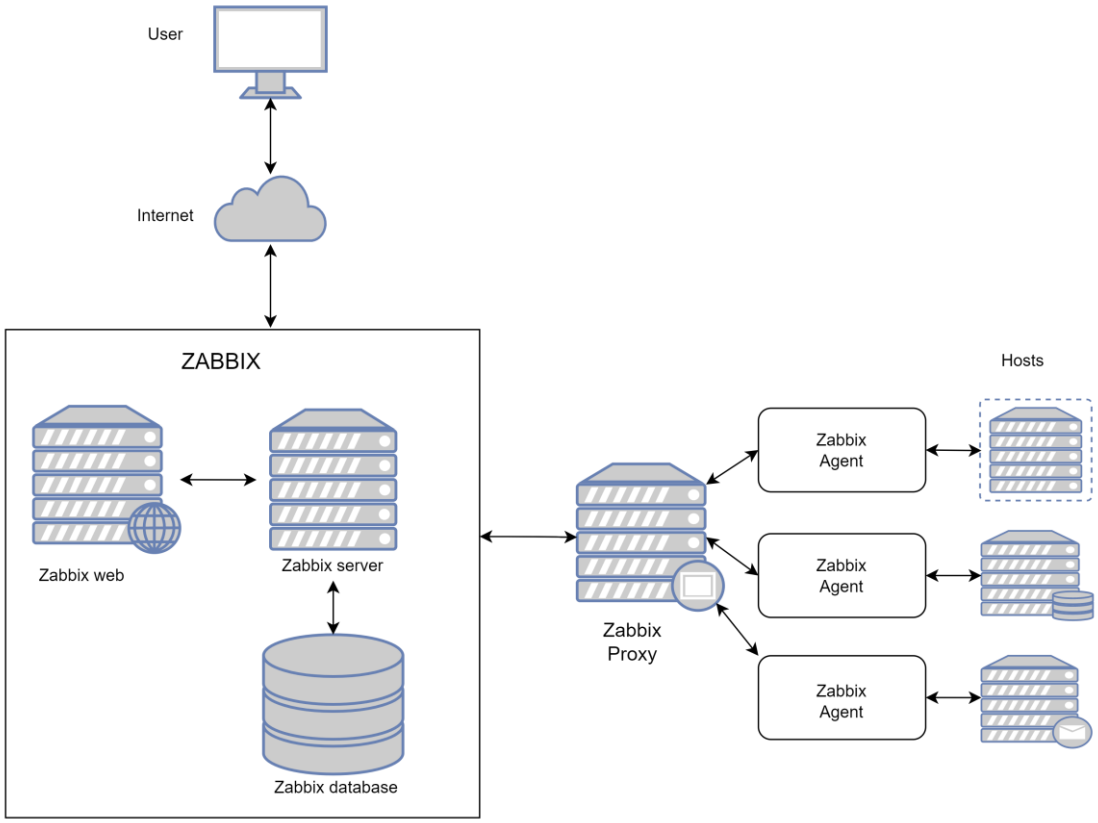
SNMP (Simple Network Management Protocol) on tietoliikenneprotokolla, jolla hallitaan verkossa olevia laitteita TCP-IP-pinon mukaisesti. Siitä on olemassa kolme eri versiota (v1-3) ja sen agentin avulla monitoroidaan verkkoon kuuluvia laitteita. SNMP:tä hallitaan NMS:än (Network Management System) kautta, jolla annetaan käskyjä agentille. SNMP:n käyttöön kuuluu vielä oleellisesti MIB (Management Information Base), joka sisältää valvottavan kohteen muuttujat. (Huawei.)

2.2 Zabbix verkonvalvontaohjelmistona

Zabbix on verkonvalvontaohjelmisto, joka tarjoaa mahdollisuuden valvoa lukuisia erilaisia laitteita tai palveluita keskitetysti. Valvontaan voidaan kytkeä niin fyysisiä laitteita, kuten kytkimiä, reitittimiä tai muita verkkolaitteita sekä esimerkiksi palvelimia tai sensoreita. Myös erilaisten virtuaalisten palveluiden tai ohjelmistojen valvonta on mahdollista. Valvonnan kohteita voivat olla niin sovellukset, pilvipalvelut, tietokannat, virtuaalikoneet (VM) kuin verkkosivut. (Zabbix, Features.)

Zabbix valvoo kohteita lähettämällä niille pyyntöjä käyttäjän määrittämällä tiheydellä, jossa pienin mahdollinen väli on yksi sekunti. Zabbix voi toimittaa valvontadatan käyttäjän toiveiden mukaisesti niin numero- tai tekstimuotoisena, kuin JSON-, XML- tai CSV-tiedostoina. Itse valvonta voidaan suorittaa niin käyttöjärjestelmään asennettavan Zabbix-agentin avulla, kuin jonkin protokollan, kuten SSH, SNMP, IPMP tai HTTP, avulla. (Zabbix, Features.)

Itse Zabbix koostuu kolmesta osa-alueesta: Zabbix-käyttöliittymä, palvelin sekä tietokanta (kuva 3). Käyttöliittymän avulla käyttäjä hallinnoi niin valvottavia kohteita, käyttäjätunnuksia kuin ohjelman toimittamaa dataa ja sen pohjalta laadittuja ilmoituksia. Agentin tai jonkin protokollan avulla suoritetun valvonnan voi hoitaa välityspalvelimen eli *proxyn* avulla. (Zabbix, Features.)



Kuva 3. Zabbixin arkkitehtuuri

Käyttäjä pystyy itse määrittämään, milloin Zabbixin kohteelta vastaanottama tieto saavuttaa tietyn raja-arvon, eli *triggerin* (kuva 4). Tällöin Zabbix lähettää ilmoituksen käyttäjälle tai vaihtoehtoisesti käyttäjä voi asettaa toiminnon, esimerkiksi

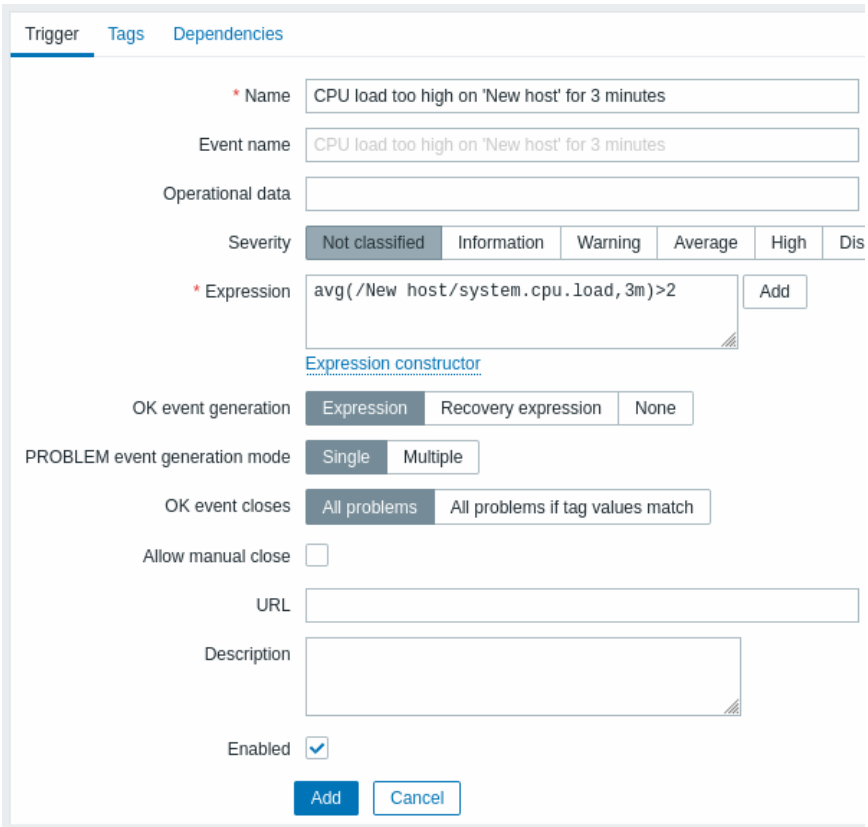
skriptin, jonka Zabbix tässä tapauksessa suorittaa. Yksinkertainen esimerkki skriptistä on HTTP-kysely, jolla haetaan valvonnassa olevan verkkosivun tiedot:

```
var request = new HttpRequest();

return request.get("https://www.example.com/release_notes");
```

(Sbcode, Administration scripts)

Valvottavat kohteet voivat olla niin laitteita (*host*) kuin tietty data (*item*). Esimerkkeinä hyödyllisistä valvottavista kohteista toimivat laitteen prosessorin (*CPU*) kuormitus tai palvelimen verkkoliikenne IP-protokollan mukaan valvottuna. Tässä tapauksessa Expressions-kohdassa on määritelty CPU-kuormituksen keskiarvo suuremmaksi kuin kaksi (avg/New host/system.cpu.load, 3m) > 2), jolloin trigger aktivoituu raja-arvon täyttyessä. (Zabbix, Features; Zabbix, Definitions.)



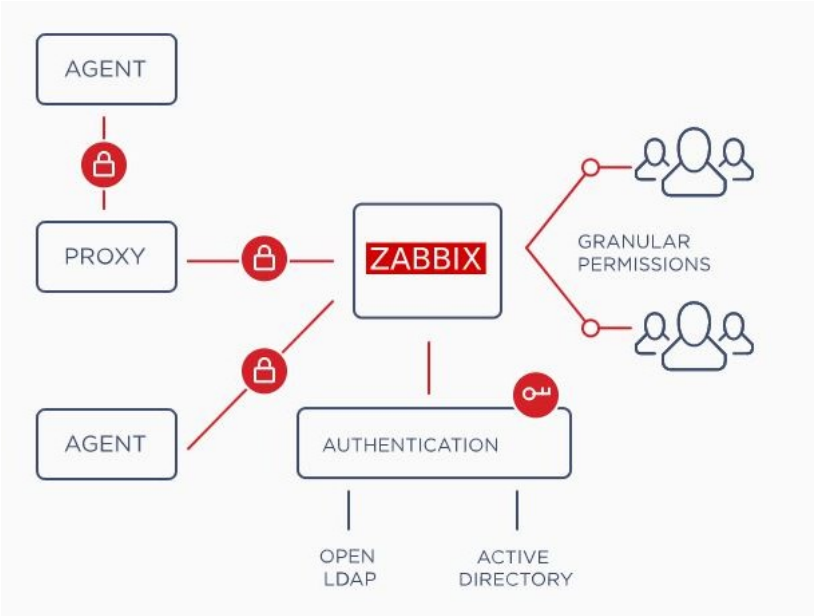
Kuva 4. Triggerin luominen (Zabbix, New trigger)

Kun triggeri käynnistyy, lähtee käyttäjälle ilmoitus hänen määrittämällään tavalla. Zabbixin tarjoamia ilmoitusvaihtoehtoja ovat niin sähköposti-, Teams- kuin Tele-

gram-viesti, monen muun ohella. Mahdollista on myös integrointi esimerkiksi ulkoiseen tikettijärjestelmään, jos palvelun käyttäjä on vaikkapa yrityksen IT-tuki. Viestin lähettäminen voidaan optimoida niin hälytyksen vakavuuden, vuorokaudenajan kuin vastaanottajien mukaan. Esimerkiksi on mahdollista lähettää vähemmän vakavat viestit sähköpostilla laajemmalle käyttäjäjoukolle ja vakavammat pikaviestinä pääkäyttäjille eli *admineille.* (Zabbix, Features.)

Zabbixin keskeisenä ominaisuutena voidaan edellä kuvatun perusteella nähdä muokattavuus, mikä tulee ilmi myös käyttäjien lisäämisessä tai Zabbixin tarjoamassa hostien monitoroinnissa. Käyttäjä pystyy Zabbixin käyttöliittymässä rakentamaan monenlaisia graafisia kuvaajia palveluiden tilasta ja tarvittaessa lähettämään kootun tiedon automaattisesti vaikkapa PDF-tiedostona tai datana rajapinnalle (API). Esimerkiksi käyttäjä voi jaotella hosteja kuvaajiin sen kategorian (laite/palvelu) mukaan tai kriittisyyden (SLA) mukaan. (Zabbix, Features.)

Zabbixin käyttäjiä voidaan luoda niin paikallisina Zabbix-käyttäjinä, kuin LDAP- tai HTTP-protokollan mukaisesti tunnistettavina käyttäjinä. Näin ollen yritys voi esimerkiksi lisätä omia käyttäjiään Zabbix-käyttäjiksi, jos tunnistautumisessa on käytössä Microsoft Active Directory tai OpenLDAP (kuva 5). Käyttäjiä voidaan hallinnoida erilaisten ryhmien kautta, vaikkapa työtehtävien tai osaston mukaan. Hallinnointi on mahdollista myös erilaisten roolien kautta, kuten ylläpitäjä tai vieraskäyttäjä. Tällöin vieraskäyttäjällä voi olla vain lukuoikeus, kun ylläpitäjä pystyy muokkaamaan hosteja tai ilmoituksia. (Zabbix, Authentication; Zabbix, User groups; Zabbix, User roles.)



Kuva 5. Zabbix-tunnistautuminen (DevOps School)

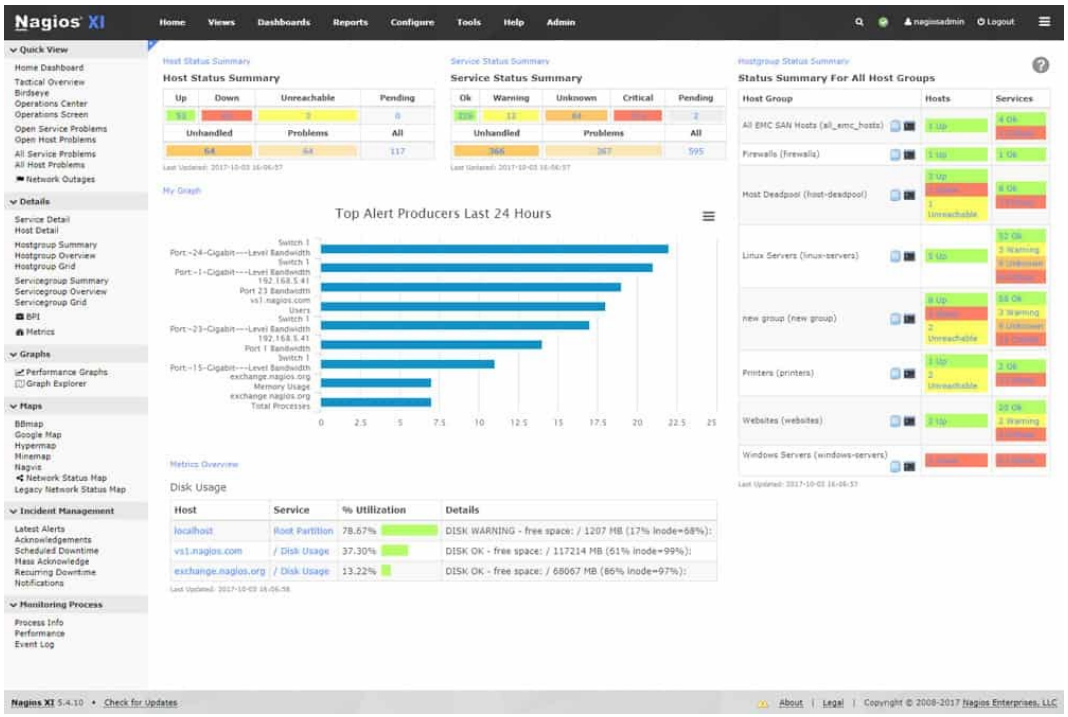
Zabbix-ohjelmisto on muokattavissa myös koodinsa puolesta, sillä ohjelmiston lähdekoodi on avoimesti saatavilla GPL General Public License version 2:lla. Ohjelmiston käyttäminen on ilmaista, vaikka sen kehittämisestä onkin vastannut Zabbix SIA-niminen yhtiö. Alun perin Zabbixin on luonut Alexei Vladishev 2000-luvun alussa Latviassa, mistä yhtiö on lähtenyt leviämään ympäri maailmaa. Nykyään Zabbixilla on toimintaa niin Latviassa, Japanissa, Yhdysvalloissa, Venäjällä kuin Brasiliassa. (Zabbix, Introduction; Zabbix, About.)

2.3 Muita verkonvalvontaohjelmistoja

Vaihtoehtoisia verkonvalvontaohjelmistoja on olemassa lukuisia, joten tässä opinnäytetyössä esitelty Zabbix ei suinkaan ole ainoa. Keskeisiä eroja eri verkonvalvontaohjelmistojen välillä lienevät maksullisuus, helppokäyttöisyys sekä kattavuus. Seuraavassa muutama poiminta verkonvalvontaohjelmistoista, jotka ovat mahdollisia vaihtoehtoja Zabbixille.

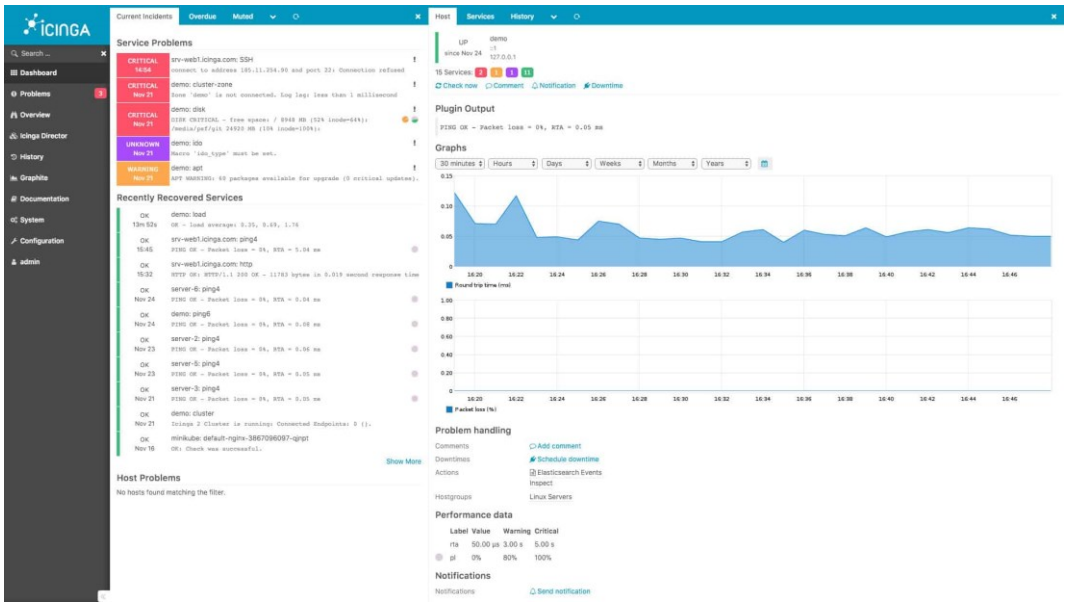
Nagios XI on Nagios Enterprises -nimisen yhtiön kehittämä avoimen lähdekoodin verkonvalvontaohjelmisto, jonka ilmainen versio on nimeltään Nagios Core. Nagioksella valvotaan Zabbixin tapaan Hostien tilaa ja järjestelmän kautta on mahdollista tilata hälytyksiä (kuva 6). Nagios Core ei kuitenkaan sisällä käyttöliittymää,

joten kyseisen version käyttö vaatii enemmän tietoteknistä osaamista kuin maksullinen versio. (Keary 2022; Nagios.)



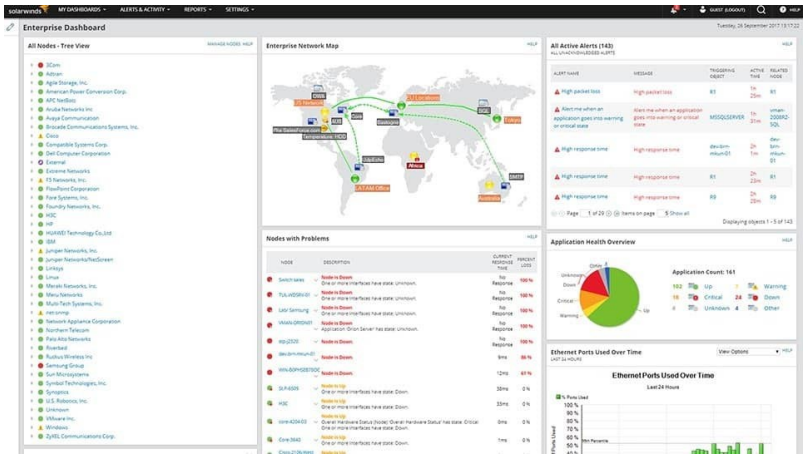
Kuva 6. Nagios XI:n käyttöliittymä (Keary 2022)

Icinga on Nagioksen pohjalta kehitetty verkonvalvontaohjelmisto, joka on ilmainen ja sisältää Nagioksesta poiketen graafisen käyttöliittymän (kuva 7). Historiansa vuoksi Icinga on yhteensopiva Nagioksen ja sen lisäosien kanssa, mutta Icingan kehittäjäyhteisö on luonut myös omia laajennuksia. Nagioksen tapaan Icingan käytössä ohjelmointitaidot ovat varsin hyödyllisiä ja käyttäjä on riippuvainen kehitysyhteisön tuesta ja päivityksistä. (Comparitech.)



Kuva 7. Icingan käyttöliittymä (Keary 2022)

Network Performance Monitor on Solarwindsin kehittämä verkonvalvontaohjelmisto (kuva 8), joka on kokeilujakson jälkeen maksullinen. Zabbixin tapaan Network Performance Monitor käyttää SNMP-protokollaa ja tunnistaa automaattisesti verkon kytketyt laitteet. Ohjelma mahdollistaa muista tässä esitellyistä ohjelmista poiketen verkkopakettien jäljityksen sekä automatisoidun verkkokaavioiden piirtotyökalun. (Keary 2022.)



Kuva 8. Solarwindsin Network Performance Monitorin käyttöliittymä (Keary 2022)

Yhteenvetona voidaan todeta, että verkonvalvontaohjelmistojen käyttäjille on tarjolla lukuisia vaihtoehtoja, jotka toisaalta tarjoavat samojakin valvontamenetelmiä, mutta joiden käytettävyys ja muokattavuus eroavat toisistaan. Seuraavassa

taulukossa on vielä koonti tässä yhteydessä esiteltyjen verkonvalvontaohjelmistojen piirteistä (taulukko 1).

Taulukko 1. Verkonvalvontaohjelmistojen vertailu.

Nimi	Maksullinen	Graafinen käyttöliittymä	Teknisesti vaativa	Avoin lähdekoodi
Nagios XI	Kyllä, mutta Nagios Core ilmainen	Ei	Kyllä	Kyllä
Icinga	Ei	Kyllä	Kyllä	Kyllä
Network Performance Monitor	Kokeilujakson jälkeen	Kyllä	Ei	Ei
Zabbix	Ei	Kyllä	Kyllä	Kyllä

3 ZABBIXIN ASENNUS ASIAKASYRITYKSESSÄ

Tämän opinnäytetyön käytännön osuus suoritettiin asentamalla Zabbix-ympäristö sekä -verkonvalvonta noin kolmellekymmenelle asiakasyrityksen kriittiseksi määritellylle palvelimelle. Tämä määrittely perustui SLA-määrittelylle, eli palvelutasosopimuksessa korkeimmalle kriittisyystasolle määritellyille kohteille. Samalla tehty työ dokumentoitiin muistiinpanoja tekemällä.

3.1 Yritys

Tässä opinnäytetyössä käsiteltävän yrityksen nimi jätetään mainitsematta tietoturvan varmistamiseksi ja siitä puhuttaessa käytetään vain nimitystä ’yritys’ tai ’asiakasyritys’. Asiakasyritys-nimitys juontaa juurensa siihen, että yritys ostaa osan IT-palveluistaan IT-alan yritykseltä, jossa toimin osa-aikaisena työntekijänä Zabbixin asennusprosessin aikana.

Tietoturvan varmistamiseksi myös Zabbixin asennusvaiheita kuvatessa pyritään välttämään teknisten yksityiskohtien esittelyä, jotta esimerkiksi käyttöjärjestelmät ja versiot eivät paljastuisi ulkopuolisille. Samasta syystä työssä esitetyt kuvankaappaukset ovat Zabbixin sivuilta, eivät itse asennustyön dokumentaatiosta.

3.2 Yrityksen tarpeiden määrittely

Yrityksessä järjestettiin Zabbixin asennusprosessin aikana palaveri, jossa käytiin läpi yrityksen tarpeita tietoturvan suhteen sekä pohdittiin vaihtoehtoja verkonvalvonnan toteuttamiseksi. Palaveriin osallistuivat yrityksen IT-päällikkö sekä kaksi tietoturvasta vastaavaa työntekijää ja itse toimin keskustelun koollekutsujana sekä sihteerinä. Zabbixin asentaminen ja käyttöönotto oli kuitenkin tässä vaiheessa varsin selvää, sillä se on ollut yrityksen käytössä IT-palveluita tarjonneen yrityksen toimittamana. (Palaverimuistio 3.6.2022.)

Yksi keskeinen näkökulma yrityksen tarpeissa oli näkyvyys infran tilanteeseen. Yrityksessä on ensinnäkin käytössä useanlaista infraa: verkkolaitteita (kytkimet, palomuurit, reitittimet), palvelimia ja sovelluksia. Kuten edellä todettiin, on yrityksen

toiminnalla merkitystä huoltovarmuuden kannalta, joten infran kaatuminen vaikuttaisi niin huoltovarmuuteen kuin yrityksen itsensä toimintaan, mutta myös asiakkaiden ja yhteistyökumppaneiden toiminta saattaisi vaikeutua tai estyä. (Palaverimuistio 3.6.2022.)

Sen ohella, että yrityksen infran tulisi olla käyttäjien käytettävissä häiriöttä, tulisi poikkeamia pystyä havaitsemaan luotettavasti, ja näin varmistaa turvallisuus. Tähän liittyen tulisi vikatilanteet pystyä ennakoimaan, jotta niiltä ja niiden aiheuttamilta eritasoisilta seurauksilta vältyttäisiin niin hyvin kuin mahdollista. Edellä lueteltujen syiden lisäksi haluttaisiin pitää data omassa ympäristössä, mikä mahdollistaa sen, että ulkopuoliset eivät pääse käsiksi esimerkiksi IP-osoitteisiin. Samalla saavutettaisiin riippumattomuus yhteistyökumppanien toiminnasta, kun tietoturvaympäristön hallinta ja seuranta olisivat omien työntekijöiden vastuulla. (Palaverimuistio 3.6.2022.)

Toinen näkökulma yrityksen tarpeissa liittyi hälytyksiin. Niiden vastaanottaminen liittyy toisaalta myös infran tilanteen näkyvyyteen, mutta yritys koki tärkeäksi niiden toimivuuden, jotta tietoturva toteutuisi. Hälytysten vastaanottaminen tulisi olla mahdollista useita eri kanavia pitkin, ja lisäksi prioriteetin mukaan luokiteltuna. Esimerkiksi tulisi pystyä vastaanottamaan kiireelliset ilmoitukset vaikkapa työntekijän puhelimeen ja vähemmän kiireelliset työntekijän sähköpostiin. (Palaverimuistio 3.6.2022)

Vikailmoitusten vastaanottaminen kiireellisellä aikataululla sekä nopea reagointi auttavat huomaamaan ja korjaamaan viat jopa ennen kuin asiakkaat tai yhteistyökumppanit huomauttavat, mikä toisaalta ylläpitää huoltovarmuutta, mutta myös ehkäisee mainehaittoja. Toisaalta nopealla reagoinnilla on myös mahdollista minimoida vian kesto sekä estää ongelmien laajeneminen muiden osastojen tai järjestelmien pariin. (Palaverimuistio 3.6.2022.)

Kolmas esiin noussut näkökulma liittyi raportointiin, sillä yrityksen pitäisi pystyä tuottamaan raportteja useisiin eri yhteyksiin. Ensisijaisen tärkeää raportointi on yrityksen IT-osastolle tai järjestelmien ylläpitäjille, jotka vastaavat ylläpidosta ja

ongelmatilanteiden korjaamisesta. Toisekseen on syytä pystyä raportoimaan yrityksen toimintavalmiudesta johdolle, jotta tilannekuva on selkeä. Kolmanneksi myös loppukäyttäjille saattaa olla tarpeen laatia raportteja. Kaiken kaikkiaan raportoinnin tulisi toimia niin reaaliaikaisesti, esimerkiksi järjestelmien toimivuudesta kyseisellä hetkellä, kuin niiden historian suhteen. Esimerkki mahdollisuudesta raportoida infran tai sen osa-alueen historiaa on vaikkapa levytilan täyttymisen syiden selvittely tai vastaavasti pyrkimys ennakoida tarve levytilan lisäämiselle. (Palaverimuistio 3.6.2022.)

3.3 Miksi Zabbix?

Zabbix valikoitui yrityksen valinnaksi useiden käytännöllisten syiden pohjalta. Zabbix oli yrityksessä jo varsin tuttu, sillä sen työntekijöiltä löytyi pitkäaikaista kokemusta sen käytöstä, koska Zabbix oli jo pidempään tullut palveluna yhteistyökumppanilta. Kuitenkin Zabbix oli koettu hyödylliseksi ja lisäksi siihen liittyviä käyttöohjeita todettiin olleen helppo löytää, sillä sen nähtiin olevan laajasti käytössä. (Palaverimuistio 3.6.2022.)

Tarkemmin erittelemättä yrityksen IT-asiantuntija totesi, että ”huonojakin puolia (Zabbixista) löytyy”, mutta työntekijöiden yhteinen näkemys aiheesta oli, että Zabbix riittää täyttämään yrityksen tietoturvan vaatimukset. Yhtenä Zabbixin hyvänä puolena mainittiin agentin mahdollisuus kuunnella useampaa palvelinta, mikä mahdollistaa monipuolisemman käytön ja usean yhteistyökumppanin hyödyntämisen. Tässä tapauksessa esimerkiksi on mahdollisuus kohdistaa erilaiset ilmoitukset eri tahoille, vaikkapa niin että toinen taho vastaanottaa ilmoituksia tietokannoista ja toinen verkkolaitteista. (Palaverimuistio 3.6.2022.)

Tiivistettynä edellisessä alaluvussa tietoturvalle esitettyjä vaatimuksia olivat:

- näkyvyys infran tilanteeseen
- hälytysten toimivuus
- mahdollisuus selkeään raportointiin

Esitettyjen kriteerien kohdalta voidaan todeta Zabbixin vastaavan varsin hyvin vaatimuksia. Zabbixin tarjoamien monipuolisten valvontamenetelmien avulla voidaan saavuttaa näkyvyys moniin erilaisiin laitteisiin tai ympäristöihin niin Zabbix-agentin kuin eri protokollien avulla. Hälytykset puolestaan voidaan räätälöidä yrityksen valitsemille työntekijöille sopiviksi viestintäkanavan, ajoituksen ja vakavuuden suhteen. Zabbixin avulla on mahdollista laatia erilaisia raportteja esimerkiksi pylväsdiagrammin muodossa ja näissä voidaan esittää kulloinkin tarvittavaa dataa, esimerkiksi edellä mainittuun levytilan täyttymiseen tai havaittuihin tietoturvapoikkeamiin liittyen.

Zabbix tarjoaa verkkosivustollaan luettelemiensa esimerkkien pohjalta lukuisia ominaisuuksia erityyppiseen valvontaan sekä kattavat mahdollisuudet mukauttaa ohjelmistoa vastaamaan kulloinkin esille nousevia tarpeita. Toisaalta on toki hyvä säilyttää tietty varaus yhtiön itsensä esittämiä mainoshenkisiä listauksia kohtaan, mutta monipuolisia mahdollisuuksia Zabbix tarjoaa, sitä ei voitane kiistää. Oma kysymyksensä on myös, kuinka laajat taidot käyttäjän tulee hallita, jotta ohjelmiston käyttäminen sujuu. Kuitenkin, kuten yllä todettiin, ainakin asiakasyrityksessä oli koettu ohjeita löytyvän kattavasti Zabbixin laajan suosion vuoksi.

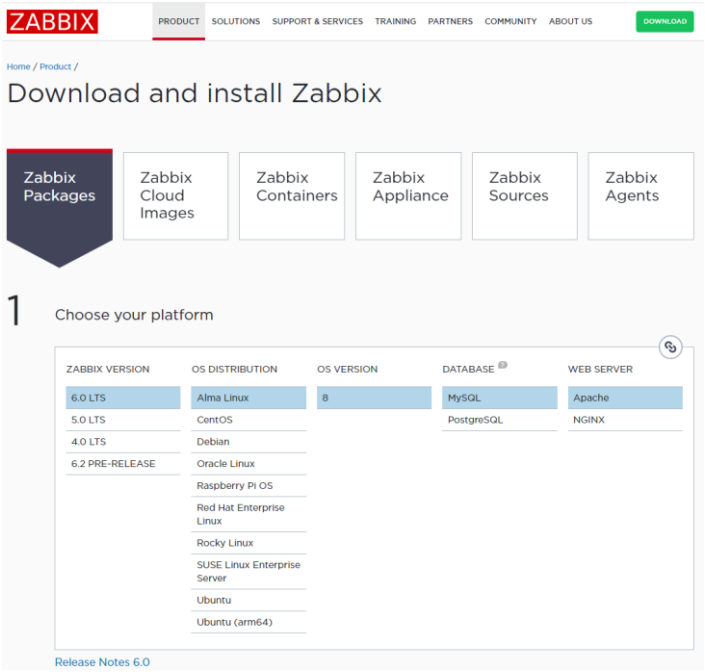
3.4 Asennus

Zabbixin asennustyöt aloitettiin helmikuussa 2022 asiakasyrityksen tiloissa ja saatettiin päätökseen elokuussa 2022. Olin jonkin verran perehtynyt Zabbixiin lukemalla sen manuaalia ja katsomalla videotutoriaaleja, mutta suurena apuna oli yrityksen IT-asiantuntija. Asennustyötä tehtiin 1–2 viikon välein noin tunnin sessioina, koska asennus hoidettiin muiden töiden ohessa. Zabbixin verkkosivuilla on varsin kattava manuaali, joka kattaa työn vaiheet pääpiirteissään, mutta asennustyön vaiheet kussakin käyttöjärjestelmässä vaativat usein googlettelua ja keskusteluforumien selaamista.

Verkkosivuillaan Zabbix mainostaa asentamisen onnistuvan minuuteissa, mikä toki on esimerkiksi käyttöliittymän osalta mahdollista (Zabbix, Features). Kuitenkin palvelimen ja tietokannan asentaminen vievät jonkin verran aikaa ja vaativat aihealueen ja tekniikoiden tuntemusta, asetusten säätämisestä puhumattakaan.

Lyhyesti kuvattuna Zabbix-asennus on kolmivaiheinen: ensin asennetaan Zabbix-palvelin UNIX-pohjaiselle käyttöjärjestelmälle, jonne asennetaan tämän jälkeen tietokanta sekä monitoroinnin hoitava Zabbix-agentti. Lopuksi asennetaan vielä web-pohjainen käyttöliittymä, jonka kautta määritellään asetukset sekä lisätään hostit ja itemit. Lisäksi on mahdollista vielä asentaa Zabbixin välityspalvelin eli *proxy*, jolla voidaan keventää palvelimen kuormitusta monitoroinnissa. (Zabbix, Introduction; Zabbix, Features.)

Ensimmäinen varsinainen vaihe Zabbixin asennustyössä on asennuspaketin lataaminen Zabbixin verkkosivuilta (kuva 9), mutta sitä ennen tulee olla selvillä mihin Zabbix varsinaisesti asennetaan. Vaihtoehtoisia asennustapoja ovat muun muassa *docker*, pilvitiedosto kuin git-repo, mutta tässä tapauksessa päädyttiin asentamaan Zabbixin asennuspaketti verkkosivun tarjoamia Linux-komentoja käyttämällä (Zabbix, Download). Verkkosivu päivittää ohjeistuksen käyttäjän valinnan mukaan sopivaksi haluttuun Zabbixin versioon, Linux-käyttöjärjestelmään, tietokantaan sekä web-palvelimeen.



Kuva 9. Zabbixin asennuspaketti (Zabbix, Features)

Asiakasyrityksen Zabbixin asentaminen käynnistettiin luomalla yritykselle uusi virtuaalipalvelin, jolle varattiin sopivaksi katsottu levytila ja valittiin käyttöjärjestel-

mäksi yksi Zabbixin tukemista vaihtoehdoista. Tälle palvelimelle asennettiin käyttöohjeen komennoilla repositorysta (tiedostolähteestä) Zabbix-palvelin, frontend (selainpuoli) ja agentti. Seuraavassa esimerkki manuaalin tarjoamista linux-komennoista, joilla edellä mainitut voidaan asentaa:

> "# rpm -Uvh https://repo.zabbix.com/zabbix/6.0/rhel/8/x86_64/zabbix-release-6.0-2.el8.noarch.rpm
> # dnf clean all
>
> # dnf install zabbix-server-mysql zabbix-web-mysql zabbix-apache-conf zabbix-sql-scripts zabbix-selinux-policy zabbix-agent". (Zabbix, Download.)

Palvelimen, frontendin ja agentin jälkeen asennetaan palvelimelle tietokanta, jolle luodaan samalla zabbix@localhost -niminen käyttäjätunnus. Zabbix-dokumentaatio on tehty MySQL:lle ja PostgreSQL:lle, mutta myös muille tietokannoille löytyy erillisiä ohjeistuksia. Kun hostille on tuotu komennolla tietokannan rakenne ja poistettu käytöstä binääriloki (binary log), ovat palvelin ja agentti valmiita käynnistettäviksi. (Zabbix, Download.)

Zabbixille on mahdollista asentaa myös välityspalvelin eli *proxy* samaan tapaan kuin asennettiin Zabbix-tietokanta. Proxy voidaan asentaa eri nimellä samalle palvelimelle, jolloin se käyttää eri tietokantaa. (Zabbix, Installation.)

3.5 Käyttöönotto ja käyttäjien lisääminen

Zabbixin käyttäminen ja hallinta tapahtuu asennuksen jälkeen hyvin pitkälle Zabbixin selainpohjaisen (frontend) sovelluksen kautta. Sovellukseen kirjaudutaan oletustunnuksilla, minkä jälkeen on mahdollista luoda omia käyttäjätunnuksia, jotka tallennetaan salattuina Zabbixin tietokantaan (Zabbix, Users and user groups).

Koska tieto kulkee Zabbixissa selaimen ja palvelimen välillä, on yhteys syytä suojata. Tässä tapauksessa luotiin SSL-sertifikaatti, jonka ansiosta tietoliikenne on salattu salausalgoritmeilla, eikä ulkopuolisilla ole mahdollisuutta ymmärtää tietoa (Digicert 2022). SSL-suojaus paitsi salaa näiden välisen liikenteen, auttaa sivuston

aitouden varmistamisessa (Kyberturvallisuuskeskus: Ohjeita viestinnän suojaamiseen, 9). Tässä tapauksessa luotiin Windowsin Certificate Managerilla sertifikaatti, joka konvertoitiin palvelimen käyttöjärjestelmään sopivaan tiedostomuotoon ja lisättiin palvelimelle.

Käyttäjiä luotaessa tule määrittää käyttäjän rooli, joita ovat Guest, User, Admin ja Super Admin (taulukko 2). Siinä missä Guest pääsee lähinnä tarkastelemaan raportteja, on Super Adminilla kaikki oikeudet. User- ja Admin-käyttäjän oikeudet muokata Host group:eja määritellään erikseen, mutta Admin pääsee oletuksena käsiksi Zabbixin asetuksiin. (Zabbix, Users and user groups.)

Taulukko 2. Käyttäjien roolit Zabbixissa (Zabbix, Permissions)

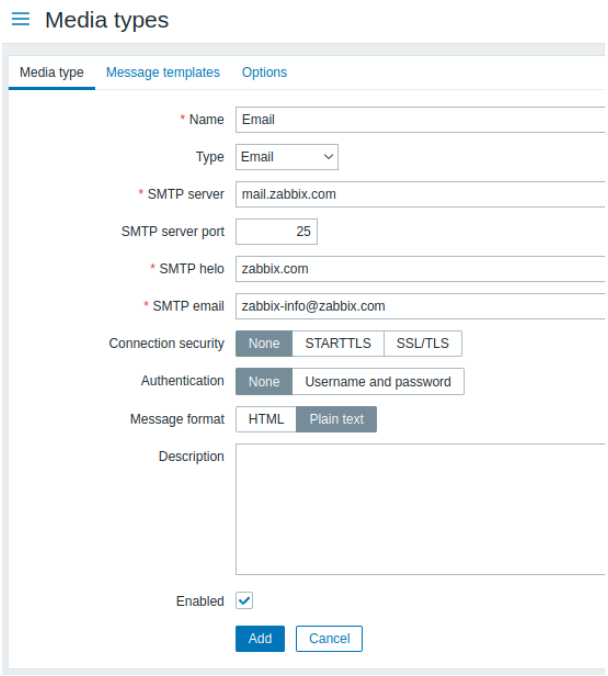
Käyttäjätyyppi	Kuvaus
Guest	Käyttäjällä on pääsy Monitoring-, Inventory- ja Reports-välilehdille, mutta ei muokkausoikeuksia.
User	Käyttäjällä on pääsy Monitoring-, Inventory- ja Reports-välilehdille. Kuitenkin tarkemmat pääsyoikeudet täytyy myöntää erikseen, kuten määritellä mitä hosteja ja templateja käyttäjä voi käsitellä.
Admin	Käyttäjällä on pääsy Monitoring-, Inventory-, Reports- ja Configuration-välilehdille. Oikeudet hostien ja templatejen muokkaamiseen määritellään erikseen.
Super Admin	Käyttäjällä on oletuksena pääsy kaikille välilehdille ja muokkaus- ja lukuoikeudet hosteille ja templateille. Pääsyjä ei voida rajata.

Käyttäjien luomisen yhteydessä lienee viisasta määrittää myös käytettävä tunnistautumistapa. Oletuksena Zabbix käyttää sen omaa Zabbix-tunnistautumista (authentication), mutta valittavissa ovat HTTP-, LDAP- ja SAML-protokollien mukaiset

tunnistautumistavat. Tunnistautumisen voi määrittää globaalisti tai ryhmätasolla, jolloin eri ryhmät voivat kirjautua eri tunnistautumismenetelmää käyttäen. Eri tunnistautumistapojen käyttöönotto vaatii jonkin verran vaivannäköä, mutta käyttöoikeuksien hallinta lienee helpompaa keskitettynä jo olemassa oleviin järjestelmiin. (Zabbix, Authentication.)

Tässä tapauksessa käyttöön otettiin yrityksessä jo käytössä oleva tunnistautumismenetelmä, jolloin samoilla käyttäjätunnuksilla kirjaudutaan yrityksen työasemille kuin Zabbixin käyttöliittymään. Tämä ei kuitenkaan tarkoita, että kaikki käyttäjät saisivat automaattisesti kirjautumisoikeuden Zabbixiin, vaan käyttäjätunnus tulee lisätä Zabbixiin Administration/Users-kohdasta valikosta.

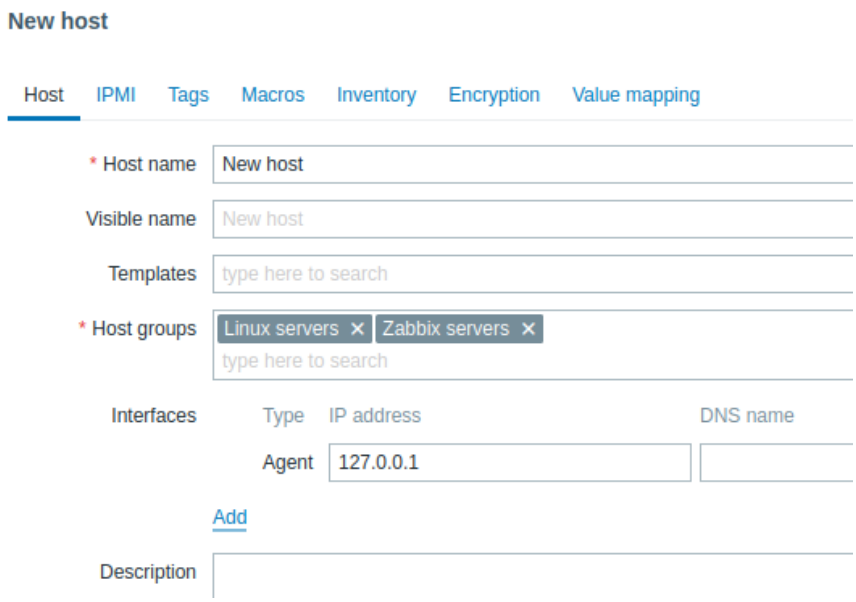
Käyttäjää luotaessa voidaan myös määrittää tapa, jolla Zabbix ilmoittaa havainnoistaan (kuva 10). Kun triggeri eli valvottavan kohteen ennalta määritelty rajaarvo saavutetaan, se kirjataan Zabbixiin. Ilmoituksia voi kertyä hyvin paljon, joten asetusten säätämällä voi rajata ilmoitukset vakaviin tai keskivakaviin ja eritellä ilmoitusten lähettämisajankohdan sekä median, jonka kautta ilmoitus lähetetään käyttäjälle.



Kuva 10. Ilmoitusten määrittäminen (Zabbix, Receiving Problem Notification)

3.6 Hostien lisääminen

Zabbixin valikosta kohdasta Configuration/Hosts/Create host saadaan lisättyä tarvittavat Hostit eli valvottavat laitteet Zabbixin käyttöliittymään (kuva 11). Asiakasyrityksen noin kolmestakymmenestä valvontaan lisättävästä kohteesta jokaiselle tuli kirjoittaa nimi ja valita sopivat Templatet ja Groupit sekä lisätä Interface-kohtaan IP-osoite ping-valvontaa tai Zabbix-agenttia varten.



Kuva 11. Hostin lisääminen (Zabbix, New Host)

Kaksi kolmasosaa valvontaan lisätyistä laitteista oli Windows-pohjaisia virtuaalipalvelimia. Lopuista palvelimista puolet oli Linux-pohjaisia virtuaalipalvelimia ja toinen puoli ping-valvontaan lisättäviä palvelimia. Hostia lisättäessä Windows- ja Linux-palvelinten ero näkyi siinä, että kullekin valittiin Group ja Template käyttöjärjestelmänsä mukaan. Eli esimerkiksi Windows-palvelimille valittiin Templateksi ’Windows’ ja agentiksi ’Windows by Zabbix Agent’. PIng-valvottaville kohteille puolestaan lisättiin Templateksi ’ICMP Ping’.

Ping-valvonnassa kyse on hostille lähetettävästä ICMP-protokollan mukaisesta IP-paketista, johon odotetaan vastausta. Kuitenkin palomuurit tai reitittimet saattavat joissakin tapauksissa estää ping-vastausten lähettämisen. (IBM 2022.)

3.7 Agentin asennus ja konfigurointi

Zabbix-agentin kautta valvottavien hostien käyttöönotto vaatii joitakin toimenpiteitä itse hostilla. Luonnollisesti agentti tulee asentaa valvottavan kohteen käyttöjärjestelmään, mutta myös määrittää agentin asennuskansiossa sijaitsevassa conf-tiedostossa valvonnan suorittavan Zabbix-palvelimen IP-osoite. (Zabbix, Agent.)

Tässä tapauksessa suurelle osalle palvelimista oli jo asennettu Zabbix-agentti palveluntarjoajan toimesta, jolloin riitti conf-tiedoston päivittäminen lisäämällä Zabbix-palvelimen IP-osoite. Windows-palvelinten päivittäminen kävi varsin kätevästi Windowsin graafisen käyttöliittymän kautta, mutta Linux-palvelimissa asentaminen tehtiin komentorivikomennoilla Zabbixin tarjoamaa repoa hyödyntäen:

```
# rpm -Uvh https://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm

# yum install zabbix-agent

# systemctl start zabbix-agent
```

(Zabbix, Agent; Zabbix, Agent Installation.)

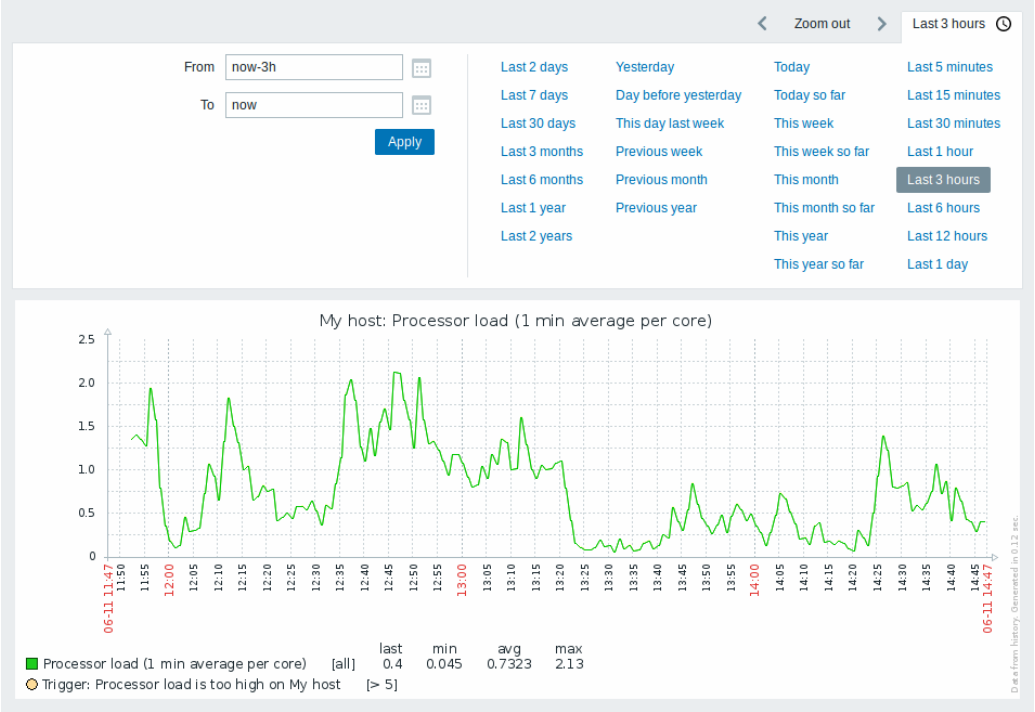
Asennuksen jälkeen agentti pitää vielä käynnistää, kuten yllä lainatun komennon viimeinen rivi tekee Linux-käyttöjärjestelmässä. Valmiiksi asennetut Zabbix-agentit tuli Windows-koneissa käynnistää uudelleen ”konffauksen” jälkeen Tehtävienhallinnan kautta.

3.8 Ilmoitukset ja kuvaajat

Kun Zabbix on asennettu ja ilmoitukset ja hälytykset saatu toimimaan, on mahdollista rakentaa erilaisia kuvaajia prosessien ja laitteiden toimintakyvystä (kuva 12). Tässä tapauksessa hostin prosessorin kuormitusesta on piirretty diagrammi viimeisen kolmen tunnin ajalta. (Zabbix, Custom graphs.)

Varsinkin jos valvottavia kohteita on runsaasti, voi visuaalinen esitystapa tarjota selkeän ratkaisun laitteiden tilan esittelemiseksi vaikkapa yrityksen johdolle. Tämän Zabbix-asennuksen yhteydessä asiakasyrityksellä ei toistaiseksi ollut tarvetta

graafisten kuvaajien laatimiselle, sillä suuremman mittakaavan valvonta tuli vielä toistaiseksi heidän yhteistyökumppaniltaan. (Zabbix, Custom graphs.)



Kuva 12. Esimerkki Zabbixin tarjoamista kuvaajista (Zabbix, Graphs).

Zabbixin käyttöliittymästä löytyy niin valmiita pohjia graafisille esityksille, kuin mahdollisuus muokata kuvaajia omiin tarpeisiin sopiviksi. Visuaalisen ilmeen ohella käyttäjä voi määrittää kuvaajien näyttämän datan triggereiden pohjalta ja muokata aikaväliä, jolta data esitellään. (Zabbix, Custom graphs.)

Zabbix tarjoaa käyttöön myös API:n eli rajapinnan. Tämän avulla voidaan paitsi muokata Zabbixin toimintaa, esimerkiksi lisäämällä item:eitä tai triggereitä, myös integroida Zabbix muihin ohjelmistoihin. Rajapinta käyttää JSON-RPC 2.0 protokollaa ja toimittaa näin ollen tiedot JSON-formaatissa. (Zabbix, API.) Rajapinnan avulla olisi mahdollista esimerkiksi rakentaa virtuaalinen ilmoitustaulu yrityksen valvonnassa olevista palveluista vaikkapa kahvihuoneeseen tai johdon tiloihin.

4 JOHTOPÄÄTÖKSET JA POHDINTA

Työ lähti liikkeelle kahdesta hyvin käytännönläheisestä tarpeesta: asiakasyritykseen oli tarpeen asentaa Zabbix-ohjelmisto omaan ympäristöön sekä itselläni oli tarve saada opinnäytetyö tehtyä. Itse asennustyölle aikataulun raamit asetti se tosiasia, että toimeksiantoni asiakasyrityksessä oli sovittu päättymään elokuun 2022 lopussa.

Asennustyö saatiin tehtyä ajallaan, vaikka pienelle loppukirille olikin aihetta juhannuksen alla, jotta työ saataisiin melko valmiiksi ennen kesälomakautta. Muutamien palvelinten konfigurointi suoritettiin vielä elokuussa, mutta aikataulu saavutettiin muutamia viikkoja etuajassa. Järjestelmä saatiin siis toimimaan aikataulun puitteissa SLA-palvelinten osalta, mutta loppujen palvelinten lisääminen valvontaan jäi yrityksen omiin käsiin siirtyessäni muihin tehtäviin.

Tämä opinnäytetyö voi toivon mukaan tarjota tietoa Zabbix-ohjelmistosta kiinnostuneille tai sen kanssa työskenteleville. Ohjelmiston käyttöönottoa mahdollisesti harkitseva voi työhön tutustumalla saada yleiskuvan asennustyön vaiheista ja vaatimuksista. Zabbixia käyttävässä yrityksessä työskentelevä henkilö, vaikkapa tämän opinnäytetyön asiakasyrityksen esimies, voi saada kattavamman kuvan Zabbixin tarjoamista mahdollisuuksista. Vaikka Zabbix tarjoaa nettisivuillaan monipuolisen dokumentaation, voi jäsennellyn suomenkielisen esityksen lukeminen tarjota helpommin lähestyttävän tavan perehtyä aiheeseen.

Tutkittua aihetta olisi ollut mahdollista lähestyä vielä teknisemmin kuin tässä opinnäytetyössä on tehty, mutta tässä yhteydessä näen tarpeelliseksi muodostaa kattavan kokonaiskuvan, joka on mahdollista ymmärtää kohtuullisten tietoturvan perustietojen pohjalta. Zabbix opinnäytetyön aiheena tarjoaa mahdollisuuksia syventää tarkastelua niin lähdekoodin, tietoverkkojen kuin protokollien suhteen. Myös erilaisten laitteiden tai ohjelmistojen lisääminen palvelinten ohella valvontaan laajentaisi tutkimuksen näkökulmaa.

Verkonvalvonnan merkittävyys aiheena ei ole laskemassa ainakaan helmikuun 2023 Kybersään pohjalta: niin verkkohuijaukset kuin haittaohjelmat ovat Kyberturvakeskuksen mukaan huolestuttavalla tasolla ja kybervakoilu jopa huolestuttavalla tasolla (Kyberturvallisuuskeskus 2023, Kybersää). Verkonvalvonnalle on siis tarvetta edelleen, kunhan osaajia sen käyttämiseen ja kehittämiseen on löydettävissä.

LÄHTEET

Candolin, C. 2022. Varautuminen sodan sumun keskellä. Digiturvaviikon webinaariluento 13.10. Viitattu 14.10. 2022. www.mediaserver.fi/live/digiturvaviikko

Comparitech. 2023. The Ultimate Guide To TCP/IP. Viitattu 16.3.2023. www.comparitech.com/net-admin/ultimate-guide-tcp-ip/

Digicert. 2022. The Ultimate Guide. What is SSL, TLS and HTTPS. Viitattu 13.12. 2022. www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https

DevOps School. 2022. What is Zabbix and use of it? Viitattu 18.11. 2022. www.devopsschool.com/blog/what-is-zabbix-and-use-of-it/

DNS Stuff. 2022. Ultimate Guide to Network Monitoring. Viitattu 30.11.2022. https://www.dnsstuff.com/network-monitoring#basics-network-monitoring

Huawei. What Is SNMP? Viitattu 30.3. 2023. www.support.huawei.com/enterprise/en/doc/EDOC1100086963

IBM. 2022. Internet Control Message Protocol (ICMP) and other layer 3 protocols. Networking on z/OS. Viitattu 13.12. 2022. www.ibm.com/docs/en/zos-basic-skills?topic=nll-internet-control-message-protocol-icmp-other-layer-protocols

Jethva, H. 2022. Network Device Monitoring Guide. Network Admin Tools. Viitattu 30.11.2022. www.netadmintools.com/network-device-monitoring-guide/#wbounce-modal

Jones IT. Designing A Computer Network For Your Business: A Step-By-Step Guide. Viitattu 30.3. 2023. www.itjones.com/blogs/2022/1/15/designing-a-computer-network-for-your-business-a-step-by-step-guide

Keary, T. 2022. 13 Best Network Monitoring Tools & Software of 2022. Comparitech. Viitattu 9.12. 2022. www.comparitech.com/net-admin/network-monitoring-tools/

Kyberturvallisuuskeskuskus. 2023. Kybersää. Helmikuu 2023. Viitattu 30.3. 2023. www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202023

Kyberturvallisuuskeskus. 2022. Kyberympäristön uhkataso noussut. Aktiviteetti Suomeakin kohtaan lisääntynyt. Viitattu 14.10. 2022. www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

Kyberturvallisuuskeskus. 2022. Ohjeita viestinnän suojaamiseen. Viitattu 7.9.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_viestinnan_suojaamiseen.pdf

Nagios. 2022. Nagioksen verkkosivut. Viitattu 9.12. 2022. www.nagios.org/

Sbcode. Administration scripts. Viitattu 16.3. 2023. www.sbcode.net/zabbix/administration-scripts/

Techtarget. 2022. What is TCP/IP and how does it work? Viitattu 30.11.2022.

Zabbix. 2022. About. Zabbix-ohjelmiston verkkosivut. Viitattu 13.6.2022. www.zabbix.com/about.

Zabbix. 2022. Authentication. Zabbix-ohjelmiston verkkosivut. Viitattu 13.6.2022. www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/administration/authentication.

Zabbix. 2022. Agent. Zabbix-ohjelmiston käyttöohje. Viitattu 16.9.2022. www.zabbix.com/documentation/current/en/manual/concepts/agent#agent-on-windows-systems

Zabbix. 2022. Agent Installation. Zabbix-ohjelmiston käyttöohje. Viitattu 16.9.2022. www.zabbix.com/documentation/3.0/en/manual/installation/install_from_packages/agent_installation

Zabbix. 2022. Custom graphs. Zabbix-ohjelmiston käyttöohje. Viitattu 21.9.2022. https://www.zabbix.com/documentation/current/en/manual/config/visualization/graphs/custom

Zabbix. 2022. Definitions. Zabbix-ohjelmiston käyttöohje. Viitattu 14.6.2022. www.zabbix.com/documentation/curren/en/manual/definitions.

Zabbix. 2022. Download. Zabbix-ohjelmiston verkkosivut. Viitattu 28.6.2022. www.zabbix.com/download.

Zabbix. 2022. Features. Zabbix-ohjelmiston verkkosivut. Viitattu 13.6.2022. www.zabbix.com/features.

Zabbix. 2022. Graphs. Zabbix-ohjelmiston käyttöohje. Viitattu 21.10. 2022. www.zabbix.com/documentation/current/en/manual/config/visualization/graphs/simple

Zabbix. 2022. New Host. Zabbix-ohjelmiston käyttöohje. Viitattu 21.10. 2022. www.zabbix.com/documentation/current/en/manual/quickstart/host

Zabbix. 2022. Receing Problem Notification. Zabbix-ohjelmiston käyttöohje. Viitattu 13.12. 2022. www.zabbix.com/documentation/6.0/en/manual/quickstart/notification

Zabbix. 2022. Installation. Installation from packages. Red Hat Enterprise Linux/Centos. Zabbix-ohjelmiston käyttöohje. Viitattu 7.9. 2022. www.zabbix.com/documentation/6.0/en/manual/installation/install_from_packages/rhel_centos#proxy-installation

Zabbix. 2022. Introduction. About. Zabbix-ohjelmiston käyttöohje. Viitattu 14.6.2022. www.zabbix.com/documentation/curren/en/manual/introduction/about.

Zabbix. 2022. New trigger. Zabbix-ohjelmiston käyttöohje. Viitattu 21.10. 2022. www.zabbix.com/documentation/current/en/manual/quickstart/trigger

Zabbix. 2022. Users and user groups. Zabbix-ohjelmiston käyttöohje. Viitattu 7.9. 2022. www.zabbix.com/documentation/6.0/en/manual/config/users_and_usergroups

Zabbix. 2022. Authentication. Zabbix-ohjelmiston käyttöohje. Viitattu 14.6.2022. www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/administration/authentication

Zabbix. 2022. User groups. Zabbix-ohjelmiston käyttöohje. Viitattu 14.6.2022. www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/administration/user_groups

Zabbix. 2022. User roles. Zabbix-ohjelmiston käyttöohje. Viitattu 14.6.2022. www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/administration/user_roles