jamk

Verkonvalvontaohjelmistojen testaus ja vertailu

Jami Mäkiranta

Opinnäytetyö, AMK
Toukokuu 2022
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Mäkiranta, Jami

Verkonvalvontaohjelmistojen testaus ja vertailu

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2022, 56 sivua.

Tietojenkäsittely ja tietoliikenne. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tarkoituksena oli testata ja verrata ilmaiseksi saatavilla olevien verkonvalvontaohjelmien ominaisuuksia ja toimintaa. Erillistä toimeksiantajaa ei ollut, vaan aihe oli itse keksitty. Tavoitteena oli testien ja vertailun pohjalta selvittää valittujen verkonvalvontasovelluksien soveltuvuutta yritysverkon valvontaan. Sovelluksiksi valittiin Zabbix ja Nagios Core.

Testaukset suoritettiin virtuaalisessa ympäristössä, joka oli rakennettu virtualboxiin. Ympäristö koostui itse valvontapalvelimista, kahdesta valvottavasta palvelimesta, jotka olivat molemmat ubuntuja, sekä pfsensestä eli palomuurista. Laitteille ajettiin mahdollisimman realistisia testejä liittyen sellaisiin tilanteisiin, joita myös oikeassa yrityksen tuotantoverkossa voisi tapahtua. Testejä olivat laitteiden resurssien käytön valvonta eli prosessorin käyttö ja levytilan käyttö, palvelun tilan valvonta, eli onko jokin palvelu käynnissä vai ei, sekä laitteiden saatavuus eli ovatko laitteet tavoitettavissa verkon yli.

Testeissä seurattiin luoko valvontaohjelmistot hälytyksiä vikatilanteista. Molemmat sovellukset suoriutuivat jokaisesta testistä odotetulla tavalla ja loivat hälytyksiä, kuten haluttiin.

Ominaisuuksien vertailu perustui lähinnä Internetistä saatavilla olevaan tietoon. Vertailussa selkein ero näiden kahden sovelluksen välille muodostui niiden käyttöliittymästä, mikä kävi ilmi sovelluksien käytön ohessa testejä tehdessä. Zabbixin web-käyttöliittymä oli selkeämpi, antoi enemmän tietoa ja sitä pystyi muokkaamaan reilusti. Nagioksen käyttöliittymä oli hyvin yksinkertainen ja se ei ollut juuri muokattavissa. Toinen selkeä ero liittyi myös sovellusten käyttöön ja se oli ero näiden konfiguroinnissa. Zabbixin konfigurointi tapahtui suoraan web-käyttöliittymästä ja Nagios Coren konfigurointi taas komentoriviltä tekstimuotoisia konfiguraatiotiedostoja muokaten.

Tuloksista voi olla hyötyä henkilölle tai taholle, jotka etsivät tietoa verkonvalvontasovelluksista ja etenkin jos juuri nämä kyseiset sovellukset ovat harkinnassa ja valintaan vaikuttaa merkittävästi käytettävyys. Tuloksista saadaan myös selville, että kumpikin sovellus soveltuu yrityksen verkonvalvontaan.

Avainsanat (asiasanat)

Verkonvalvonta, Zabbix, Nagios Core

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Mäkiranta, Jami

Comparison and testing of network monitoring software

Jyväskylä: JAMK University of Applied Sciences, May 2022, 56 pages.

Information and Communications. Degree Programme in Information and Communication Technology. Bachelor's thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The purpose of this research was to test and compare features of free network monitoring software. There was no specific client for this, the subject was self invented. The objective, based on the tests and comparison, was to determine if free software is suitable for monitoring a real life enterprise network. The software was chosen to be Zabbix and Nagios Core.

Tests were done in a virtual network built in virtualbox. The environment consisted of the monitoring servers, two monitored servers that were both ubuntus, and a pfsense firewall. The devices were put through realistic tests, situations that could have happened in a real production network of an enterprise. Tests consisted of resource monitoring (processor and disk usage), monitoring the status of a service meaning checking whether the service is up or not and monitoring the reachability of the network devices.

While doing the tests on the monitored devices the monitoring servers were expected to raise alarms. Both servers performed as expected creating alarms when necessary.

The comparison of features was mostly done based on information available on the internet. The most obvious difference between these two was the user interface. That was noticed while using the software and running tests. Zabbix's user interface was clearer, gave more information and it was modifiable. Respectively Nagios's user interface was simplistic and less informative and it couldn't be modified. Another clear difference was also related to operating these and it was the way they were configured. Zabbix's configuration changes could be done on the web interface while Nagios configuration happened only on the command shell modifying text based configuration files.

The results can be of use to someone looking for a suitable monitoring software to them, especially if these two are in consideration and good usability is one of the desired features. The results also point out that both of these are well suited for monitoring an enterprise network.

Keywords/tags (subjects)

Network monitoring, Zabbix, Nagios Core

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

Opinnäytetyön tarkoituksena oli testata ja vertailla kahden ilmaiseksi saatavilla olevan verkonvalvontaohjelmiston ominaisuuksia. Aiheenvalinta sai inspiraation omasta kiinnostuksesta aihepiiriä kohtaan. Aihe on itse keksitty.

Työtä varten pystytettiin pienimuotoinen virtuaaliympäristö, joka koostui muutamasta kohde palvelimesta ja verkkolaitteesta, sekä itse hallintapalvelimista, joille valvontaohjelmistot asennettiin. Testauksia varten suunniteltiin muutama eri skenaario, joilla mitattiin ohjelmien suoriutumista verkonvalvonnallisista tilanteista. Ohjelmien suoriutumista testeistä vertailtiin keskenään ja lisäksi vertailuun sisältyi myös sovelluksien muita ominaisuuksia, jotka eivät päässeet testeihin mukaan.

Valitut sovellukset olivat Zabbix ja Nagios Core. Molemmat ovat täysin ilmaisia, mikä oli tärkein valintaperuste. Lisäki molemmat lukeutuvat yleisimmin käytettyihin ilmaiseksi saatavilla oleviin sovelluksiin, mikä oli toisena tärkeänä valintaperusteena. Tarkoituksena olikin testata ja verrata relevantteja sovelluksia, jolloin työstä voi olla lukijalle apua verkonvalvontasovelluksen valitsemisessa.

2 Tutkimusasetelma

Tutkimusongelmana oli ilmaisten verkonvalvontasovellusten valvontaominaisuuksien kattavuus ja soveltuvuus oikean tietoverkon valvontaan. Tarkoituksena oli testata ja vertailla niiden ominaisuuksia. Testien ja vertailun kohteeksi rajautui lopulta perus toiminnot, kuten laitteiden resurssien, saatavuuden ja palveluiden tilan valvonta.

Työssä käytetty tutkimusmenetelmä on laadullinen tutkimus. Tutkimuskysymyksiksi valikoitui seuraavat kysymykset. Kuinka hyvin ilmaisohjelmat soveltuvat verkonvalvontaan? Kuinka kaksi suosittua valvontaohjelmaa vertautuvat toisiinsa ominaisuuksiltaan?

3 Verkonvalvonta yleisesti

Tietoverkko koostuu erilaisista verkkolaitteista, kuten kytkimistä, reitittimistä, tukiasemista, palomuureista ja palvelimista, joita on voi olla tarpeen valvoa. Verkonvalvonta on yksi olennainen ja tärkeä osa verkonhallintaa. Verkonvalvonnan tarkoituksena on tunnistaa verkosta ja sen laitteista

vikoja ja mahdollisia ongelmia. Yleisimpiin ongelmiin kuuluu laitteiden ylikuormittuminen, kaatuminen ja jumiutuminen. Valvonnan tehtävänä on havaita nämä ja luoda niistä hälytyksiä, jotta ongelmat huomataan ajoissa ja niihin voidaan reagoida.

Korkealla tasolla ajateltuna valvonta on melko yksinkertaista. Verkosta täytyy valita laitteet, joita halutaan valvoa. Valvonta kohdistuu usein verkon toiminnan kannalta kriittisiin laitteisiin, kuten runkoreitittimiin ja -kytkimiin, palomuureihin ja tärkeisiin palvelimiin. Seuraavaksi mietitään mitä näiltä laitteilta valvotaan. Reitittimiltä ja kytkimiltä valvotaan yleensä porttien tilanmuutoksia, reititykseen liittyviä muutoksia, sekä resurssien käyttöä. Palvelimilta valvotaan resurssien käyttöä ja palvelujen tilaa, eli esim. web-palvelimen kannalta tärkeää on web-sisältöä tuottavan sovelluksen käynnissä pysyminen.

Valvontaan määritetään asetuksia, kuten valvontakyselyiden tiheys riippuen kohdelaitteen kriittisyydestä. Tärkeimpien laitteiden tilaa on syytä tarkistaa useammin, kuin ei niin tärkeiden. Muita määrityksiä ovat esim. viitearvot, joiden sisällä vaikkapa palvelimen levynkäyttö tulee pysyä ennen kuin siitä nostetaan hälytys. (Network monitoring definition n.d.)

3.1 Agentillinen ja agentiton valvonta

Verkkolaitteiden valvonta on joko agentillista tai agentitonta. Agentillisesta valvonnasta puhutaan silloin, kun valvottavalle laitteelle asennetaan erikseen ohjelma, eli valvonta-agentti, laitteen valvontaa varten. Valvonta-agentti kerää laitteesta tietoa ja lähettää sitä valvontapalvelimelle. Agentiton valvonta vastaavasti tarkoittaa sitä, että erillistä ohjelmaa ei tarvita vaan valvonta tapahtuu eri protokollia, kuten esim. SNMP:tä, Netflowta tai SSH:ta hyödyntäen. (Karimi 2020.) SNMP ja Netflow ovat esitelty luvussa 4. SSH eli Secure Shell on protokolla, jolla voidaan ottaa etäyhteys laitteesta toiseen ja esim. välittää tiedostoja näiden välillä tai hallita toista laitetta (What is SSH and how do I use it? N.d.).

4 Yleisimmät teknologiat ja protokollat

Valvontaan liittyy useita eri teknologioita ja protokollia. Tässä luvussa esitellään ja käydään läpi näistä yleisimpiä ja olennaisimpia.

4.1 ICMP

Internet control message protocol (ICMP) on OSI-mallin verkkokerrokselle sijoittuva protokolla, jonka päätarkoituksena on testata verkkoyhteyden toimivuutta kahden laitteen välillä. ICMP ei käytä kuljetuskerroksen protokollia TCP:tä tai UDP:ta, vaan se toimii itsenäisenä yhteydettömänä protokollana, joka ei myöskään käytä portteja. ICMP:llä saadaan selville onko laitteiden välillä toimiva yhteys vai ei. Jos yhteydessä on jokin ongelma, ICMP:n tehtävä on kertoa siitä lähettävälle laitteelle.

ICMP:n toinen käyttötarkoitus on diagnosoida mahdollinen ongelma laitteiden välillä. Yleisessä käytössä olevat teminaalisovellukset ping ja traceroute hyödyntävät ICMP:tä.

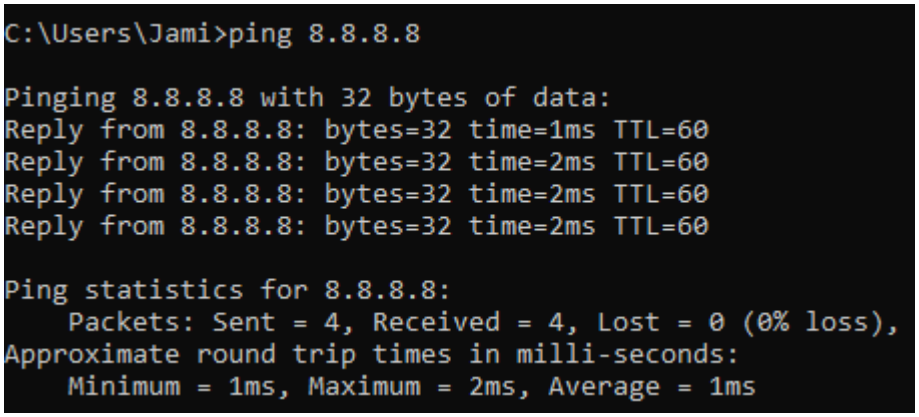
Traceroutella saadaan selville reitti, jota pitkin data kulkee verkossa testattavien laitteiden välillä. Reitillä tarkoitetaan fyysisiä laitteita, joiden kautta liikenne kulkee matkalla päämääräänsä. Traceroute tulosteessa jokainen rivi on hyppy, eli fyysinen laite verkossa. Traceroute kertoo myös kuinka kauan kullakin hypyllä kesti vastata. Alla olevassa kuviossa 1 esimerkkituloste traceroute komennosta Googlen osoitteeseen 8.8.8.8.

```
C:\Users\Jami>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  dna.WLAN [192.168.1.1]
  2     2 ms     1 ms     1 ms  159-255-240-2.bb.dnainternet.fi [159.255.240.2]
  3     1 ms     1 ms     1 ms  hel7-sr22.net.dnaip.fi [62.78.117.15]
  4     2 ms     1 ms     1 ms  142.250.169.179
  5     3 ms     2 ms     2 ms  142.250.169.178
  6     2 ms     2 ms     1 ms  142.251.52.195
  7     3 ms     3 ms     2 ms  142.250.229.83
  8     2 ms     2 ms     2 ms  dns.google [8.8.8.8]

Trace complete.
```

Kuvio 1. Esimerkki traceroute-komennosta

Ping sovellus on traceroutesta yksinkertaisempi versio. Sillä voidaan nopeasti ja helposti testata yhteydellisyys kahden laitteen välillä. Pingillä selviää myös aika, eli latenssi, joka kohteella kestää vastata sekä mahdollinen pakettihävikki. Latenssi ja pakettihävikki kertovat yhteyden laadusta,

mitä korkeampia ne ovat, sitä huonompi laatuinen yhteys on. Pakettihävikkiä ei tulisi olla yhtään, mutta latenssi nousee melkein aina fyysisen etäisyyden kasvaessa. Kuviossa 2 esimerkkituloste pingistä osoitteeseen 8.8.8.8. (What is the Internet Control Message Protocol (ICMP)? N.d.)



Kuvio 2. Esimerkki ping-komennosta

4.2 SNMP

Simple network management protocol (SNMP) on verkkojen hallintaan ja valvontaan suunniteltu protokolla, jonka toiminta pohjautuu agentti-manager malliin. SNMP toiminnallisuus on sisäänrakennettu useimpiin verkkolaitteisiin tehden siitä universaalin ja laajalti käytetyn protokollan.

SNMP:tä tukevilla laitteilla on management information base (MIB), joka on hierarkinen tietorakenne asioista ja tiedoista, joita kyseiseltä laitteelta voidaan kerätä ja joita voidaan konfiguroida SNMP:n avulla. MIB koostuu OID:ista (object identifyer), jotka tarkentavat mistä ominaisuudesta hierarkiassa on kyse. MIB:ejä on olemassa IETF:n ja ISO:n standardisoimissa muodoissa, mutta myös laitevalmistajien, kuten Cisco ja ohjelmistotuottajien, kuten Microsoft ja Oracle omissa muodoissa. (What is Simple Network Management Protocol (SNMP)? N.d.)

SNMP:stä on olemassa kolme eri versiota: SNMPv1, SNMPv2 ja SNMPv3. Näistä yleisimmin käytetty on SNMPv2. Versiossa kaksi on paranneltu virheen käsittelyä ja komentoja edelliseen verrattuna. Kolmannessa versiossa muutokset kohdistuvat lähinnä paranneltuun turvallisuuteen. (What is SNMPv1, SNMPv2c, and SNMPv3? N.d.)

Toiminta

SNMP:n toimintaperiaate on, että manager eli valvontapalvelin, lähettää kyselyn laitteelle, johon laitteella toimiva SNMP agentti vastaa. Valvottava laite voi myös lähettää itsenäisesti tiedon jostakin merkittävästä tapahtumasta SNMP managerille. SNMP operaatiot kuvattuna ja selitettynä alla:

- Get request: manager pyytää muuttujan tai muuttujaryhmän arvot agentilta
- Set request: manager muuttaa konfiguraatiota agentilla tai ajaa muun komennon
- Getnext request: manager pyytää MIB hierarkiassa seuraavien muuttujien arvot
- Getbulk request: manager ajaa useita getnext requestejä pyytääkseen paljon tietoa kerralla
- SNMP response: agentin vastaus sille tulleseen SNMP kyselyyn
- SNMP trap: agentin lähettämä tieto jostakin merkittävästä tapahtumasta laitteella ilman erillistä pyyntöä
- SNMP inform: managerin vahvistus SNMP trapin vastaanottamisesta

(What is Simple Network Management Protocol (SNMP)? N.d.)

4.3 Netflow

Netflow on alunperin Ciscon laitteilla julkaistu teknologia verkkoliikenteen seurantaan ja valvontaan. Nykyään sitä voidaan käyttää myös muiden valmistajien laitteilla. Netflow:n avulla voidaan analysoida ja visualisoida datavirtoja verkossa. Tämä mahdollistaa verkkoliikenteen valvonnan käyttäjä-sovellus tasolla. Verkkoliikenteen analysoinnin pohjalta voidaan myös tehdä suunnittelua, tunnistaa mahdollisia pullonkauloja ja täten tarvittaessa lisätä laitteita tai ottaa laitteilla käyttöön lisää resursseja, kuten portteja. (Clavel 2018.)

4.4 Syslog

Syslog on standardisoitu lokitus protokolla, joka toimii todella laajalla kirjolla erilaisia laitteita ja sovelluksia. Se mahdollistaa tekstipohjaisten lokiviestien lähetyksen keskitetylle palvelimelle.

Syslog viesteissä on kentät vakavuudelle (engl. severity) ja toiminnolle (engl. facility). Kenttien tarkoituksena on helpottaa ja selkeyttää viestin käsittelyä. Koska syslog viestit ovat vapaamuotoisia, ilman edellä mainittuja kenttiä viestien käsittely olisi todella paljon hankalampaa.

Vakavuuskenttä

Vakavuus ilmoitetaan numeroilla nollasta seitsemään. Nolla koodi on vakavin ja seitsemän vastaavasti vähiten vakava. Koodit selitetty alla olevassa taulukossa 1.

Taulukko 1. Syslog-viestin vakavuuskenttä

Numerokoodi	**Vakavuus**	**Tarkoitus**
0	Emergency	Järjestelmä on käyttökelvoton
1	Alert	Vaatii välitöntä toimenpidettä
2	Critical	Kriittinen tila
3	Error	Virhetilanne
4	Warning	Varoitus
5	Notice	Normaali, mutta merkittävä tila
6	Informational	Informatiivinen viesti
7	Debug	Debug viesti

Emergency tason viestit ovat niin vakavia, että niitä ei yleensä näe valvontapalvelimella asti. Järjestelmä on siis niin huonossa tilassa silloin, että ei kykene viestejä lähettämään. Debug tason viestit taas eivät ole siinä mielessä kriittisiä, että niitä edes haluttaisiin lähettää minnekään. Yleisesti lokitustaso asetetaan tasolle 5 tai 6, eli kaikki kyseiseen tason viestit ja sitä vakavammat lähetetään keskitetylle palvelimelle. Kaikki syslogit tallentuvat myös itse paikalliselle laitteelle.

Toimintokenttä

Toimintokentällä ei nykypäivänä ole enää samaa käyttöarvoa kuin ennen. Ennen syslog-palvelimet järjestelivät syslog-viestejä toimintokentän koodin perusteella, kun taas nykyään kaikki viestit ohjataan yleiseen tietokantaan ja toimintokentän arvo toimii vain yhtenä mahdollisena hakukriteerinä. Toimintokentän arvo on siis lähinnä entisajan jäänne ja sen arvolla viitataan johonkin tiettyyn järjestelmään tai toimintoon. Liitteessä 1 on selitetty toimintokenttien eri arvot ja niiden tarkoitukset.

Toiminto- ja vakavuuskoodit ovat aina syslog-viestin alussa kulmasulkeiden sisällä. Esimerkiksi “<115>” tarkoittaa FTP daemon viestiä vakavuudella 5.

Laitteet voivat lähettää syslog-viestejä palvelimelle käyttäen joko TCP- tai UDP-protokollaa. Suositeltavaa olisi käyttää TCP:tä johtuen sen paremmasta luotettavuudesta, mutta UDP on silti yleisimmin käytetty. (Dooley 2020.)

5 Valitut ohjelmistot

Tässä luvussa esitellään valitut verkonvalvontasovellukset.

5.1 Zabbix

Zabbix on yritystason verkonvalvontaan suunniteltu ilmainen avoimen lähdekoodin sovellus. Zabbixilla voidaan valvoa palvelimia, verkkolaitteita, pilvipalveluita ja muita IT komponentteja. Sen perus ominaisuuksiin lukeutuu:

- visualisointi
- ilmoitukset (esim. sähköpostitse ja sms)
- helppo käyttöönotto
- metriikoiden keräys
- ongelmien havaitseminen
- konfigurointi web-käyttöliittymästä
- Zabbix-agent
- laitteiden valvonta hyödyntäen yleisimpiä protokollia

(Kumar 2022.)

5.2 Nagios Core

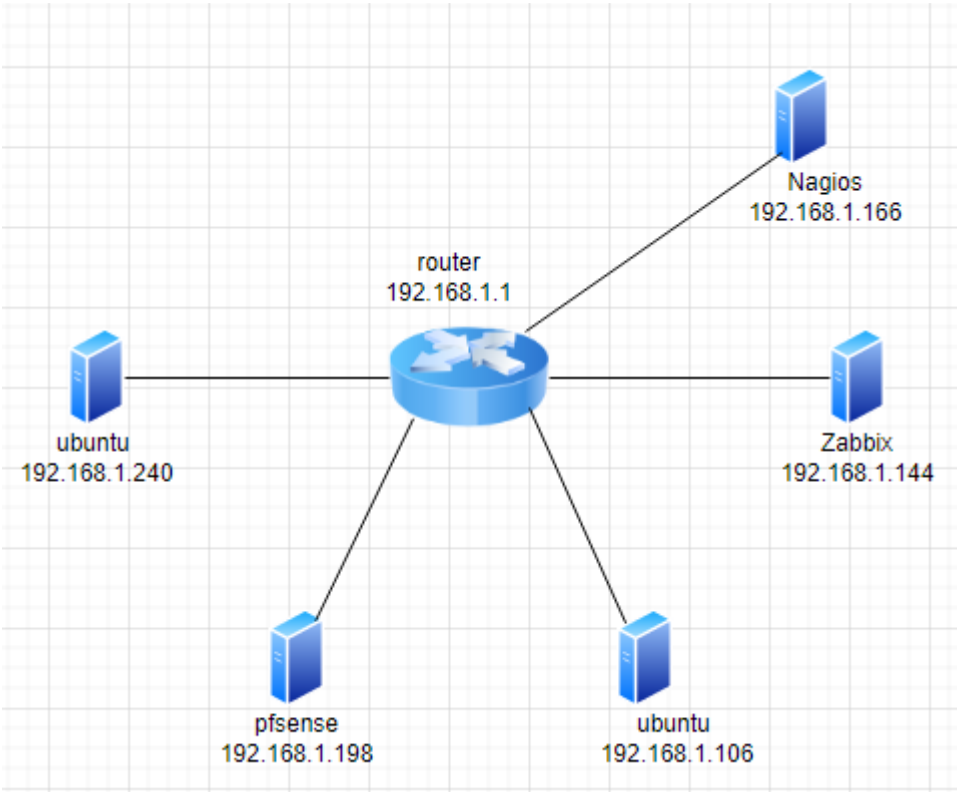
Nagios Core on myös avoimeen lähdekoodiin pohjautuva valvontasovellus. Se on suunniteltu verkkolaitteiden ja palvelimien valvontaan. Nagios Coren ominaisuuksia:

- web-käyttöliittymä (ei voi käyttää konfigurointiin)
- ilmoitukset (esim. sähköpostitse)
- pluginit eli valvonta-agentti
- laitteiden valvonta hyödyntäen yleisimpiä protokollia

(What Is Nagios Core? N.d.)

6 Testiympäristö

Testiympäristö toteutettiin virtuaalisilla laitteilla Virtualboxissa. Kokoonpanoon kuuluu kaksi Ubuntu palvelinta, pfsense palomuuri sekä zabbix ja nagios koneet, jotka molemmat pyörivät Ubuntun päällä. Liikenne virtuaalilaitteilta tulee sillattuna kotireitittimelle, joten ne ovat ikään kuin kytkettynä siihen ja saavat reitittimeltä IP-osoitteet. Topologia ja IP-osoitteet näkyvät kuviossa 3.



Kuvio 3. Testiympäristön topologia

7 Toteutus

7.1 Zabbixin asennus

Zabbix asennettiin Ubuntu koneelle. Tässä kohdassa käydään läpi asennuksen eri vaiheet. Aluksi asennetaan Zabbix repository komennoilla:

wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu20.04_all.deb
dpkg -i zabbix-release_6.0-1+ubuntu20.04_all.deb
apt update

Seuraavaksi asennetaan Zabbix-ohjelma, frontend ja Zabbix-agentti. Tämä tehdään alla näkyvällä komennolla:

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent

Toimiakseen Zabbix tarvitsee tietokannan. Alla olevilla komennoilla luodaan uusi tietokanta, käyttäjä sitä varten ja asetetaan oikeudet käyttäjälle.

mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix. to zabbix@localhost;*
mysql> quit;

Seuraaravaksi ajetaan komento:

zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p Zabbix

Zabbix-palvelimen konfiguraatiotiedostoon asetetaan tietokannan salasana. Tiedosto löytyy polusta “/etc/zabbix/zabbix_server.conf” ja sieltä rivi “DBPassword=password”.

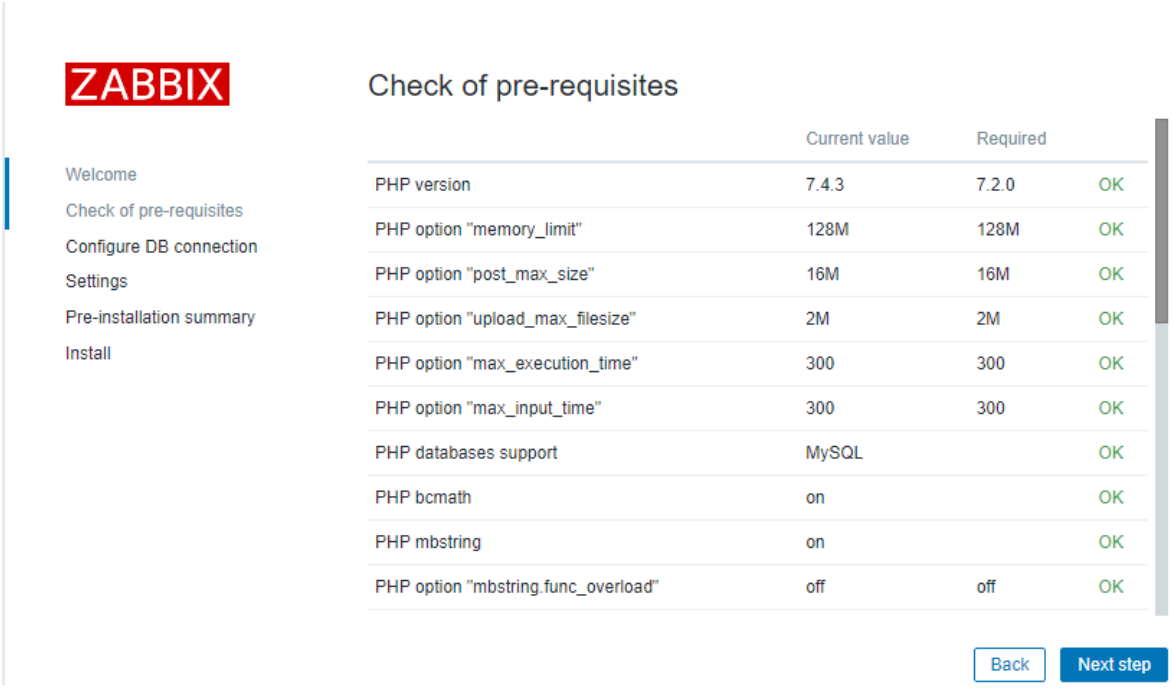
Tarvittavat prosessit käynnistetään uudelleen ja asetetaan ne käynnistymään itsestään aina palvelimen käynnistyessä komennoilla:

systemctl restart zabbix-server zabbix-agent apache2
systemctl enable zabbix-server zabbix-agent apache2

Tässä vaiheessa päästään selaimella kiinni palvelimeen sen IP-osoitteella. Asennus viedään loppuun sitä kautta. Alkunäkymä alla olevassa kuviossa 4.

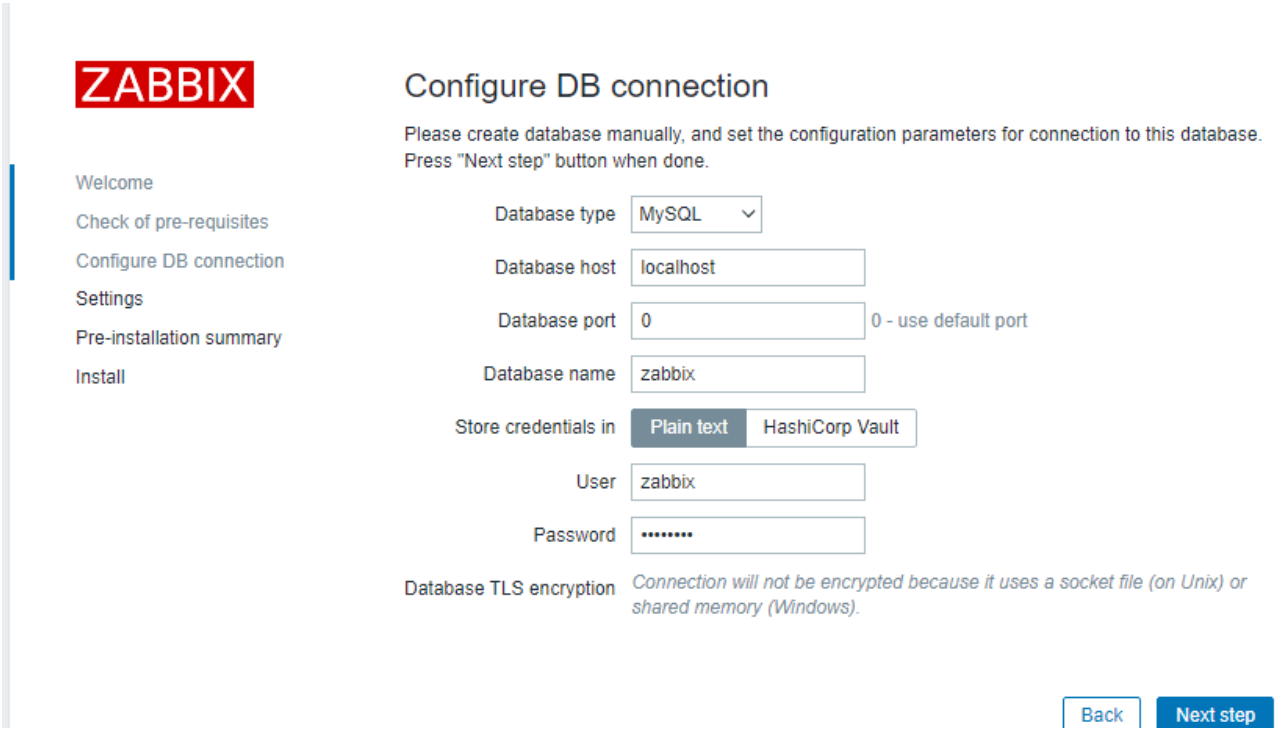
Kuvio 4. Zabbixin alkunäkymä selaimella

Seuraava asennusohjelman vaihe kuviossa 5. Ohjelma tarkistaa, että kaikki tavittavat asennukset ja määritykset löytyvät ja näyttää näiden tiedot.



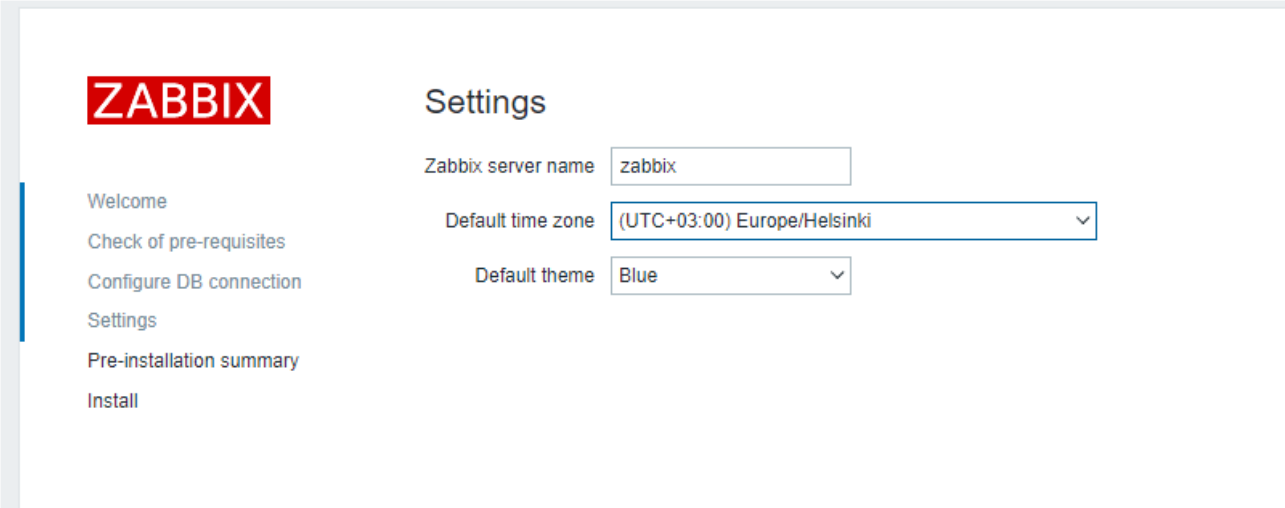
Kuvio 5. Zabbix asennusohjelman toinen vaihe

Seuraavaksi määritetään tietokannan tiedot, kuten käyttäjä, salasana ja sijainti, joka on tässä tapauksessa paikallinen kone. Nämä näkyvät kuviossa 6 alla.



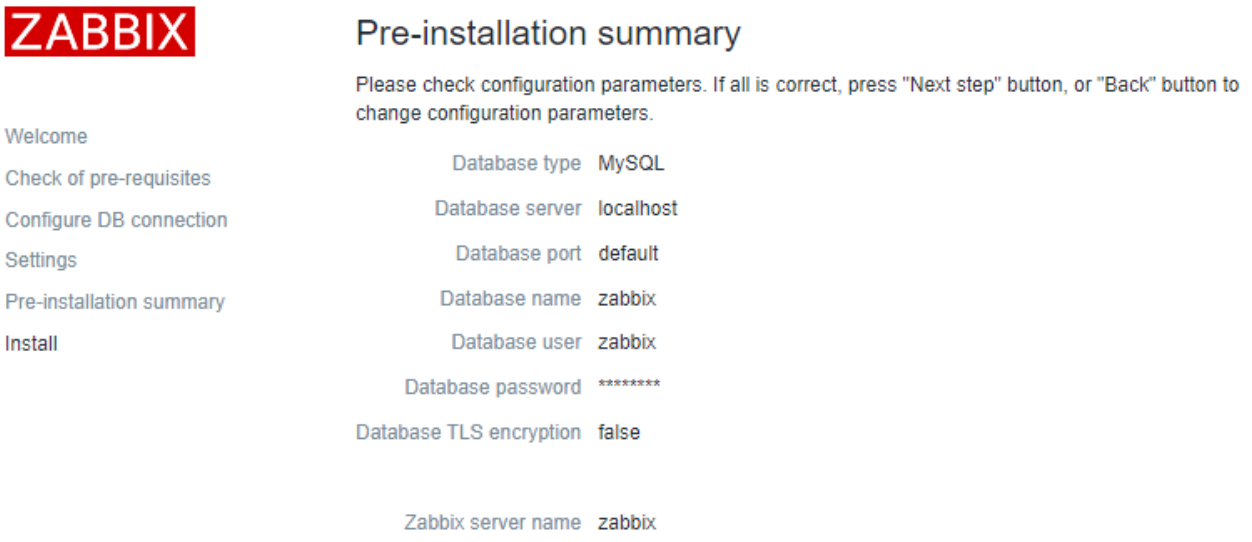
Kuvio 6. Zabbix tietokannan määritys

Määritetään Zabbix-palvelimen nimi ja aikavyöhyke kuvion 7 mukaisesti. Myös oletusteemaa voisi tässä kohdassa halutessaan muuttaa.



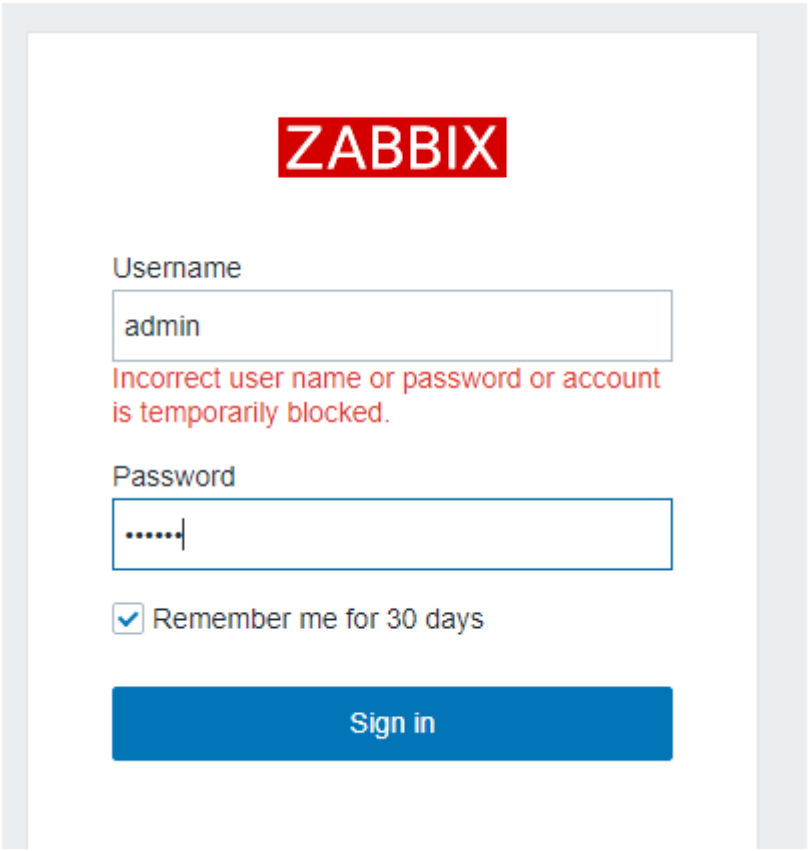
Kuvio 7. Zabbix palvelimen nimi ja aikavyöhyke

Seuraavaksi asennusohjelma näyttää yhteenvedon esiasennuksessa määritetyistä asetuksista. Tämä nähdään kuviossa 8.



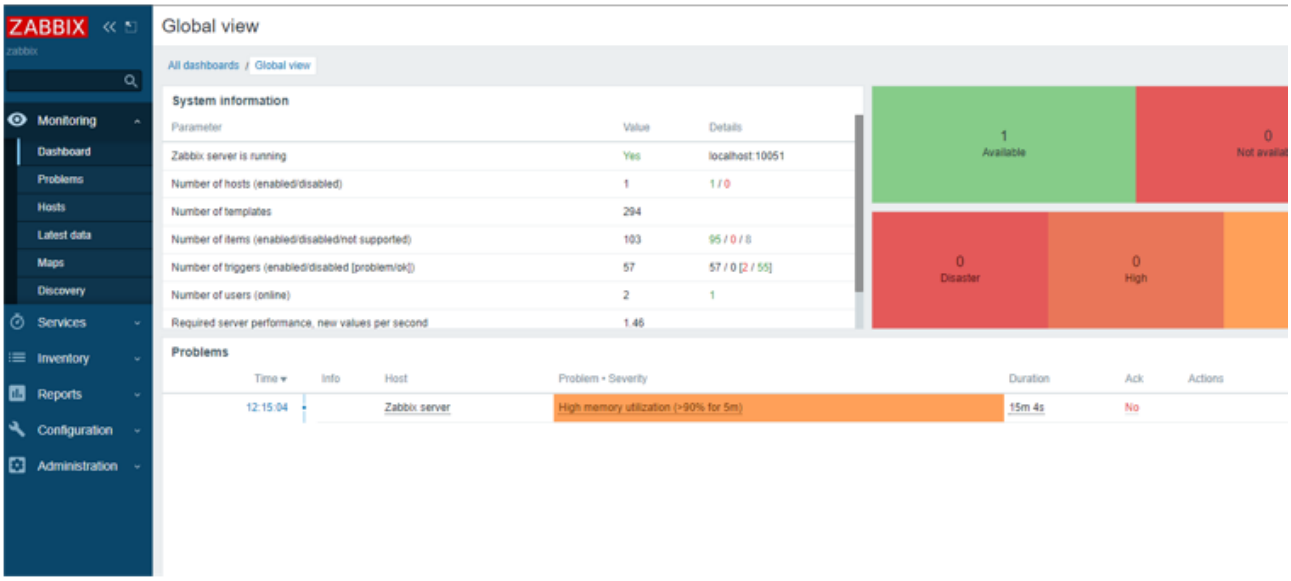
Kuvio 8. Zabbix asetusten yhteenveto

Asennus on valmis. Ensimmäinen sisäänkirjautuminen tapahtuu oletustunnuksella Admin ja salasana zabbix. Kuviossa 9 alla näkyy kirjautumisikkuna.



Kuvio 9. Zabbixin kirjautumisikkuna

Onnistuneen sisäänkirjautumisen jälkeen esille tulee Zabbixin perusnäkymä. Perusnäkymä näkyy kuviossa 10.

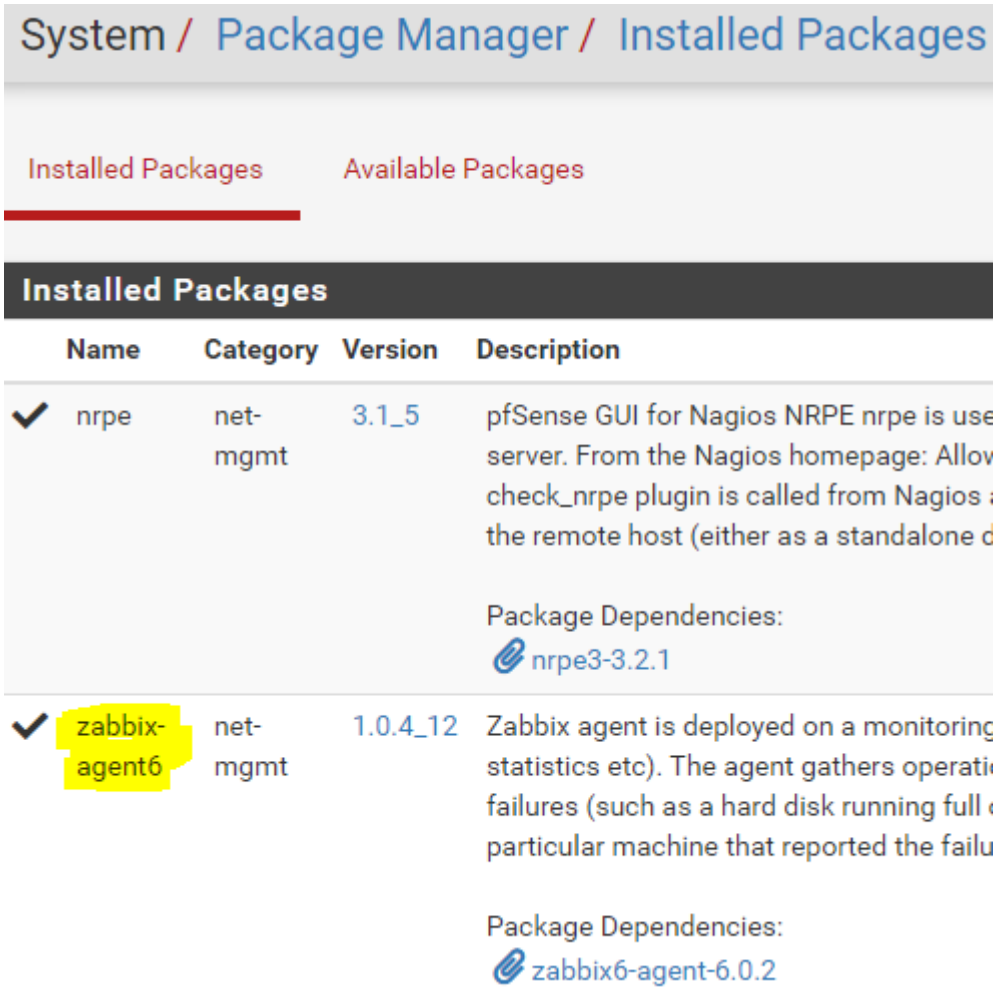


Kuvio 10. Zabbix perusnäkymä

Tässä vaiheessa Zabbix on valmis käytettäväksi. (Download and install Zabbix n.d.)

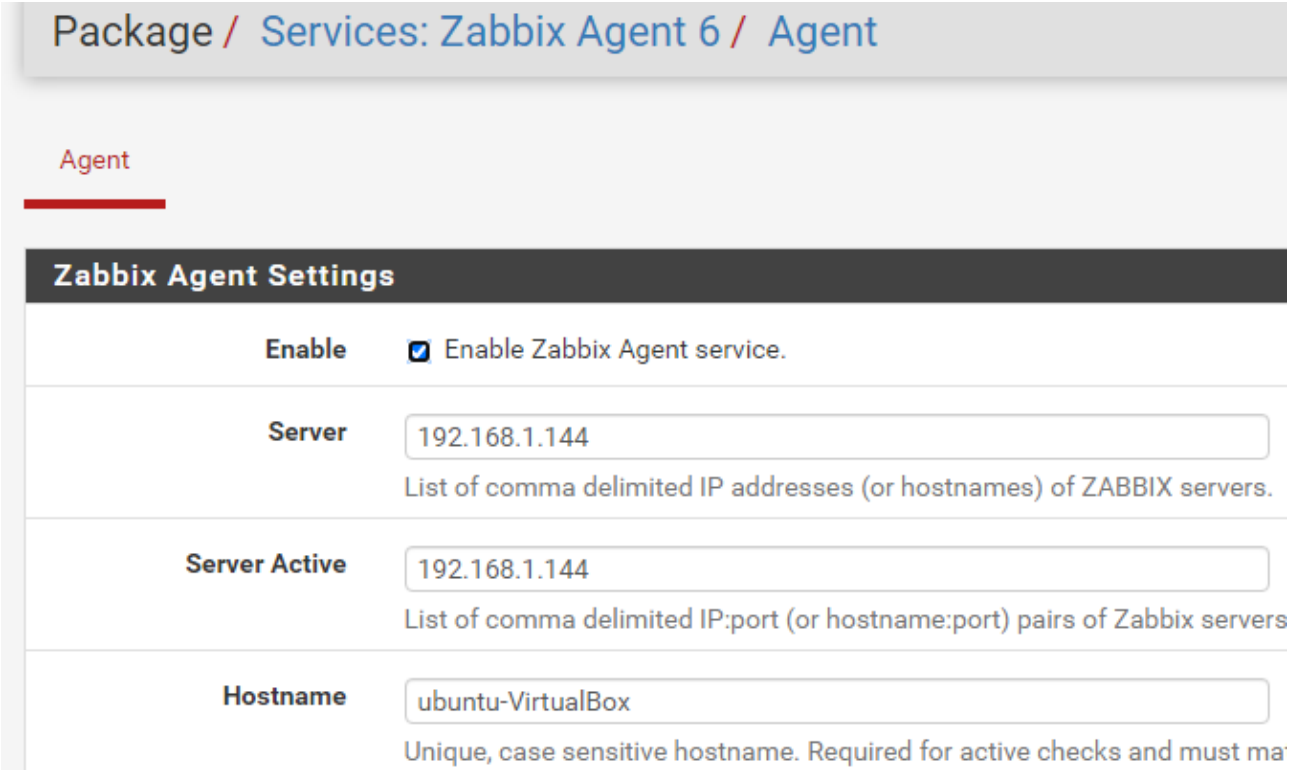
Zabbix agentin asennus pfsenseen

Zabbix agent löytyy pfsenseen menemällä system -> package manager -> available packages ja hakemalla Zabbix. Paketti ladataan ja asennetaan. Kuviossa 11 Zabbix agent on asennettuna.



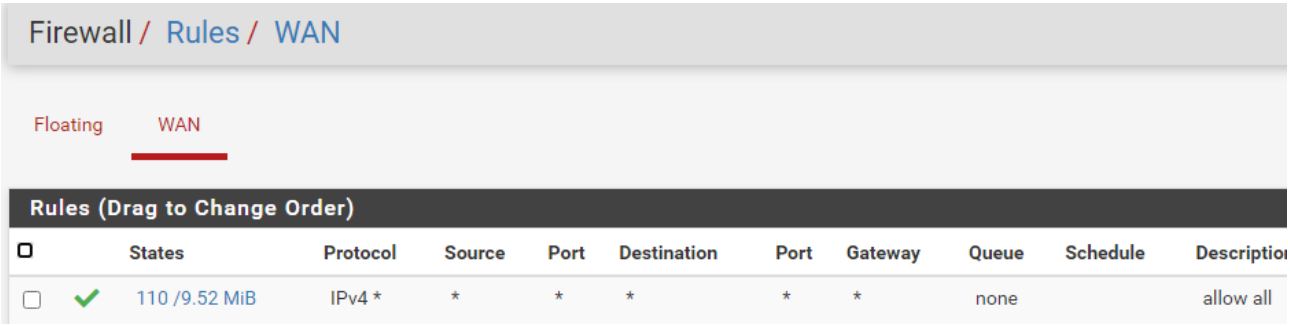
Kuvio 11. Zabbix agent pfsensellä

Agentin asetuksiin laitetaan Zabbix-palvelimen IP-osoite ja pfsensen hostname. Agentti piti myös laittaa päällä. Nämä on tehty kuviossa 12.



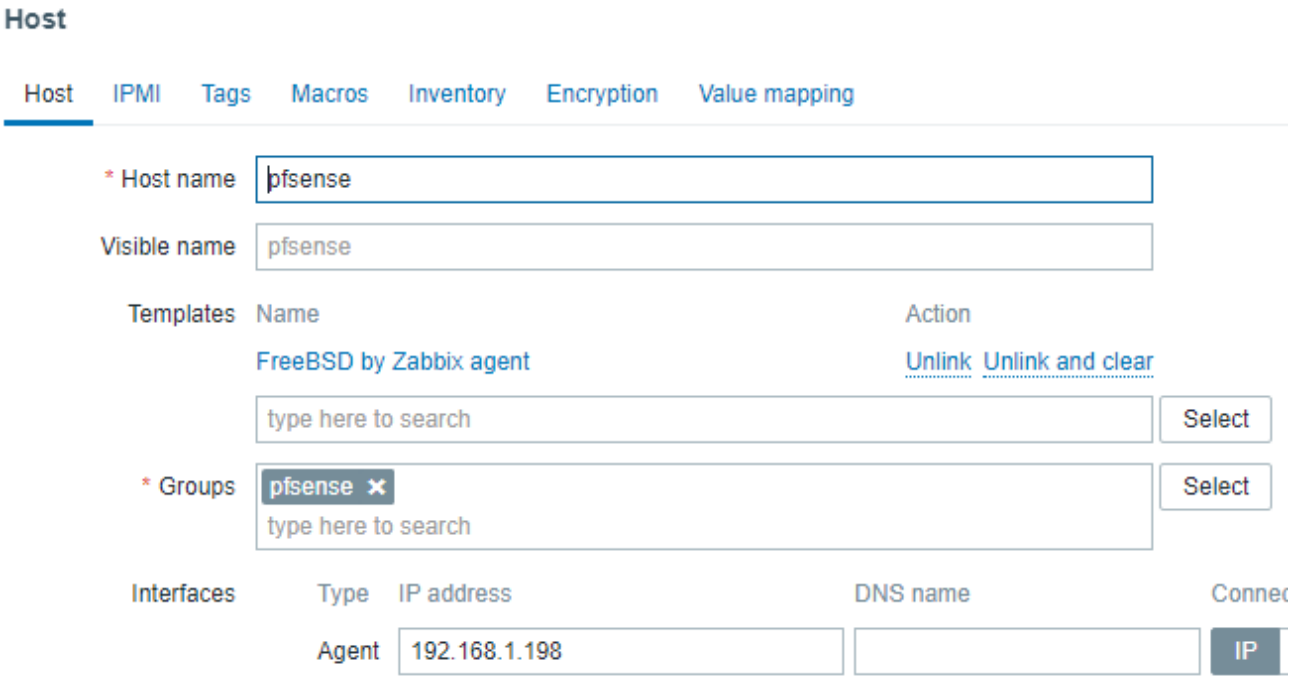
Kuvio 12. Pfsense zabbix agent asetukset

Pfsenseen täytyy tehdä sääntö, jolla sallitaan TCP liikenne Zabbixin osoitteesta agentin käyttämään porttiin 10050. Kuviossa 13 alla on tehty sääntö, joka sallii kaiken liikenteen.



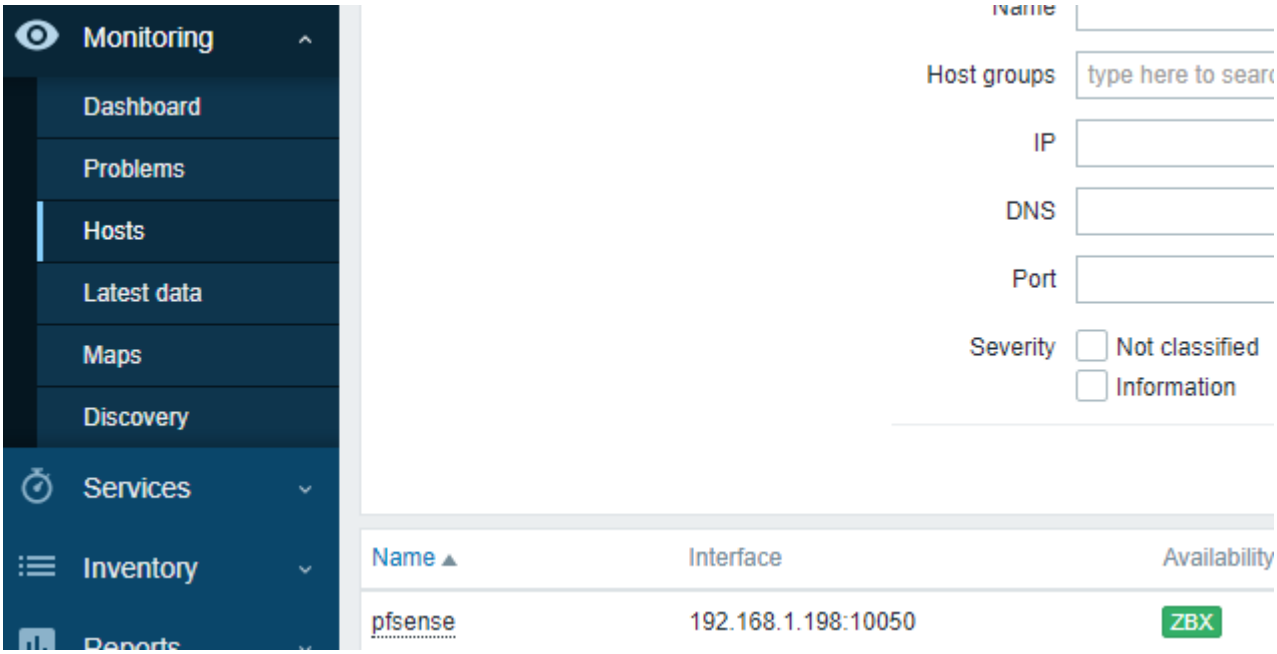
Kuvio 13. Sääntö agenttia varten

Seuraavaksi lisätään pfsense Zabbixiin käyttämällä create host toimintoa. Sinne määritetään pfsensen IP-osoite, nimi, ryhmä ja template kuvion 14 mukaisesti.



Kuvio 14. Pfsense valvontaan zabbixilla

Laite on nyt valvonnassa ja se löytyy esim. monitoring välilehdeltä hosts osiosta. Tämä näkyy kuviossa 15. (Zabbix - Monitoring PFSense using agent n.d.)



Kuvio 15. Pfsense on valvonnassa

Zabbix agentin asennus Ubuntulle

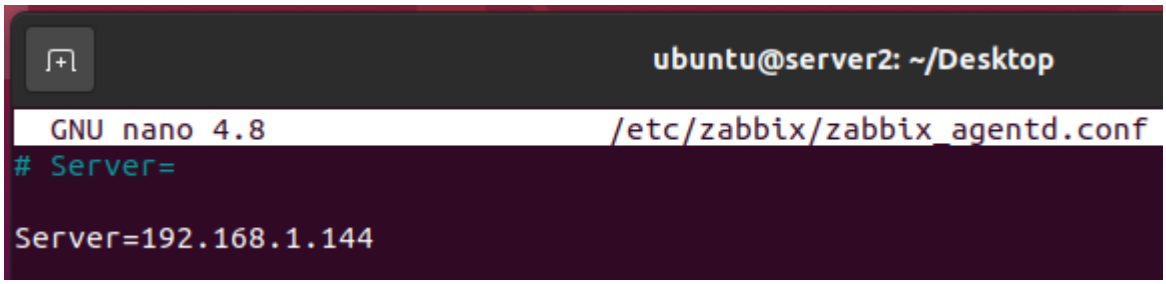
Lisätään Zabbix repository komennolla:

wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1%2Bfocal_all.deb

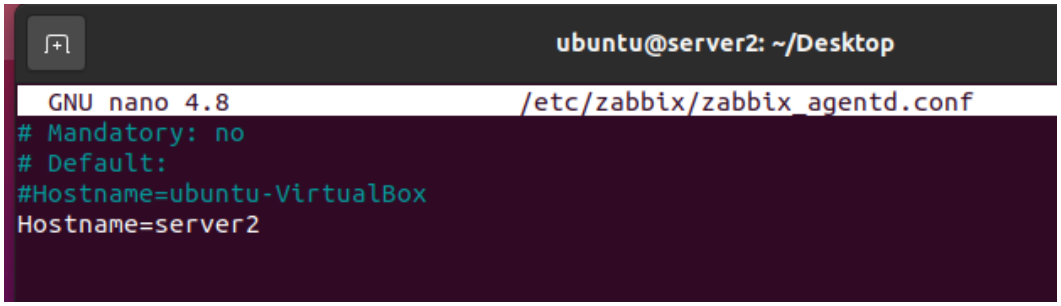
Asennetaan zabbix-agent komennoilla:

sudo apt update
sudo apt install -y zabbix-agent

Määritetään agent konfiguraatioon Zabbix-palvelimen IP ja paikallisen palvelimen hostname, kuten kuvioissa 16 ja 17 alla.



Kuvio 16. Ubuntu zabbix agent palvelimen IP

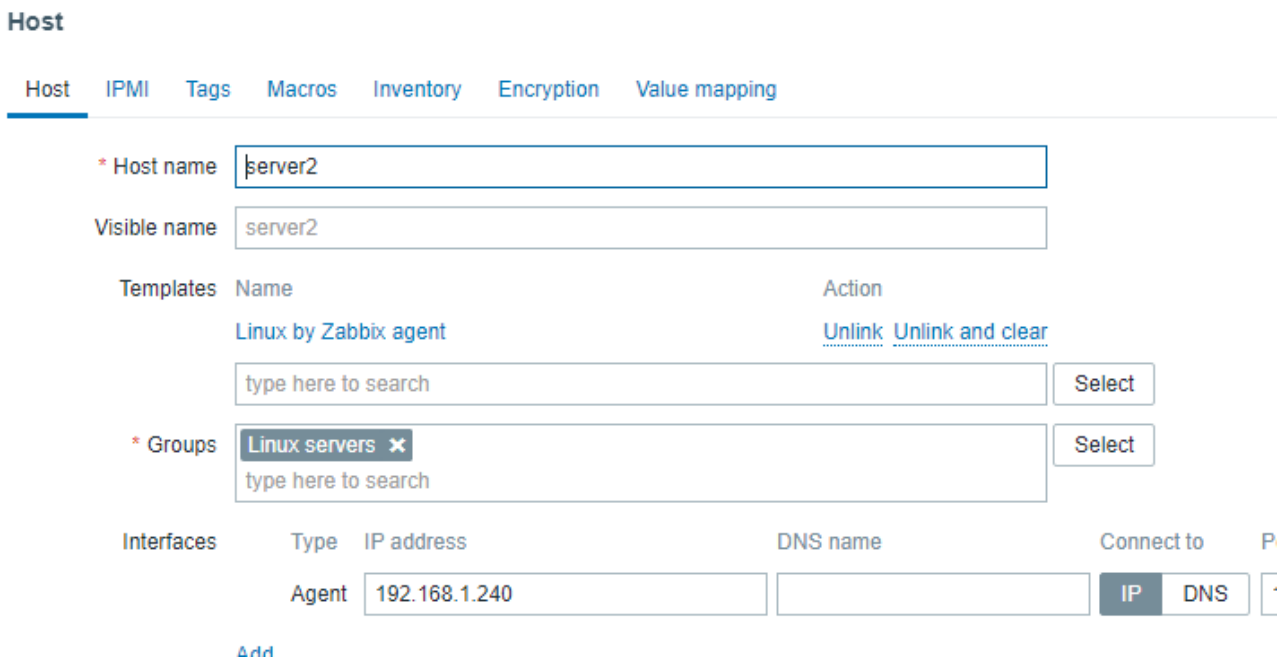


Kuvio 17. Zabbix agent hostname

Uudelleen käynnistetään agentti komennolla:

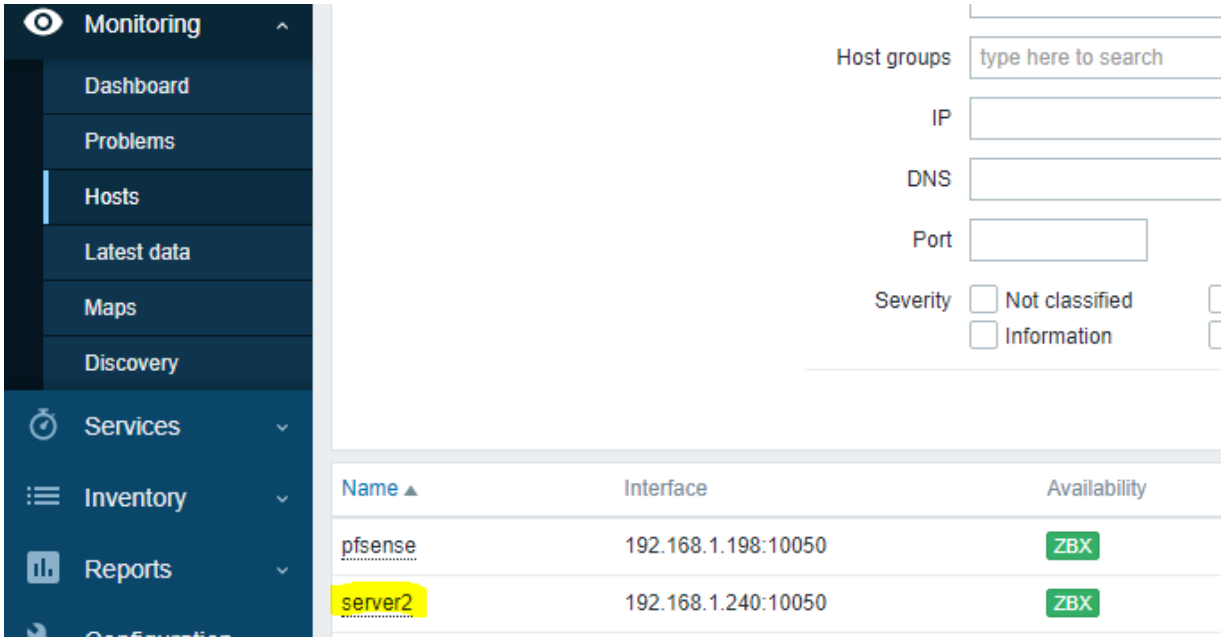
sudo systemctl restart zabbix-agent

Lisätään palvelin Zabbixiin käyttämällä create host toimintoa. Asetuksiin määritetään palvelimen nimi, IP-osoite, template ja ryhmä, kuten alla olevassa kuviossa 18.



Kuvio 18. Ubuntu palvelimen lisääminen zabbixiin

Palvelin on onnistuneesti lisätty valvontaan. Tämä nähdään myös kuviosta 19.



Kuvio 19. Ubuntu palvelin on lisätty zabbixiin

(Kiarie 2021.)

7.2 Nagios Coren asennus

Nagios Core asennettiin myös Ubuntu koneelle. Tässä käydään läpi asennuksen vaiheet.

Asennetaan tarvittavat ohjelmistot alla olevalla komennolla. Näihin lukeutuu mm. apache2, joka vastaa web-palveluista.

sudo apt install wget unzip curl openssl build-essential libgd-dev libssl-dev libapache2-mod-php php-gd php apache2 -y

Ladataan Nagios Coren asennustiedostot. Tässä ladataan sovelluksesta versio 4.4.6.

wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz

Ladattu tiedosto on pakattu. Puretaan juuri ladattu tiedosto komennolla:

sudo tar -zxvf nagios-4.4.6.tar.gz

Siirrytään kansioon, johon tiedoston sisältö purettiin ja ajetaan alla olevat komennot. Kahdella alimmaisella komennolla suoritetaan konfigurointiskripti ja kootaan ohjelmat.

cd nagios-4.4.6
sudo ./configure
sudo make all

Luodaan tarvittava ryhmä ja käyttäjä sekä lisätään www-data käyttäjä nagios ryhmään:

sudo make install-groups-users
sudo usermod -a -G nagios www-data

Asennetaan Nagios ja alustetaan konfiguraatioskriptit:

sudo make install
sudo make install-init

Alla olevilla komennoilla asennetaan ja määritetään käyttöoikeuksia, asennetaan konfiguraatiotiedostot ja asennetaan apachen tiedostot.

sudo make install-commandmode
sudo make install-config
sudo make install-webconf

Muokataan apachen asetuksia sallimalla moduulit “rewrite” ja “cgi” ja käynnistetään apache uudelleen:

sudo a2enmod rewrite
sudo a2enmod cgi
sudo systemctl restart apache2

Luodaan käyttäjä ja asetetaan sille salasana. Tällä käyttäjällä kirjaudutaan myöhemmin Nagioksen web-käyttöliittymään.

sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Ladataan Nagios Core plugin ja puretaan ladattu tiedosto:

cd ~/
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
sudo tar -zxvf nagios-plugins-2.3.3.tar.gz

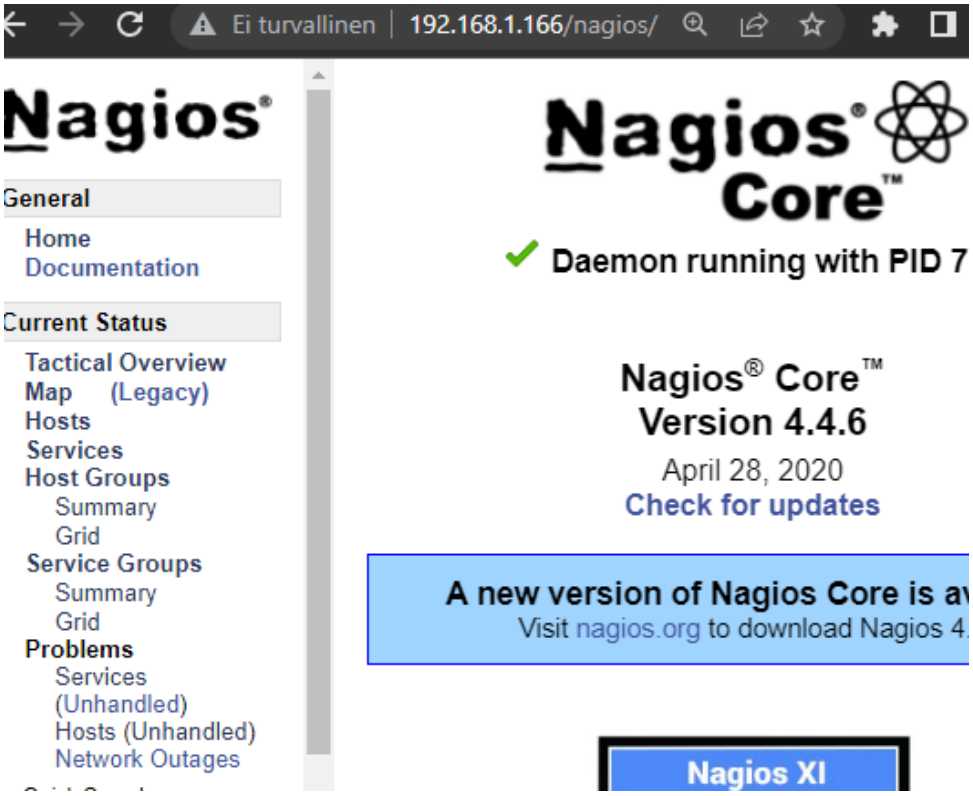
Siirrytään kansioon, johon tiedosto purettiin, ajetaan pluginin konfigurointiskripti ja asennetaan plugin komennoilla:

cd nagios-plugins-2.3.3/
sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios
sudo make
sudo make install

Tarkistetaan konfiguraatio ja määritetään Nagios käynnistymään itsestään aina palvelimen käynnistyessä:

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
sudo systemctl start nagios
sudo systemctl enable nagios

Asennus on valmis ja Nagiokseen pääsee kiinni palvelimen IP-osoitteella. Tunnus on aiemmin määritetty nagiosadmin ja salasana admin. (Install Nagios on Ubuntu 20.04 2021.) Kuviossa 20 alla on näkymää Nagioksen etusivulta ensikirjautumisella.



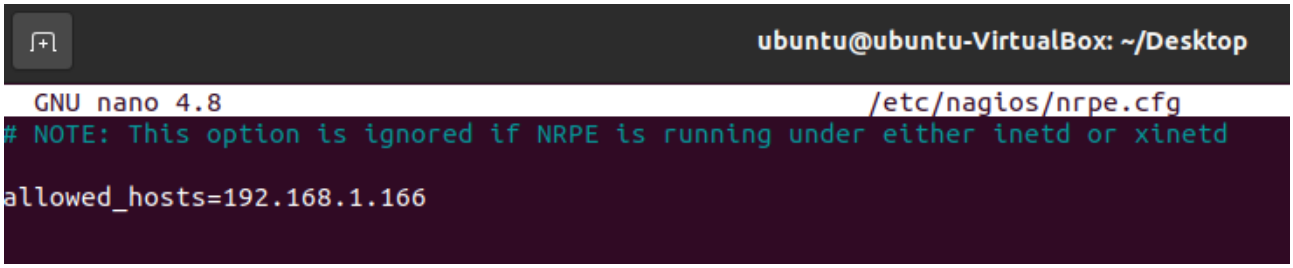
Kuvio 20. Nagioksen etusivu

Nagios-agentin asentaminen Ubuntulle ja valvonnan aktivointi

Asennus tapahtuu seuraavien vaiheiden mukaan. Aluksi valvottavalle palvelimelle asennetaan NRPE ja Nagios plugin komennolla:

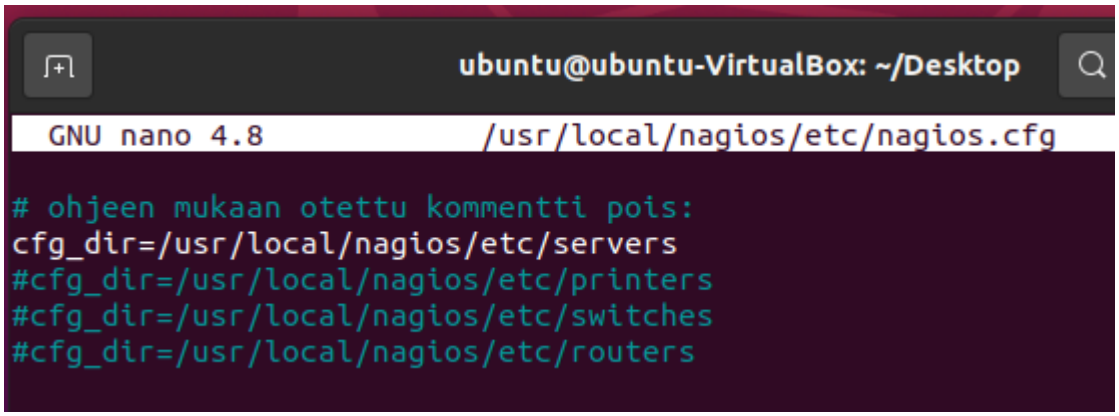
sudo apt install -y nagios-nrpe-server nagios-plugins

Konfiguraatiotiedostoon määritetään Nagios-palvelimen IP-osoite kuvion 21 osoittamalla tavalla. Asetus kertoo agentille mistä IP-osoitteesta tulevat yhteydenotot sallitaan.



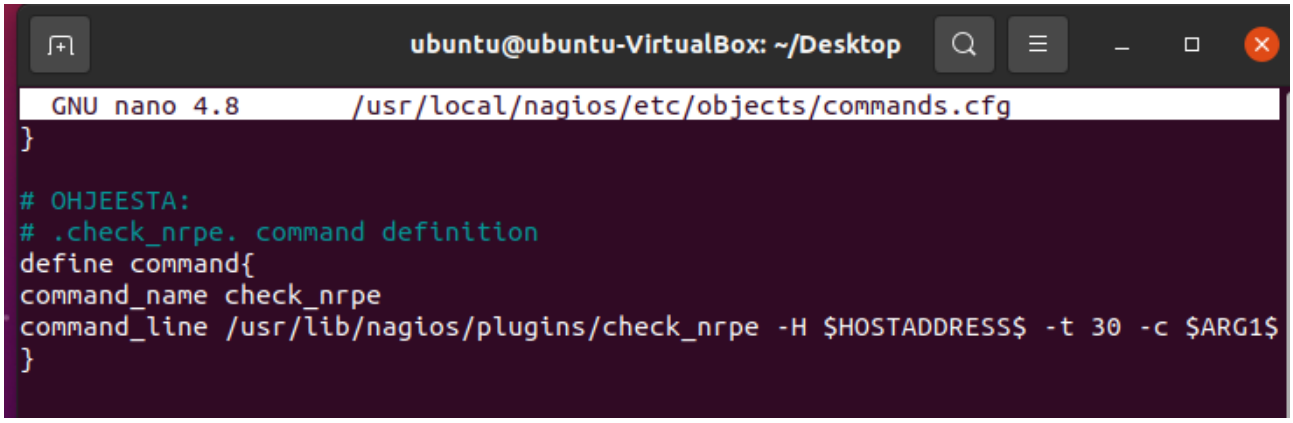
Kuvio 21. NRPE konfiguraatiotiedosto

Muokataan Nagios-palvelimelta konfiguraatiotiedostoa poistamalla kommenttimerkki kuviossa 22 näkyvällä tavalla. Tämä tehdään, jotta Nagios huomioi kaikki kyseisestä polusta löytyvät tiedostot.



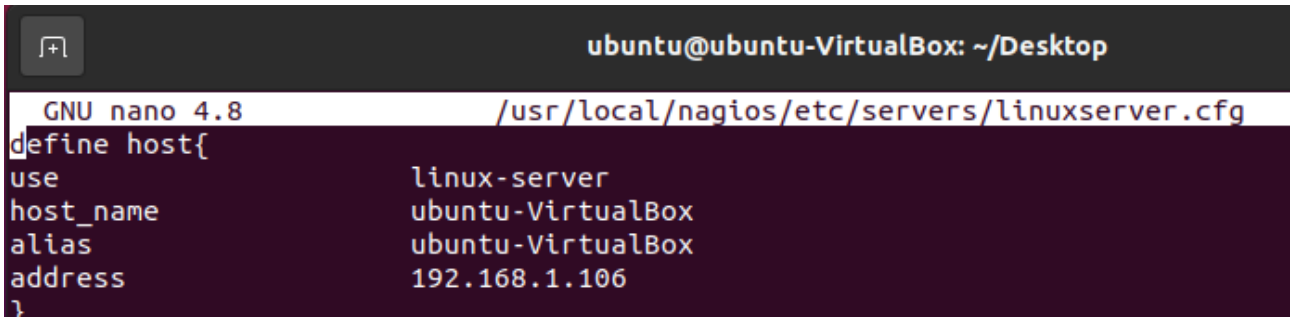
Kuvio 22. Nagios.cfg tiedoston muokkaus

Lisätään kuviossa 23 näkyvä sisältö kyseiseen tiedostoon Nagios-palvelimella. Tämä aktivoi NRPE pluginin.



Kuvio 23. Commands.cfg

Luodaan uusi tiedosto Nagios-palvelimelle. Siellä määritellään valvottavan kohteen valvonta-asetuksia. Tämä näkyy kuviossa 24.



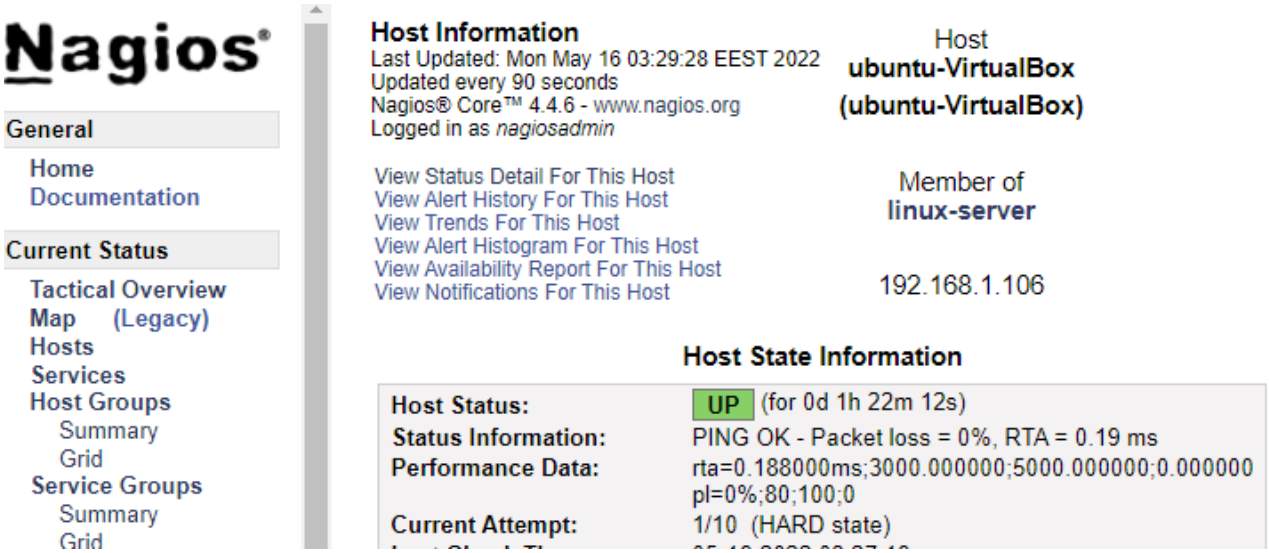
Kuvio 24. linuxserver.cfg

Tarkastetaan, että konfiguraatiossa ei ole virheitä ja uudelleen käynnistetään Nagios. Nämä komennot ajetaan Nagios-palvelimella.

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

sudo systemctl restart nagios

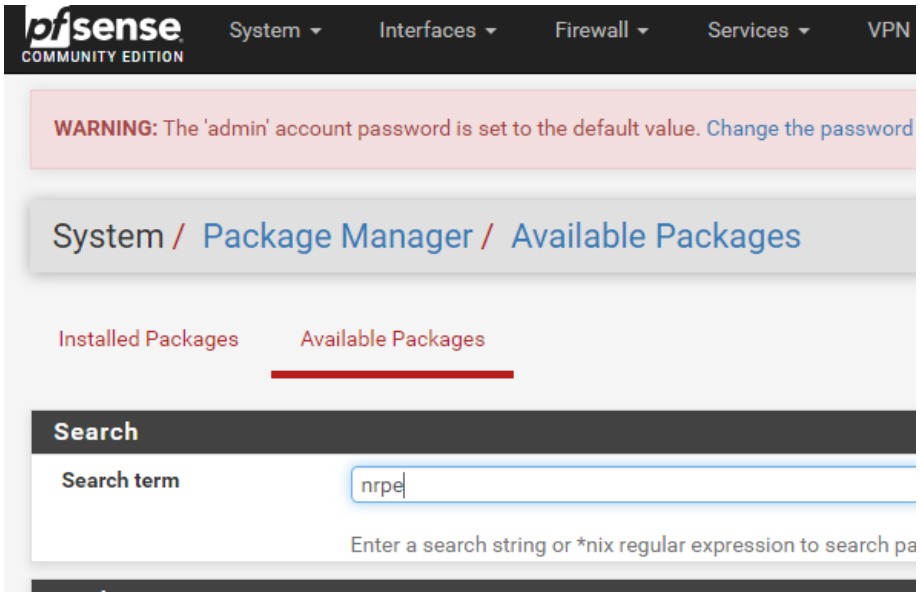
Tarkistetaan vielä Nagioksen web-käyttöliittymästä, että palvelin on valvonnassa. Tämä on tehty kuviossa 25. Palvelin on lisätty valvontaan onnistuneesti. (How To Monitor Remote Linux Systems With Nagios Monitoring Tool 2019.)



Kuvio 25. Linux palvelin Nagioksessa

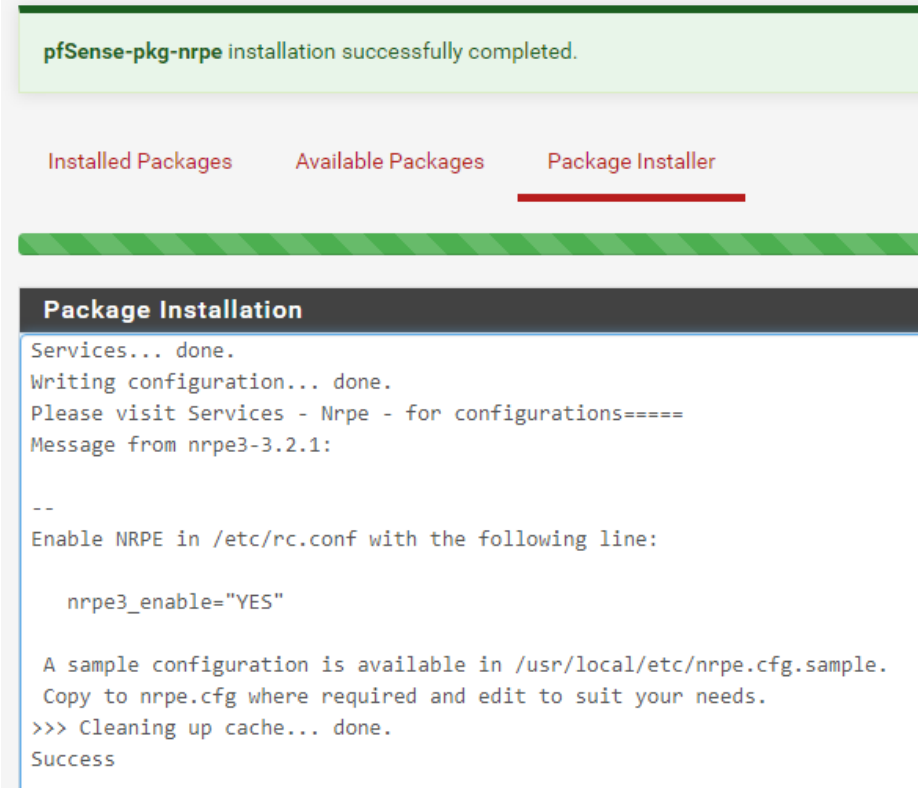
Nagios agentin asentaminen pfsenseen ja valvonnan aktivointi

Asennus tapahtuu menemällä pfsensen hallintasivulla system -> package manager -> available packages ja sieltä kirjoittamalla hakukenttään nrpe alla olevan kuvion 26 mukaisesti.



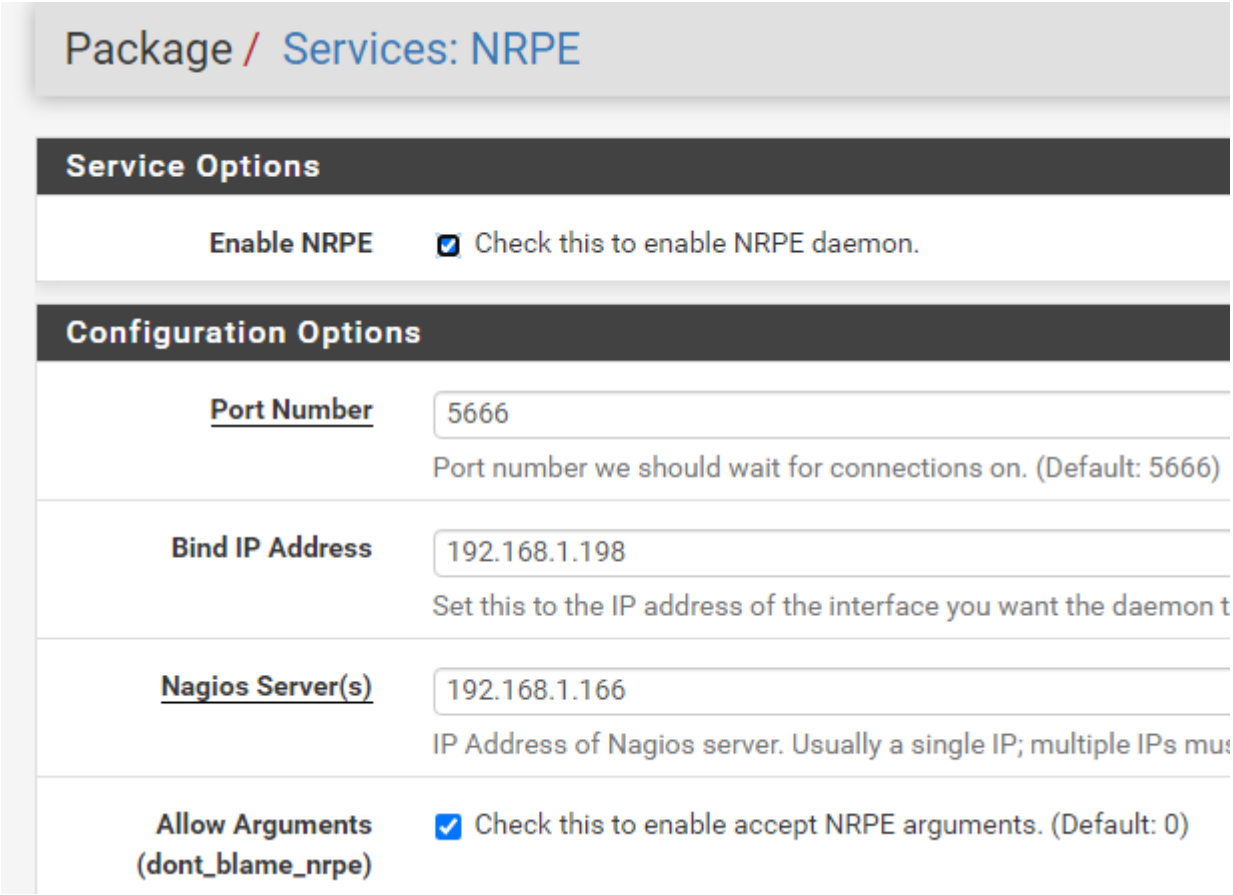
Kuvio 26. Pfsense package manager

Seuraavassa kuviossa 27 NRPE on asentumassa. NRPE:llä tarkoitetaan Nagioksen valvonta-agenttia.



Kuvio 27. NRPE asentuu pfsenseen

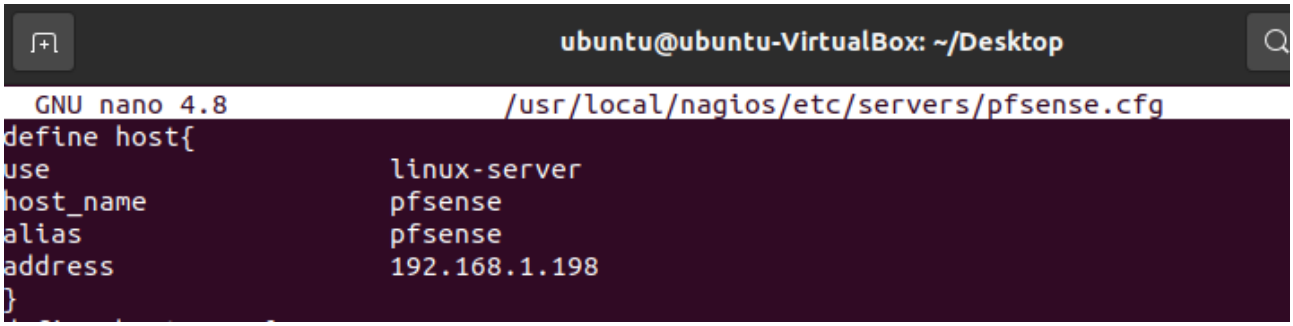
NRPE:n asetuksiin määritetään Nagios-palvelimen IP-osoite ja pfsensen IP-osoite, joka kuuntelee palvelimelta tulevia yhteyksiä. Tämä on tehty kuviossa 28.



Kuvio 28. NRPE asetukset

(Monitor pfSense with nagios 2019.)

Nagios-palvelimelle luodaan tiedosto pfsensen valvonta-asetuksia varten. Tiedosto näkyy kuviossa 29.



Kuvio 29. Pfsense.cfg

7.3 Valvontaominaisuuksien testaukset

Laitteilta valvottiin resurssien käyttöä, palveluita ja saatavuutta. Molemmilla sovelluksilla suoritettiin testejä ja katsottiin miten ne reagoivat eri valvontatilanteisiin.

7.3.1 Nagios Core

Levytilan valvonta ubuntu-palvelimelta

Ensimmäisessä testissä testattiin levytilan valvontaa ubuntu palvelimelta. Lähtötilanteessa levy ei hälytä valvonnassa, kuten nähdään kuviosta 30. Levyn tila näkyy rivillä “root / partition”.

Host	Service	Status	Status Information
ubuntu-VirtualBox	Current Load	OK	OK - load average: 0.01, 0.03, 0.00
	Current Users	OK	USERS OK - 1 users currently logged in
	Root / Partition	OK	DISK OK - free space: / 1786 MB (19% inode=67%):
	SWAP Usage	OK	SWAP OK - 70% free (312 MB out of 448 MB)
	Total Processes	WARNING	PROCS WARNING: 193 processes

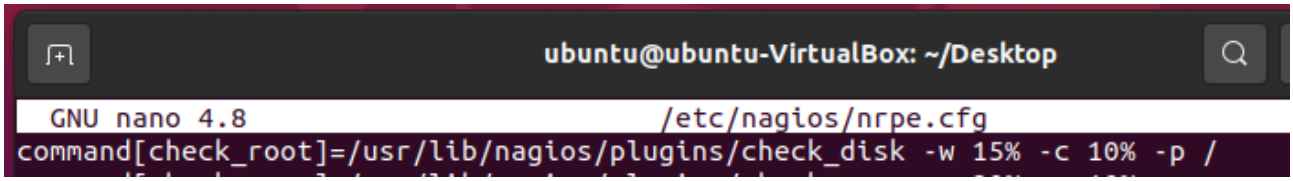
Kuvio 30. Ubuntun levytilan valvonta nagioksella

Levytila lähtötilanteessa palvelimelta katsottuna kuviossa 31. Levyn käyttöaste oli 81%

```
ubuntu@ubuntu-VirtualBox:~/Desktop$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            454M     0  454M   0% /dev
tmpfs            98M  1,3M   96M   2% /run
/dev/sda5       9,3G  7,1G  1,8G  81% /
```

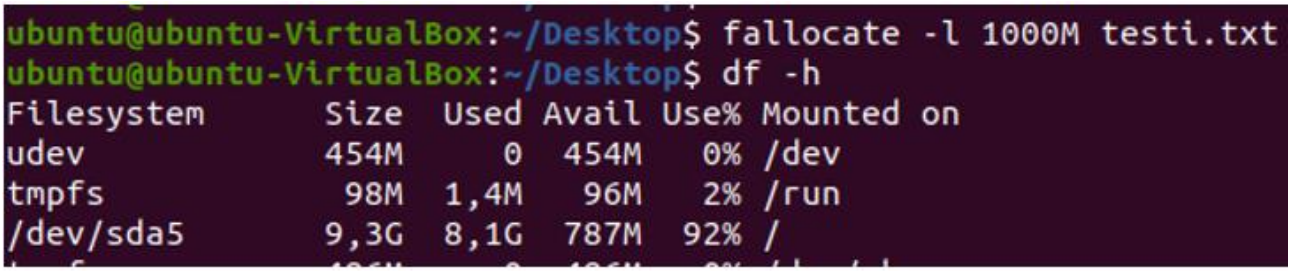
Kuvio 31. Ubuntu vapaa levytila

Nagiokselle määritettiin hälytysrajat seuraavasti. Kun levytilaa on vapaana alle 15%, näkyy levy varoitustilassa hälytysnäkymässä ja kun vapaana on alle 10%, tila on kriittinen. Asetus löytyy valvottavan koneen valvonta-agentin asetuksista, kuten nähdään kuviosta 32. Samalla määritetään valvottava levyosio, joka siis on tässä tapauksessa root eli “/”.



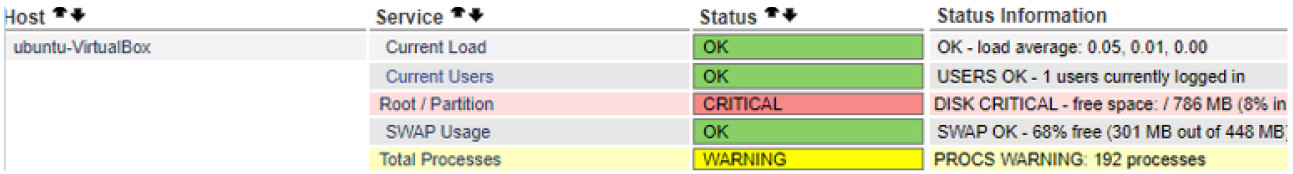
Kuvio 32. Nrpe.cfg hälytysrajat

Palvelimelle luotiin yhden gigan kokoinen tiedosto, jotta levytila ylittää hälytysrajat. Tiedoston luonti ja levytilan tarkistus sen jälkeen kuviossa 33.



Kuvio 33. Tiedoston luonti ja tilan tarkistus

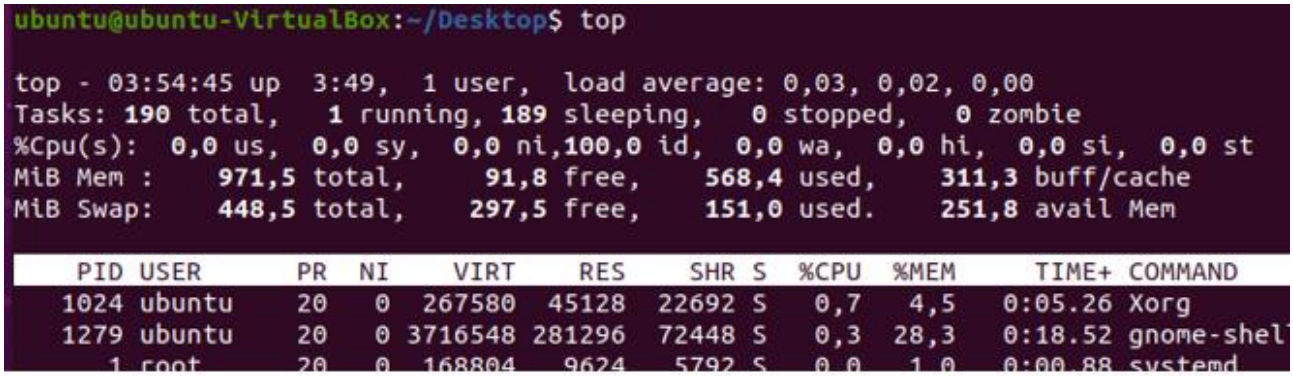
Root-osion käyttö oli 92% eli molemmat hälytysrajat ylittyivät. Kuviosta 34 nähdään, että levy hälyttää valvonnassa kriittistä tilaa.



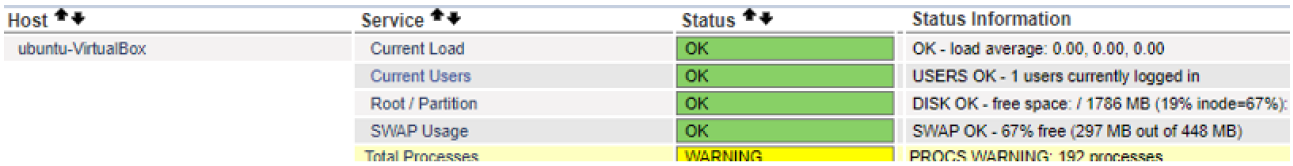
Kuvio 34. Ubuntun levy hälyttää Nagioksessa

Prosessorin käyttöasteen valvonta ubuntu-palvelimelta

Lähtötilanteessa käyttöaste oli nollissa, kuten nähdään kuviosta 35 palvelimelta katsottuna ja kuviosta 36 nagioksesta katsottuna kohdassa service – current load.

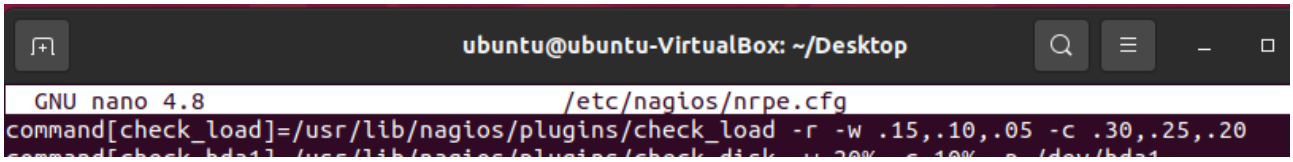


Kuvio 35. Ubuntu prosessorin käyttö lähtötilanne



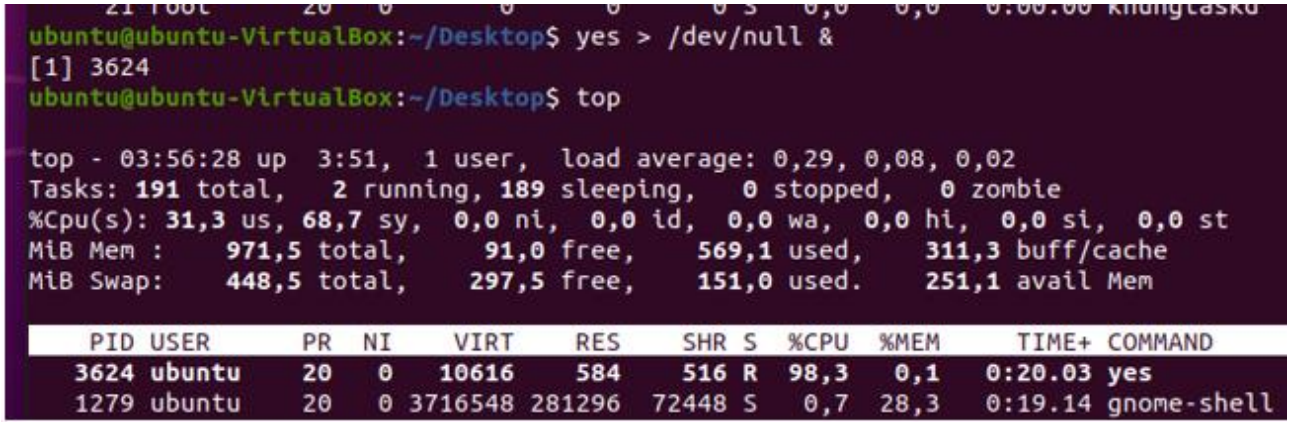
Kuvio 36. Ubuntu prosessorin käyttö nagioksessa

Alla olevassa kuviossa 37 näkyy prosessorin valvonnan määritykset. Ne löytyvät valvonta-agentin konfiguraatiotiedostosta. Agentti valvoo prosessorin käytön muutosta.



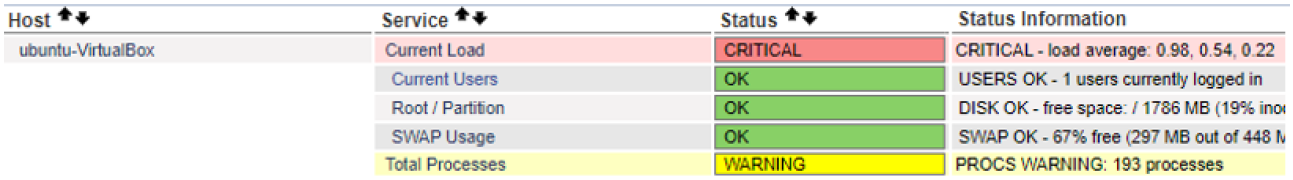
Kuvio 37. Nrpe.cfg prosessorin käytön valvonta

Seuraavaksi prosessorille luotiin kuormaa. Tähän käytettiin komentoa ”yes > /dev/null &”, jolla prosessoria saadaan helposti kuormitettua (Easy way to load CPU / memory on Linux n.d). Kuvi-osta 38 nähdään, että prosessorin käyttö oli lähellä 100%.



Kuvio 38. Ubuntu prosessorin kuormitus

Nagios hälyttää ubuntu-palvelimen korkeasta prosessorin käytöstä. Tämä nähdään kuviosta 39.

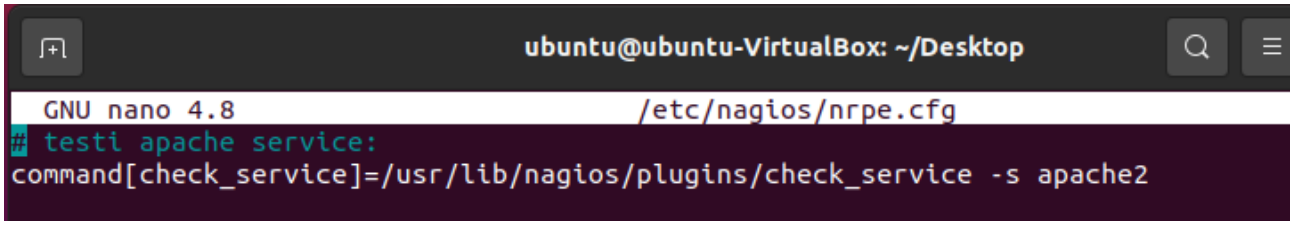


Kuvio 39. Prosessorin käyttö hälyttää nagioksessa

Palvelun tilan valvonta ubuntulla

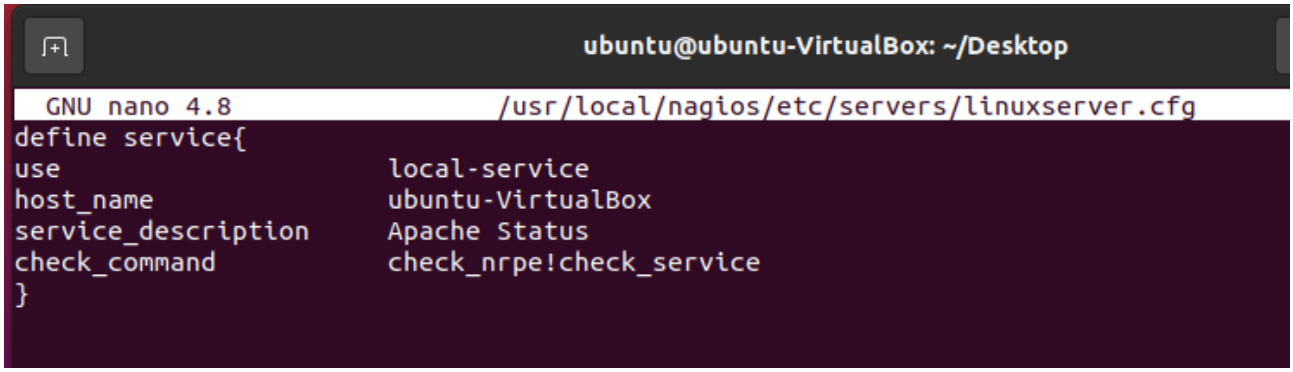
Ubuntu-palvelimelta testattiin myös valvoa palvelun tilaa eli onko jokin tietty palvelu käynnissä. Valvottava palvelu oli apache2.

Palvelun valvontaa varten kohdepalvelimelle ladattiin check_service -plugin, joka tarkistaa halutun palvelun tilan ja palauttaa tiedon valvontapalvelimelle (https://exchange.nagios.org/directory/Plugins/Reporting/Linux-Check-Service/details). Tiedosto ladattiin kuviossa 40 näkyvään polkuun ubuntu-palvelimelle ja plugin määritettiin seuraamaan apache2-palvelun tilaa valvonta-agentin konfiguraatioon, kuten samasta kuviosta nähdään.



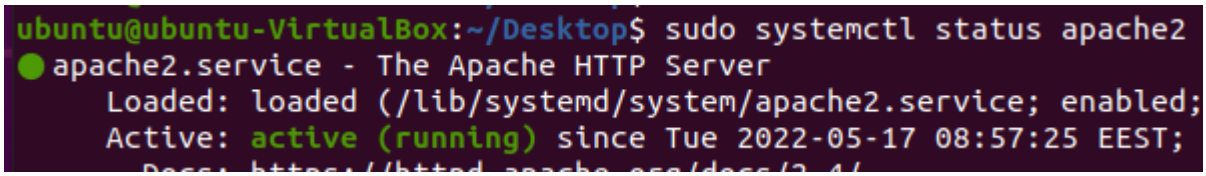
Kuvio 40. Check_service -plugin

Lisäksi Nagioksen asetuksiin piti vielä määrittää check_service -pluginin käyttö kohdepalvelimen asetustiedostoon. Määritys näkyy kuviossa 41.



Kuvio 41. Check_service -pluginin käyttöönotto

Lähtötilanteessa palvelu oli käynnissä. Kuviossa 42 näkyy palvelun tila palvelimelta katsottuna ja kuviossa 43 Nagioksesta katsottuna.



Kuvio 42. Apache2 palvelu käynnissä

Host	Service	Status	Status Information
ubuntu-VirtualBox	Apache Status	OK	OK: Service apache2 is running!
	Current Load	OK	OK - load average: 0.03, 0.06, 0.03
	Current Users	OK	USERS OK - 1 users currently logged in
	Root / Partition	OK	DISK OK - free space: / 1777 MB (19% inode=67
	SWAP Usage	OK	SWAP OK - 68% free (303 MB out of 448 MB)
	Total Processes	WARNING	PROCS WARNING: 190 processes

Kuvio 43. Apache2 palvelu käynnissä nagioksesta katsottuna

Seuraavaksi palvelu sammutettiin. Kuviosta 44 nähdään, että palvelu on pysähtynyt.

```
ubuntu@ubuntu-VirtualBox:~/Desktop$ sudo systemctl stop apache2
ubuntu@ubuntu-VirtualBox:~/Desktop$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled
     Active: inactive (dead) since Tue 2022-05-17 11:20:16 EEST;
       Docs: https://httpd.apache.org/docs/2.4/
```

Kuvio 44. Apache2 palvelu sammutettu

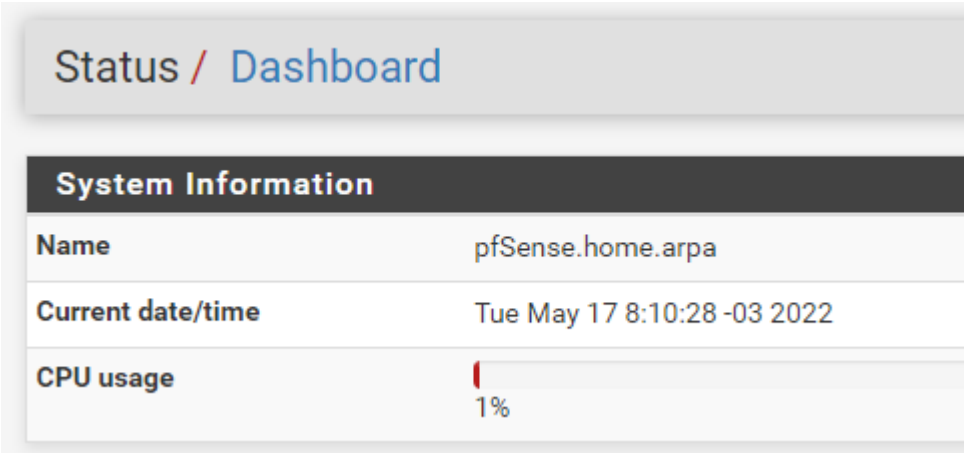
Nagios alkoi hälyttämään, että palvelu on alhaalla. Tämä nähdään kuviosta 45 alla.

Host	Service	Status	Status Information
ubuntu-VirtualBox	Apache Status	CRITICAL	CRITICAL: Service apache2 is not running!
	Current Load	OK	OK - load average: 0.00, 0.02, 0.02
	Current Users	OK	USERS OK - 1 users currently logged in
	Root / Partition	OK	DISK OK - free space: / 1777 MB (19% inode=67%):
	SWAP Usage	OK	SWAP OK - 68% free (303 MB out of 448 MB)
	Total Processes	WARNING	PROCS WARNING: 189 processes

Kuvio 45. Apache palvelu hälyttää nagioksessa

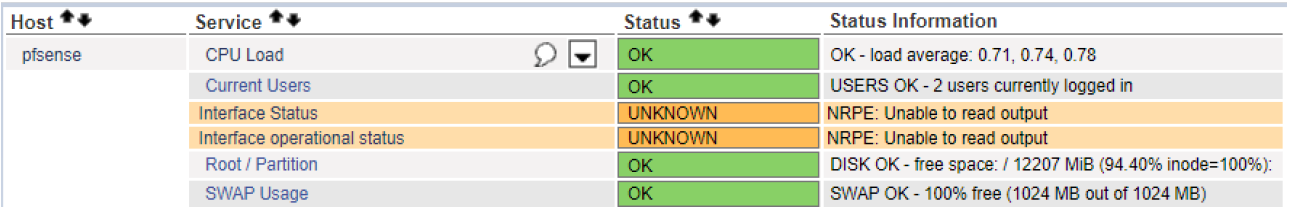
Prosessorin käytön valvonta pfsensellä

Alkutilanteessa käyttöä ei juuri ollut. Kuviossa 46 prosessin käyttö pfsensen käyttöliittymästä katsottuna.



Kuvio 46. Pfsense prosessorin käyttö alussa

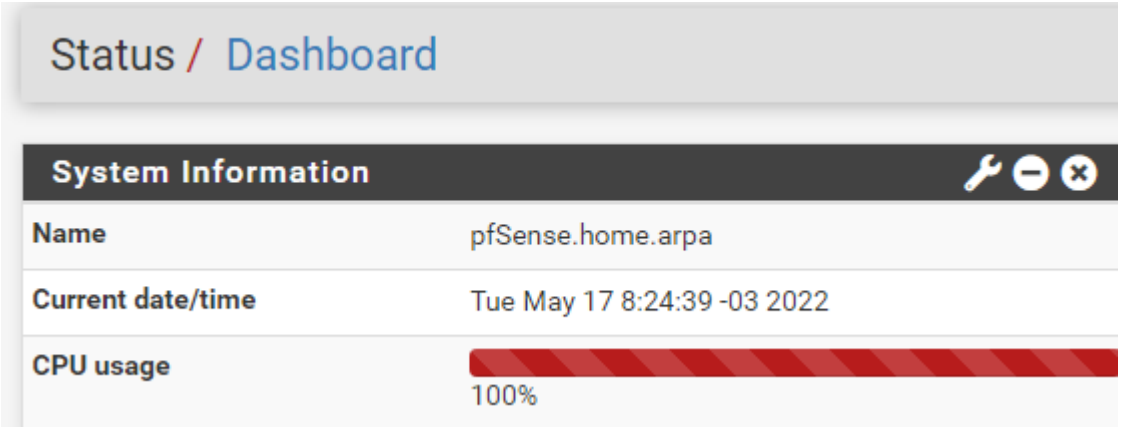
Nagioksesta katsottuna prosessorin käyttö myös ok-tilassa. Tämä näkyy kuviosta 47 rivillä ”CPU load”.



Host	Service	Status	Status Information
pfsense	CPU Load	OK	OK - load average: 0.71, 0.74, 0.78
	Current Users	OK	USERS OK - 2 users currently logged in
	Interface Status	UNKNOWN	NRPE: Unable to read output
	Interface operational status	UNKNOWN	NRPE: Unable to read output
	Root / Partition	OK	DISK OK - free space: / 12207 MiB (94.40% inode=100%):
	SWAP Usage	OK	SWAP OK - 100% free (1024 MB out of 1024 MB)

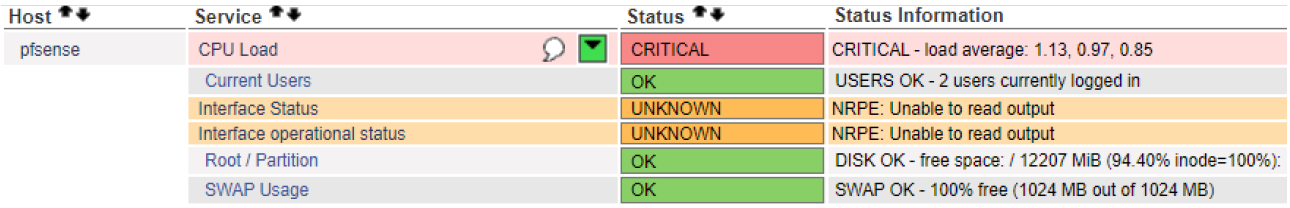
Kuvio 47. Pfsense prosessorin käyttö nagioksessa

Prosessorille luotiin kuormaa ”yes > /dev/null &” komennolla. Käyttö nousi 100%:iin, kuten nähdään kuviosta 48.



Kuvio 48. Pfsense prosessorin käyttö 100%

Nagios alkoi hälyttämään korkeasta prosessorin käytöstä. Hälytys tästä näkyy kuviossa 49.



Kuvio 49. Pfsense prosessorin käyttö hälyttää

Levytilan valvonta pfsenseltä

Alussa levyllä oli reilusti vapaata tilaa. Levylle luotiin 10 gigan kokoinen tiedosto, jolla saatiin levy melkein täyteen. Kuten ubuntunkin kanssa, myös pfsenseltä valvotaan root-osiota. Kuviossa 50 näkyy alkutilanne, tiedoston luonti ja sen seurauksena levyn täyttyminen 85%:iin asti.

```
[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: df -h
Filesystem              Size    Used   Avail Capacity  Mounted on
pfSense/ROOT/default     13G    724M     12G     6%    /
devfs                   1.0K    1.0K      0B   100%    /dev
pfSense/cf               12G     96K     12G     0%    /cf
pfSense/home             12G     96K     12G     0%    /home
pfSense                  12G     96K     12G     0%    /pfSense
pfSense/tmp              12G    188K     12G     0%    /tmp
pfSense/var              12G    3.2M     12G     0%    /var
pfSense/cf/conf          12G    512K     12G     0%    /cf/conf
pfSense/reservation      13G     96K     13G     0%    /pfSense/reservation
pfSense/var/cache        12G    4.1M     12G     0%    /var/cache
pfSense/var/log          12G    568K     12G     0%    /var/log
pfSense/var/db           12G    3.6M     12G     0%    /var/db
pfSense/var/empty        12G     96K     12G     0%    /var/empty
pfSense/var/tmp          12G    104K     12G     0%    /var/tmp
tmpfs                   4.0M    128K    3.9M     3%    /var/run
devfs                   1.0K    1.0K      0B   100%    /var/dhcpd/dev
[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: dd if=/dev/urandom of=testi.txt bs=1G count=10
10+0 records in
10+0 records out
10737418240 bytes transferred in 58.546477 secs (183399902 bytes/sec)
[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: df -h
Filesystem              Size    Used   Avail Capacity  Mounted on
pfSense/ROOT/default     13G     11G    1.9G    85%    /
```

Kuvio 50. Pfsensen levyn täyttäminen

Kuviossa 51 alla näkyy alkutilanne Nagioksesta katsottuna. Rivillä ”root / partition” näkyy levyn tilanne.

Host	Service	Status	Status Information
pfsense	CPU Load	OK	OK - load average: 1.01, 0.86, 0.84
	Current Users	OK	USERS OK - 2 users currently logged in
	Interface Status	UNKNOWN	NRPE: Unable to read output
	Interface operational status	UNKNOWN	NRPE: Unable to read output
	Root / Partition	OK	DISK OK - free space: / 12207 MiB (94.40% inode=100%):
	SWAP Usage	OK	SWAP OK - 100% free (1024 MB out of 1024 MB)

Kuvio 51. Pfsense levy nagioksessa

Valvonta-agentin konfiguraatioon on määritetty hälytysrajoiksi varoitustilalle 20% vapaata levytilaa ja kriittiselle tilalle 10% vapaata levytilaa. Tämä nähdään kuviosta 52 alimmalta riviltä.

```
[2.6.0-RELEASE][admin@pfSense.home.arpa]/root: cat /usr/local/etc/nrpe.cfg
log_facility=daemon
pid_file=/var/run/nrpe3.pid
server_port=5666
nrpe_user=nagios
nrpe_group=nagios
allowed_hosts=192.168.1.166
dont_blame_nrpe=1
debug=0
command_timeout=60
connection_timeout=300
command[check_users]=/usr/local/libexec/nagios/check_users -w 5 -c 10
command[check_load]=/usr/local/libexec/nagios/check_load -w 15,10,5 -c 30,25,20
command[check_root]=/usr/local/libexec/nagios/check_disk -w 20% -c 10% -p /
```

Kuvio 52. Pfsense levytilan valvontarajat

Levytilaa on vapaana 15%, joten se hälyttää varoitustilaa Nagioksessa. Tämä näkyy kuviossa 53.

Host	Service	Status	Status Information
pfsense	CPU Load	OK	OK - load average: 0.61, 0.80, 0.86
	Current Users	OK	USERS OK - 2 users currently logged in
	Interface Status	UNKNOWN	NRPE: Unable to read output
	Interface operational status	UNKNOWN	NRPE: Unable to read output
	Root / Partition	WARNING	DISK WARNING - free space: / 1960 MiB (15.16% inode=99%):
	SWAP Usage	OK	SWAP OK - 92% free (936 MB out of 1024 MB)

Kuvio 53. Pfsensen levy varoitustilassa

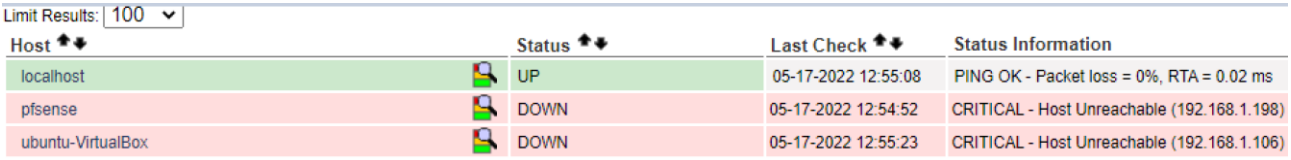
Saatavuuden valvonta

Saatavuuden valvontaa testattiin sammuttamalla pfsense ja ubuntu-palvelin. Valvonta toimii pingillä eli kun laite ei vastaa pingiin, toteaa Nagios laitteen olevan alhaalla. Lähtötilanteessa laitteet olivat päällä ja nagioksesta nähdään laitteiden olevan ylhäällä. Kuviossa 54 näkyy laitteiden tila.

Host	Status	Last Check
localhost	UP	05-17-2022 12:50:08
pfsense	UP	05-17-2022 12:47:18
ubuntu-VirtualBox	UP	05-17-2022 12:46:31

Kuvio 54. Laitteet ylhäällä nagioksessa

Seuraavaksi palvelimet sammutettiin virtualboxista. Nagios alkoi hälyttämään, että laitteet ovat saavuttamattomissa, kuten kuviosta 55 näkyy.



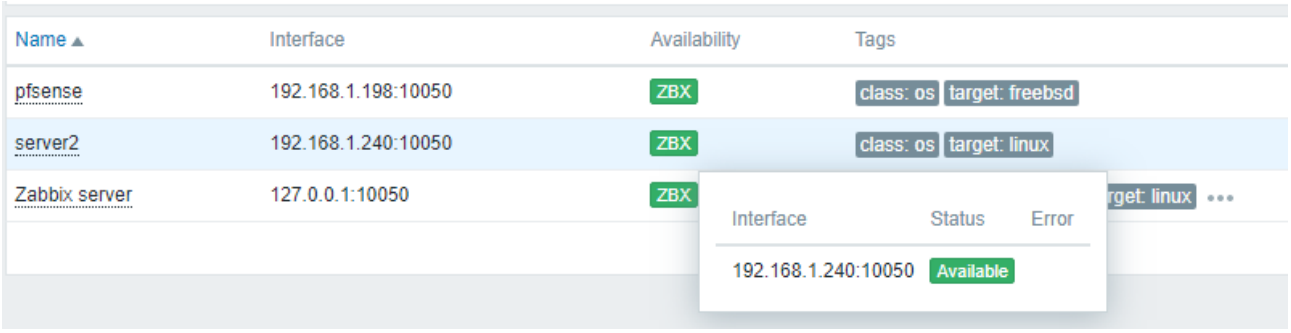
Kuvio 55. Laitteet saavuttamattomissa

7.3.2 Zabbix

Zabbixilla testattiin myös prosessorin ja levytilan valvontaa sekä laitteiden saatavuutta ja palvelun tilaa.

Palveluiden saatavuus

Saatavuutta testattiin sammuttamalla pfsense ja ubuntu-palvelin. Alussa koneet olivat päällä, kuten nähdään kuviosta 56. Availability sarakkeessa vihreä ZBX-merkki tarkoittaa, että laite on saavutettavissa.

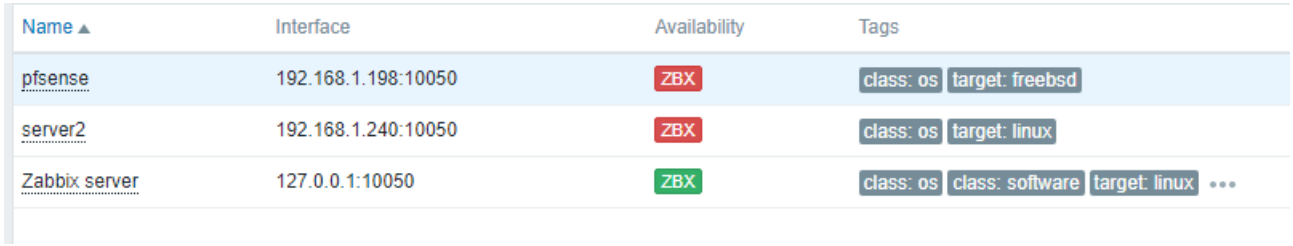


Kuvio 56. Laitteet saavutettavissa zabbixissa

Seuraavaksi laitteet sammutettiin. Zabbixin etusivulle syntyi hälytykset molemmista laitteista, kuten nähdään kuviosta 57.

Kuvio 57. Laitteet hälyttävät

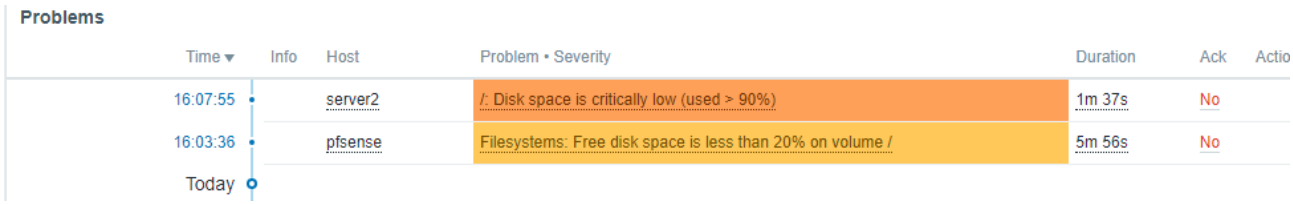
Myös näkymässä, jossa kaikki valvottavat laitteet ovat listattuna, näkyi että laitteet ovat alhaalla. Tämä nähdään kuviosta 58 alla.



Kuvio 58. Laitteet alhaalla

Levytilan valvonta

Testi suoritettiin samalla kaavalla, kuin Nagios coren kanssa. Laitteille luotiin tarpeeksi suuret tiedostot, jotta hälytysraja ylitty. Kuviossa 59 alla näkyy, että pfsense ja ubuntu-palvelin hälyttävät korkeaa levynkäyttöä.

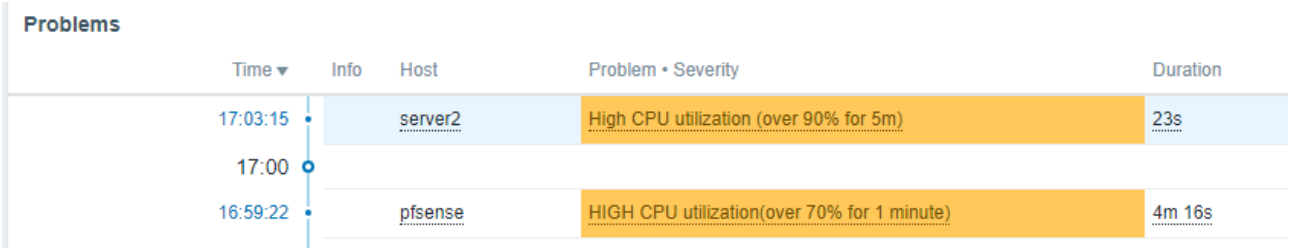


Kuvio 59. Levynkäyttö hälytykset zabbix

Prosessorin käytön valvonta

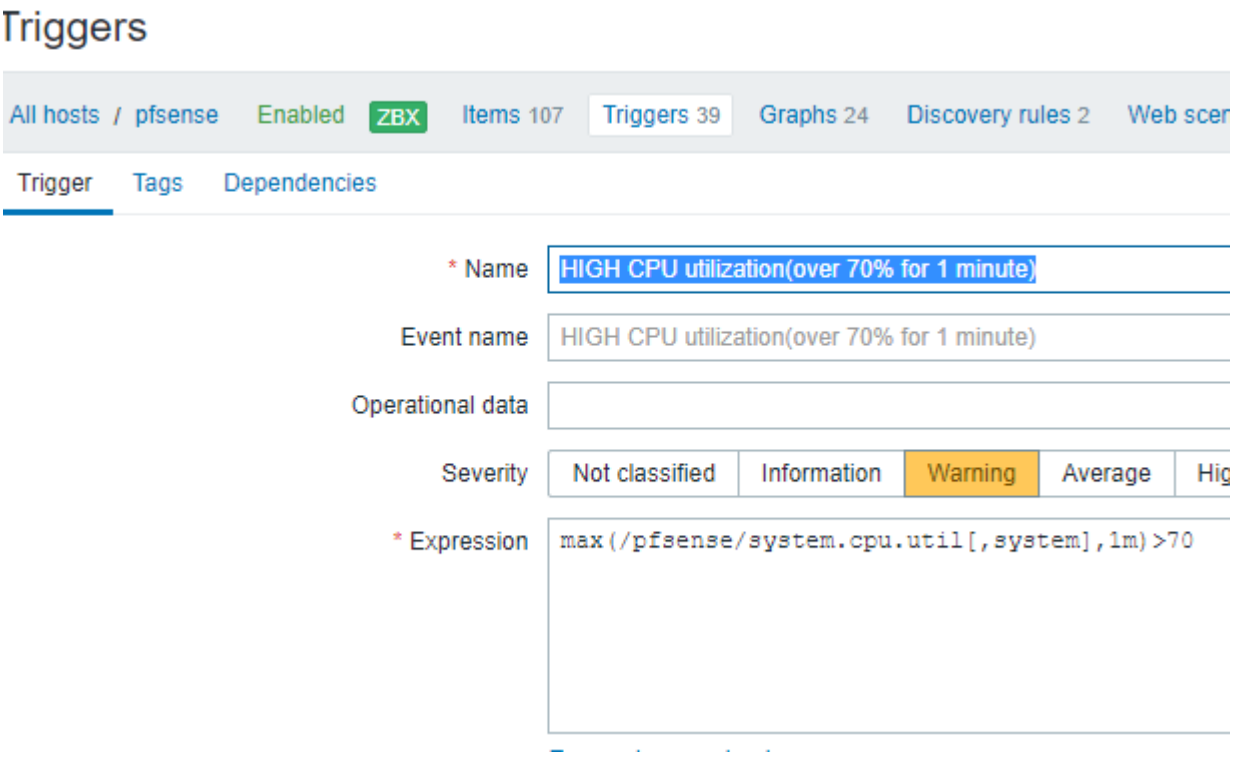
Tämäkin testi noudattaa samaa kaavaa kuin Nagioksella tehty vastaava testi. Pfsenselle ja ubuntu-

palvelimelle luotiin prosessorikuormaa siten, että käyttö on n. 100%. Alla olevasta kuviosta 60 nähdään, että Zabbix alkoi hälyttämään korkeaa prosessorin käyttöä molemmilla koneilla.



Kuvio 60. Prosessorinkäyttö-hälytykset

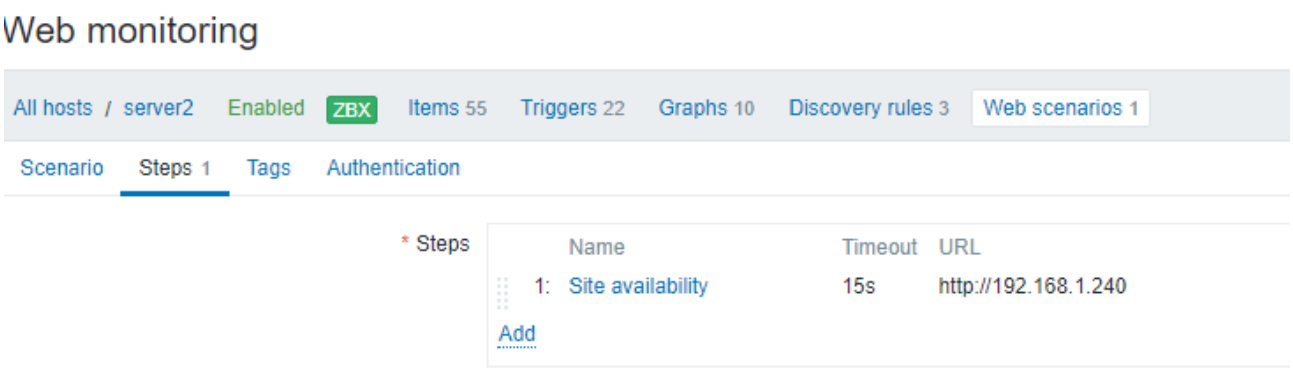
Hälytysraja ubuntu-palvelimelle oli 90%. Tämä on oletusasetus, joka tulee templatesta, johon palvelin määritettiin asennusvaiheessa. Pfsensen templatessa ei ollut oletuksena määritetty hälytyksiä prosessorin käytöstä, joten sitä varten luotiin asetus. Hälytysrajaksi asetettiin 70% ja ajaksi minuutti. Eli kun prosessorin käyttö on viimeisen minuutin ajalta yli 70%, siitä syntyy hälytys. Asetus näkyy kuviossa 61.



Kuvio 61. Pfsense prosessorin valvonta

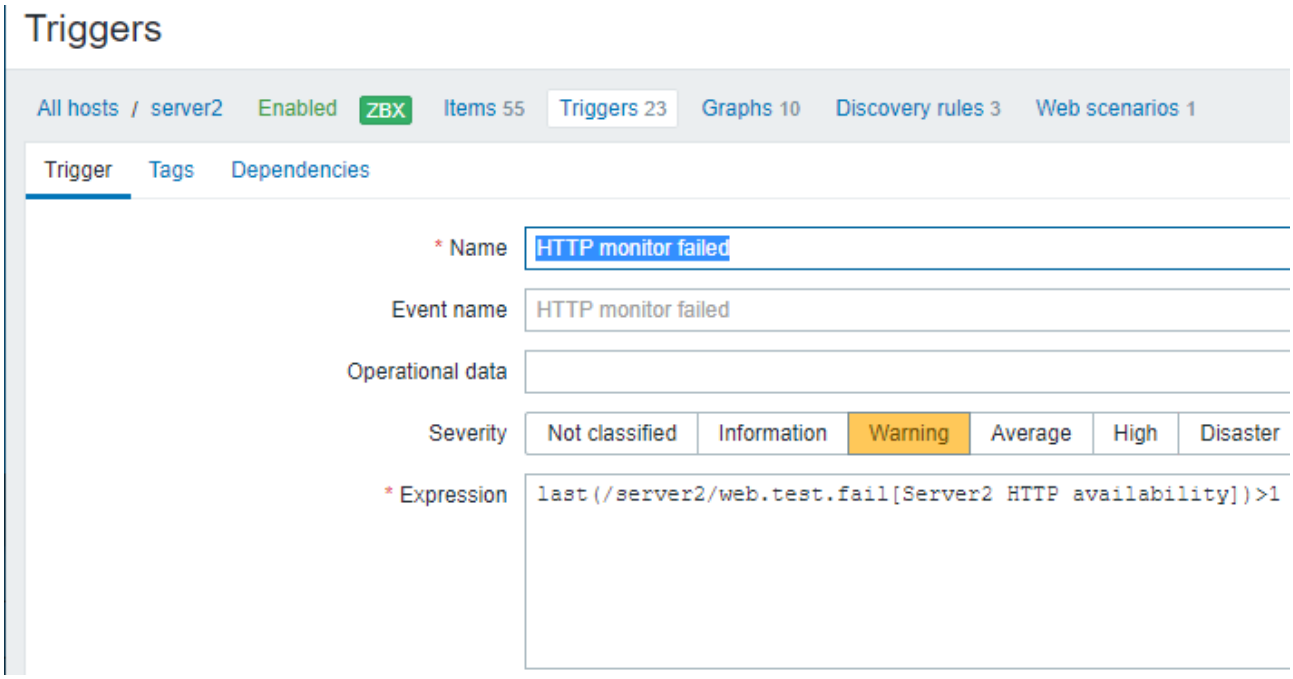
Palvelun valvonta ubuntulta

Ubuntulta valvottiin apache2 palvelun tilaa. Valvonta toimi niin, että Zabbix testaa yhteyttä HTTP:llä palvelimen IP-osoitteeseen porttiin 80, jota apache2-palvelu kuuntelee. Zabbixille tehtiin kuviossa 62 näkyvä määritys tätä varten.



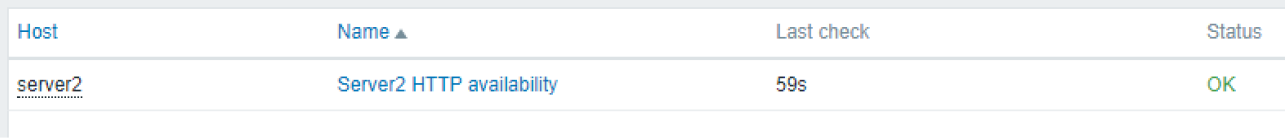
Kuvio 62. Zabbix web monitoring

Jotta tästä nousee hälytys, luotiin zabbixiin myös kuviossa 63 näkyvä asetus. Asetuksessa määritetään, että kun HTTP-testi epäonnistuu enemmän kuin kerran, siitä luodaan hälytys.



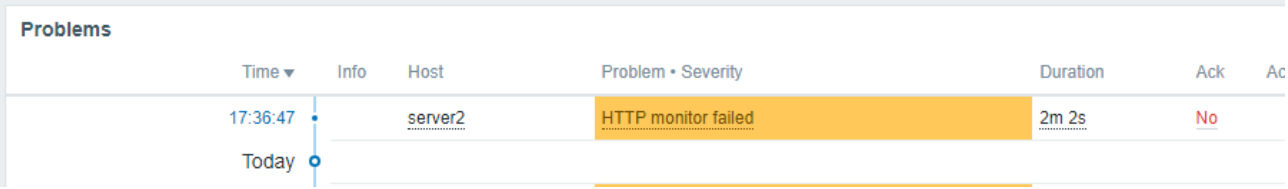
Kuvio 63. HTTP valvonnan hälytyksen asetus

Kuviossa 64 alla näkyy tilanne Zabbixissa, kun apache2-palvelu on päällä ubuntu-palvelimella. HTTP-valvonnan status on ok.



Kuvio 64. Apache2 palvelu on päällä

Seuraavaksi palvelu sammutettiin. Zabbix alkoi hälyttämään, kuten alla olevasta kuviosta 65 nähdään.



Kuvio 65. Apache palvelu sammutettu

8 Ohjelmistojen vertailu

Tehtyjen testien pohjalta voidaan todeta, että perus valvontaominaisuudet toimivat hyvin ja kuten pitääkin molemmissa sovelluksissa. Suurimmat erot tulivatkin esiin käytettävyydessä ja käyttöliittymissä.

Zabbixin hallinta tapahtuu sen graafisesta käyttöliittymästä, mikä on huomattavan paljon käyttäjäystävällisempää, kuin hallinta komentokehotteelta, kuten Nagios coren hallinta. Lisäksi Zabbixin käyttöliittymä tarjoaa kattavamman yleisnäkymän verkon laitteista ja niiden hälytyksistä. Näkymä on oletuksena jo ihan käyttökelpoinen ja selkeä ja sitä pystyy muokkaamaan reilusti, jolloin siitä saa tehtyä enemmän käyttäjän mieltymysten mukaisen. Nagioksen käyttöliittymä puolestaan on hyvin yksinkertainen ja vanhanaikaisen oloinen. Siinä ei myöskään oletuksena ole yhtä ja selkää päänäkymää hälytyksille ja laitteille, vaan ne löytyy eri valikoiden alta. Tiedot ovat siis löydettävissä, mutta ne voisi olla esillä selkeämminkin ja koostetusti yhdellä sivulla.

Liitteessä 2 on vielä yhteenvetoa ja vertailua sovelluksien ominaisuuksista (Keary 2020).

9 Pohdinta

Opinnäytetyössä testattiin ja vertailtiin kahden ilmaisen verkonvalvontasovelluksen, Zabbixin ja Nagios Coren toimintaa. Tavoitteena oli selvittää näiden soveltuvuutta verkonvalvontaan ja tehdä vertailua niiden ominaisuuksista. Sovelluksien toimintaa testattiin työtä varten pystytetyssä virtuaalisessa ympäristössä ja kummallekin sovellukselle tehtiin saman tyyppiset testit. Testien pohjalta saadun käyttökokemuksen myötä suoritettiin vertailua.

Testaukset onnistuivat hyvin, halutut testit saatiin onnistuneesti ajettua ja molemmat sovellukset suoriutuivat niistä odotetulla tavalla. Testiskenaariot olivat mahdollisimman realistisia, joten tuloksia on mahdollisimman helppo rinnastaa oikeisiin tilanteisiin. Testien onnistuneiden tuloksien perusteella voidaan sanoa, että sovellukset soveltuvat siihen, mihin ne ovat suunniteltukin, eli yritysverkkojen valvontaan. Vertailun kannalta mieleenpainuvin tulos oli sovelluksien käytettävyys. Zabbix oli huomattavan paljon modernimman oloinen ja miellyttävämpi käyttää. Molemmista kuitenkin löytyy suurin piirtein samat ominaisuudet, joten suuria eroja toiminnallisuuksissa ei ole.

Yllätyksenä tuli se, miten paljon ominaisuuksia ilmaisista ohjelmista voikaan löytyä. Työn aikataulu oli kiireellinen, joten testien kohteeksi pääsi vain olennaisimmat ja selkeimmin testattavissa olevat valvontaominaisuudet. Jos aikaa olisi ollut enemmän, olisi voitu suunnitella ja suorittaa kattavammat testaukset ja pystyttää enemmän oikeaa yritysverkkoa simuloiva ympäristö. Olisi myös ollut hyvä ja mielenkiintoakin lisäävä asia, jos työssä olisi ollut mahdollisuus käyttää oikeita laitteita, kuten esim. kytkimiä ja reitittimiä.

Lähteet

Clavel, T. 2018. What Is NetFlow? How NetFlow Works and Why to Use It. Blogikirjoitus blog.gigamon -verkkosivustolla. Viitattu 30.4.2022. https://blog.gigamon.com/2018/01/08/what-is-netflow/.

Dooley, K. 2020. What Is Syslog and How Does It Work? Artikkeli auvik -sivustolla. Viitattu 29.4.2022. https://www.auvik.com/franklyit/blog/what-is-syslog/.

Download and install Zabbix. N.d. Dokumentaatiota zabbixin verkkosivuilta. Viitattu 10.5.2022. https://www.zabbix.com/download?zabbix=6.0&os_distribution=ubuntu&os_version=20.04_focal&db=mysql&ws=apache.

Easy way to load CPU / memory on Linux. N.d. Dokumentaatio linuxtut -verkkosivustolla. Viitattu 15.5.2022. https://linuxtut.com/en/8fba88debe66fa8d2b39/.

How To Monitor Remote Linux Systems With Nagios Monitoring Tool. 2019. Artikkeli itzgeek -verkkosivustolla. Viitattu 11.5.2022. https://www.itzgeek.com/how-tos/linux/centos-how-tos/monitor-remote-linux-system-with-nagios-3.html.

Install Nagios on Ubuntu 20.04. 2021. Artikkeli vultr -verkkosivustolla. Viitattu 10.5.2022. https://www.vultr.com/pt/docs/install-nagios-on-ubuntu-20-04.

Keary, T. 2020. Nagios Core vs Zabbix Comparison. Artikkeli comparitech -verkkosivustolla. Viitattu 18.5.2022. https://www.comparitech.com/net-admin/nagios-vs-zabbix/.

Karimi, S. 2020. What is the difference between agent and agentless monitoring? Artikkeli panopta -verkkosivustolla. Viitattu 17.5.2022. https://www.panopta.com/resources/agent-vs-agentless-monitoring/.

Kiarie, J. 2021. How to Add Linux Host in Zabbix Server for Monitoring. Artikkeli linuxtechi -verkkosivustolla. Viitattu 7.5.2022. https://www.linuxtechi.com/add-linux-host-zabbix-server-for-monitoring/.

Kumar, R. 2022. What is Zabbix and How it works? An Overview and Its Use Cases. Artikkeli devopsschool -sivustolla. Viitattu 1.5.2022. https://www.devopsschool.com/blog/what-is-zabbix-and-how-it-works-an-overview-and-its-use-cases/.

Monitor pfSense with nagios. 2019. Foorumikeskustelu serverfault -verkkosivustolla. Viitattu 12.5.2022. https://serverfault.com/questions/453715/monitor-pfsense-with-nagios.

Network monitoring definition. N.d. Artikkeli avinetworks -verkkosivustolla. Viitattu 27.4.2022. https://avinetworks.com/glossary/network-monitoring/.

What Is Nagios Core? N.d. Dokumentaatiota nagioksen verkkosivuilta. Viitattu 5.5.2022. https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/about.html.

What is Simple Network Management Protocol (SNMP)? N.d. Artikkeli thousandeyes -verkkosivustolla. Viitattu 28.4.2022. https://www.thousandeyes.com/learning/techtorials/snmp-simple-network-management-protocol.

What is SNMPv1, SNMPv2c, and SNMPv3? N.d. Artikkeli dpstele -verkkosivustolla. Viitattu 28.4. https://www.dpstele.com/snmp/v1-v2c-v3-difference.php.

What is SSH and how do I use it? N.d. Artikkeli ucl.ac.uk -sivustolla. Viitattu 17.5.2022. https://www.ucl.ac.uk/isd/what-ssh-and-how-do-i-use-it.

What is the Internet Control Message Protocol (ICMP)? N.d. Artikkeli cloudflare -verkkosivustolla. Viitattu 27.4.2022. https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/.

Zabbix - Monitoring PFSense using agent. N.d. Artikkeli techexpert -sivustolla. Viitattu 6.5.2022. https://techexpert.tips/zabbix/zabbix-monitoring-pfsense-agent/.

Liitteet

Liite 1. Syslog viestin toimintokenttä

Numerokoodi	**Toiminto**	**Käyttötarkoitus**
0	Kernel viestit	Unix kernel
1	Käyttäjätason viestit	Sovelluksien viestit
2	Sähköposti	Unix sähköposti
3	Järjestelmän palveluprosessit	Unix järjestelmän prosessit
4	Turvallisuus/autorisointi viestit	Unix autentikaatio ja autorisointi viestit
5	Syslogd luomat viestit	Syslog prosessi
6	Linjatulostin alajärjestelmä	Unix linjatulostin
7	Network news subsystem	Unix news system
8	UUCP subsystem	Unix-to-unix copy protocol
9	Clock daemon	
10	Security/authorization viestit	
11	FTP daemon	

12	NTP subsystem	
13	Log audit	
14	Log alert	
15	Clock daemon	
16-23	Local use 0-7	

Liite 2. Nagios coren ja Zabbixin ominaisuuksien vertailua

	Nagios Core	**Zabbix**
Web-käyttöliittymä	Tarjoaa tietoa laitteista ja niiden tilasta. Ei mahdollista konfigurointia. Ei muokattavissa.	Tarjoaa selkeän koostetun näkymän verkon laitteista ja hälytyksistä. Muokattavissa. Mahdollista konfiguroinnin.
Konfigurointi	Komentoriviltä	Web-käyttöliittymästä tai komentoriviltä
Visualisointi (esim. CPU graafi)	Ei oletuksena. Mahdollista ladata ominaisuus erikseen.	Luo graafeja oletuksena
Verkon laitteiden automaattinen löytäminen (engl. auto-discovery)	Kyllä	Kyllä
Protokollatuki	HTTP, FTP, SMTP, SNMP, POP3, SSH, MySQL	HTTP, FTP, SMTP, POP3, SSH, MySQL
Ilmoitukset	Email ja SMS	Email ja SMS