VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Kim Karvonen

VERKKOLAITTEIDEN VALVONTA

Palvelimien, reitittimien ja kytkimien valvonta Icinga 2:lla

Tekniikka
2021

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Kim Karvonen
Opinnäytetyön nimi	Verkkolaitteiden valvonta
Vuosi	2021
Kieli	suomi
Sivumäärä	49
Ohjaaja	Antti Virtanen

Tämä työ suoritettiin Kokkolan Halpa-Halli Oy:lle. Työ suoritettiin, koska HalpaHallilla oli tarve kehittää keskitettyä verkkolaitteiden valvontaa. Työllä pyrittiin saamaan keskeisimmät verkkolaitteet valvonnan alle, jotta ongelmatilanteet pystytään havaitsemaan ja paikantamaan nopeasti. Valvontaan liitettäviin laitteisiin kuuluvat palvelimet, reitittimet ja kytkimet.

Jo ennen työn aloitusta HalpaHallissa oli päätetty tutkia Icinga 2:n soveltavuutta keskitettyyn verkkolaitteiden monitorointiin, joten työ toteutettiin käyttäen Icinga 2:sta, joka on haarauma Nagios-valvontaohjelmasta. Icinga 2 on palvelimelle asennettava valvontajärjestelmä, joka hakee dataa laitteille asennetun agentin avulla tai muilla protokolilla. Icinga 2 toimii käyttäen yhtä tai useata pääpalvelinta, joilla ajetaan komentoja ja talletetaan data. Palvelimia valvotaan asentamalla agentti ja verkkolaitteita käyttäen SNMP-protokollaa.

Työn tuloksena on hajautettu valvontajärjestelmä, jolla valvotaan verkkolaitteiden tilaa. Osittain valvotaan myös palveluita, kuten verkkosivuja. Valvontajärjestelmällä pyritään nopeampaan ongelmatilanteiden ratkaisemiseen mahdollisimman aikaisessa vaiheessa ennen ongelman laajenemista.

Avainsanat verkkovalvonta, verkkolaitteet, SNMP, Icinga 2

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Kim Karvonen
Title	Monitoring of Network Devices
Year	2021
Language	Finnish
Pages	49
Name of Supervisor	Antti Virtanen

This thesis was made for Kokkolan Halpa-Halli Oy. The thesis was done because HalpaHalli had a need to develop a centralised monitoring of network equipment. The aim was to bring the most important network devices and servers under monitoring so that problems could be detected and located quickly.

HalpaHalli had already decided to investigate the applicability of Icinga 2 for centralised network device monitoring, so the thesis was carried out using Icinga 2, a fork of the Nagios monitoring software. Icinga 2 is a server-based monitoring system that retrieves data using an agent installed on devices or other protocols. Icinga 2 runs using one or more master servers to run commands and store data. Servers can be monitored by installing an agent and network devices using SNMP-protocol.

The result is a distributed monitoring system that monitors the status of network devices and servers. It also partially monitors services. The monitoring system aims at a faster resolution of problems as early as possible before the problem escalates.

Keywords Network monitoring, network devices, Icinga 2, SNMP

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

KUVA-, TAULUKKO- JA KEHYSLUETTELO

KÄSITTEET JA LYHENTEET

1 JOHDANTO 10

2 TYÖN ALKUTILA JA SEN JATKAMINEN 11

2.1 Verkonvalvonta alussa 11

2.2 Kokonaiskuva verkkolaitteista, palvelimista ja palveluista 11

2.3 Verkonvalvonnan kehittäminen 11

3 VERKONVALVONTAOHJELMISTOT 12

3.1 Nagios Core 12

3.2 Icinga 2 13

3.2.1 Masteri-, satelliitti- ja agenttirakenne 14

3.2.2 Masteri- ja agenttirakenne 15

3.2.3 Ilmoitukset / Hälytykset 16

3.2.4 Komennot 17

3.3 Icinga Web 2 19

3.4 Grafana 19

3.5 SNMP-protokolla 19

3.5.1 SNMP POLLING 20

3.5.2 SNMP TRAP 20

4 KEHITYSTYÖ 21

4.1 Infrastruktuurin selvittäminen 21

4.2 Arkkitehtuuri 21

4.3 Grafanan jatkokehitys 22

4.4 Ohjelmistojen asentaminen 23

4.4.1 Icinga 2 Masterin asentaminen 24
4.4.2 Icinga 2 Agentin asentaminen 25
4.4.3 Icinga Web 2 asentaminen 28
4.5 Tietokannat 30
4.5.1 MySQL 31
4.5.2 InfluxDB 31
4.6 Icinga Web 2 33
4.7 Icinga 2:n rakenne ja ilmoituksien raja-arvojen konfigurointi 36
4.7.1 Icinga 2:n rakenne 36
4.7.2 Icinga 2:n raja-arvojen konfigurointi 37
4.8 Verkkolaitteet 42
5 TULOKSET 44
5.1 Metriikkadatan visualisointi 44
5.2 Varoitusilmoitukset 45
6 JOHTOPÄÄTÖKSET 47
LÄHTEET 48

KUVA-, TAULUKKO- JA KEHYSLUETTELO

Kuva 1. Nagiosin toimintaperiaate 13

Kuva 2. Icingan hajautettu valvonta käyttäen satelliitteja 15

Kuva 3. Icingan hajautetun valvonnan periaate pelkillä agenteilla ja masterilla . 16

Kuva 4. Icingan lähettämiä ilmoituksia Slackiin webhookkien avulla..... 17

Kuva 5. Valvonnan arkkitehtuuri 22

Kuva 6. Grafanan kantakysely valikolla 23

Kuva 7. Grafanan kantakysely tekstillä, joka tukee regexiä. 23

Kuva 8. Icinga 2:n Windows-käyttöliittymä agentin asentamiseen 28

Kuva 9. InfluxDBn metriikkadatan säilytyspolitiikka..... 32

Kuva 10. Icinga Web 2 Hostgroups 34

Kuva 11. Icinga Web 2 Servicegroups..... 34

Kuva 12. Icinga Web 2 History Event Grid 35

Kuva 13. Icinga Web 2 Index Dashboard 35

Kuva 14. Icinga 2:n rakenne master-to-agent toteutuksessa..... 37

Kuva 15. Icinga 2 global-templates konfigurointitiedostot 38

Kuva 16. Icinga 2 hostien ja palveluiden konfigurointi. 39

Kuva 17. Icinga 2 Sääntöjen soveltaminen malleilla..... 40

Kuva 18. Icinga 2 hostien ja palveluiden ryhmittäminen. 41

Kuva 19. Palvelimen konfigurointi. 42

Kuva 20. Palvelin x:n datan visualisointi 45

Taulukko 1 Agenteilla ajettavat komennot 18

Kehys 1. Icinga 2:n palvelun käyttöönotto ja uudelleenkäynnistys 24

Kehys 2. Luodaan satunnainen kolmekymmentä merkkinen tiiviste..... 25

Kehys 3. Vakio muuttuja tiketin suolalle 25

Kehys 4. Icigan 2:n node wizardin aloitus..... 25

Kehys 5. Tiketin luonti agentille..... 26

Kehys 6. Agentilla ajettava wizardi 26

Kehys 7. Tiketin tiivisteen syöttäminen 26
Kehys 8. Masterin konfigurointien ja komentojen hyväksyminen 27
Kehys 9. Ladataan tarvittavat paketit MySQL-tietokantaa varten Icinga Web 2:lle 29
Kehys 10. Luodaan tietokanta ja annetaan tarvittavat oikeudet sille. 29
Kehys 11. Icinga 2 IDO:n skeeman ajo. 29
Kehys 12. IDO-palvelun käyttöönotto 29
Kehys 13. Apache 2-verkkopalvelimen asennus 30
Kehys 14. Icinga 2 APIn asennus 30
Kehys 15. InfluxDBn asennus 31
Kehys 16. InfluxDBn tietokanta ja säilytyskonfigurointi 33
Kehys 17. Icinga hostgroup konfigurointi 33

KÄSITTEET JA LYHENTEET

Agentti	Ohjelmistoagentti on tietokoneohjelma, joka tekee käyttäjän puolesta haluttuja toimenpiteitä.
CSR	Certificate Signing Request, varmenteen allekirjoituspyyntö
ERP	Enterprise Resource Planning on tärkeimpien liiketoimintaprosessien toiminnanohjausjärjestelmä
Hash	Tiiviste tai hajautusarvo, joka tarkoittaa datan tiivistämistä pienempään tilaan, että voidaan verrata alkuperäisiä datoja niiden tiivisteiden avulla.
HTTP	Hypertext Transfer Protocol, protokolla, jota käytetään tiedonsiirtoon.
IDO	Icinga Data Output on Icinga 2:n ominaisuus, joka huolehtii kaikkien konfigurointi- ja tilatietojen viemisestä tietokantaan
IETF	Internet Engineering Task Force, Internet-protokollien standandoinnista vastaava organisaatio
MIB	Management Information Base on virtuaalinen tietokanta, jota käytetään SNMP-protokollassa.
Master	Icinga 2:ssa nimitys, jota käytetään pääpalvelimelle.
Node	Solmupiste tai solmu on joko uudelleenjakelupiste tai tiedonsiirron päätepiste riippuen asiayhteydestä.
OID	Object Identifiers, yksilöintitunnus
Regex	Regular expression käännettynä säännöllinen lauseke on joukko merkkejä, joilla voidaan tarkistaa tai muotoilla käyttäjän syöte.
REST API	Representational State Transfer on HTTP-protokollaan perustuva arkkitehtuurimalli ohjelmointirajapintojen toteuttamiseen.

RFC	Request for Comments, IETF:n julkaisemia standardeja
Salt	Käsite kryptografiassa eli salakirjoituksessa satunnaiselle merkkijonolle, jota käytetään hashausta varten.
Slack	Organisaation sisäiseen viestintään suunniteltu pikaviestintäsovellus.
SNMP	Simple Network Management Protocol, verkkojen hallinnassa käytetty tietoliikenneprotokolla.
SSL	Secure Sockets Layer, tietoverkkosalausprotokolla
TCP/IP	Transmission Control Protocol / Internet Protocol on internetin arkkitehtuurin kuvaamisessa käytetty tietoliikenneverkkojen viitemalli. Vastaa kahden laitteen välisestä tiedonsiirrosta ja huolehtii myös kadonneiden pakettien uudelleenlähetyksestä.
UDP	User Datagram Protocol, yhteydetön tietoliikenneprotokolla
UPS	Uninterruptible Power Supply, eli varavirtalähte
Webhook	Webhook on käyttäjän määrittelemä HTTP-kutsu, jotka käynnistyvät tietyistä tapahtumista.

1 JOHDANTO

Tämä opinnäytetyö tehtiin Kokkolan Halpa-Halli Oy:n IT-osastolle, jossa heillä on tarvetta sisäverkossa olevien verkkolaitteiden, palvelimien ja palveluiden valvonnalle. HalpaHallilla on verkkolaitteita jokaisessa myymälässä (joita on 35kpl), logistiikkakeskuksella ja konttorilla, joten laitteita on yhteensä lähes satakunta.

Verkonvalvontaa toteutetaan osana verkon ylläpitoa. Mitä laajempi verkko, sitä suurempi tarve on nykyaikaisille työkaluille ja järjestelmille verkonhallintaan ja -valvontaan.

Tavoitteena on tehdä verkonvalvonnasta mahdollisimman yksinkertaista. Verkkolaitteita ja niiden tilaa voidaan helposti seurata ja tarkastella ohjelmilla luoduilla näkymillä. Verkonvalvonnan yksinkertaisuutta edistävät laitteiden varoitus- ja kriittisen tilan ilmoitukset. Työ toteutettiin käyttäen Icinga 2:ta, joka on ilmainen avoimen lähdekoodin ohjelmisto, joka tarjoaa helposti liitettäviä lisäosia, jotka edistävät datan visualisointia ja tilojen tarkastelua keskitetyillä nettisivuilla.

2 TYÖN ALKUTILA JA SEN JATKAMINEN

Kuten johdannosta selviää, oli HalpaHallilla osittainen valvonta jo aluillaan ja minun tehtäväni oli jatkaa kyseistä projektia. Projektissa oli tavoitteena ottaa kaikki HalpaHallin hallitsemat palvelimet, reitittimet ja kytkimet valvontaan.

2.1 Verkonvalvonta alussa

HalpaHalli oli jo toteuttanut osittaisen master-to-agent-mallin. Valvottiin muutamalta palvelimelta niiden kuormituksia ja niitä visualisoitiin käyttäen Grafanaa. Icingan-metriikkadataa säilöttiin InfluxDB-aikasarjatietokantaan.

Master-palvelin oli asennettu virtuaaliselle Linux-palvelimelle, joka käyttää Debian 11 Bullseye Linux-jakelupakettia.

2.2 Kokonaiskuva verkkolaitteista, palvelimista ja palveluista

HalpaHallilla on verkkolaitteita ja palvelimia logistiikkakeskuksella, konttorilla ja myymälöissä, joten verkosto on erittäin hajautettu. Palvelimia on fyysisiä sekä virtuaalisia.

Osa ohjelmista ajetaan virtuaalipalvelimilla eikä fyysisillä palvelimilla. Ohjelmistot ja ohjelmat ovat pääosin Windows-sovelluksia, mutta on myös merkittävä osa web-palveluita, joita käytetään selaimella ja loput ovat Linux-sovelluksia.

2.3 Verkonvalvonnan kehittäminen

Työssä haluttiin erityisesti keskittyä siihen, että valvotaan sisäverkon sisältöä, josta ollaan itse vastuussa. Ilmoitukset olivat myös hyvin tärkeitä, jotta voidaan ongelmatilanteisiin reagoida hyvissä ajoin.

Tehtävänä oli lisätä jäljellä olevat palvelimet ja verkkolaitteet. Näiden lisäksi, koska kytkimiä ei ollut etukäteen valvottu, piti selvittää miten kytkimet saadaan valvonnan piiriin, ja miten niistä saadaan metriikkadataa ja ilmoituksia.

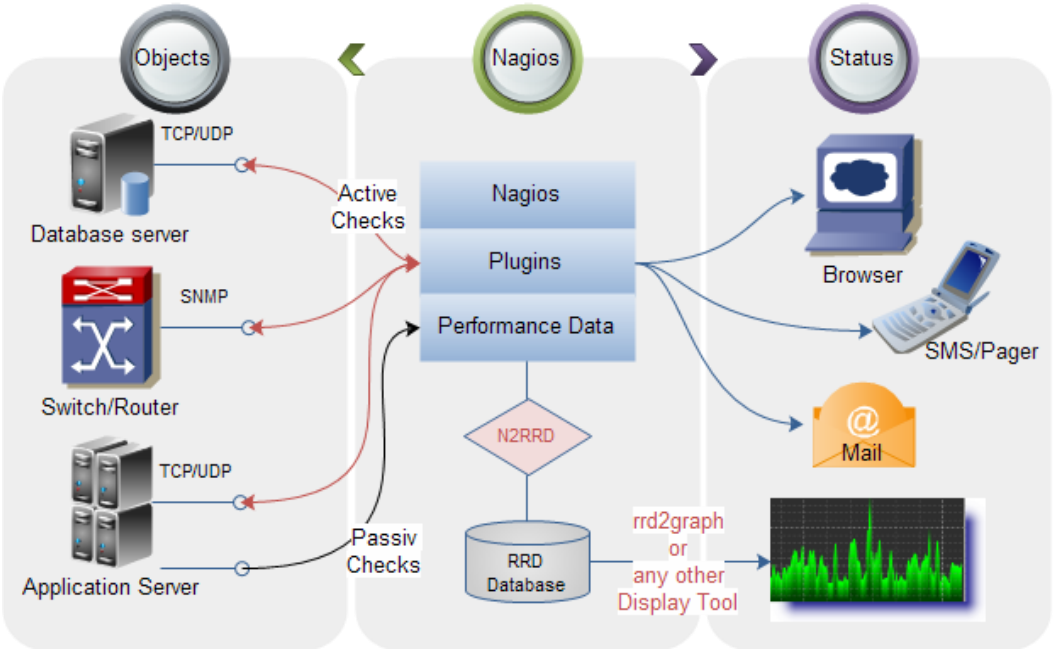
3 VERKONVALVONTAOHJELMISTOT

Verkonvalvontaohjelmistoja on olemassa useita ja tässä työssä keskityttiin Icinga 2:en, joka on suosittu maailmanlaajuisesti. Käytettiin tässä työssä Icinga 2:sta, joka on aikoinaan haarautettu Nagiosta. Tultiin tähän johtopäätökseen, koska Nagios vaatii enemmän työtä perusasioissa siihen nähden kuinka paljon Icinga 2 tekee valmiiksi.

3.1 Nagios Core

Nagios Core on aiemmin tunnettu Nagiosina, nimi vaihdettiin vuonna 2009. Nagios on ilmainen avoimen lähdekoodin ohjelmisto, joka valvoo järjestelmiä, verkostoja ja infrastruktuureja. Nagios tarjoaa valvontaa ja hälytyksiä palvelimille, kytkimille, sovelluksille ja palveluille. [1] Kuvasta 1 selviää Nagiosin toimintaperiaate. Icinga 2:n toimintaperiaate on sama. Avataan toimintaperiaatetta Icinga 2:n yhteydessä.

[1] SNMP selityksiä. Viitattu 25.7.2021. https://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/SNMP.html



Kuva 1. Nagiosin toimintaperiaate[2]

3.2 Icinga 2

Icinga haarautui aikoinaan yllä mainitusta Nagios Coresta. Kuten Nagios Core on myös Icinga ilmainen avoimen lähdekoodin ohjelmisto, jolla voidaan valvoa verkkoa ja sen laitteita. Molemmat tarjoavat ilmoituksien lähetykset sähköpostiin ja kännykkään, mutta molemmat tarvitsevat kolmannen osapuolen lisäosan, jotta ilmoitukset saadaan erilliseen ohjelmaan, kuten työssä toivottuun Slackiin. [3]

Perusvalvonta on erittäin nopea ottaa käyttöön Icingalla verrattuna Nagiosiin.

Icinga 2 toteutetaan käyttäen hajautettua valvontaa. Hajautettu valvonta tarkoittaa, että valvonta-agentteja on hajautettu ympäri valvottavaa verkostoa. Icingan

[2] Nagiosin toimintaperiaate esitettynä kuvassa. Viitattu 22.4.2021. https://upload.wikimedia.org/wikipedia/commons/1/1a/Monitoring.png
[3] Mikä on Icinga 2? Viitattu 22.4.2021. https://icinga.com/docs/icinga-2/latest/

agentit lähettävät kerätyn datan satelliitille ja satelliitti lähettää sen masterille, tai agentti voi lähettää datan suoraan masterille.

Icinga tallentaa raportoitua dataa jatkuvasti haluttuun aikasarjatietokantaan kuten InfluxDB, joka valittiin tähän työhön. Icinga pystyy hankkimaan kyseisten resurssien tietoja Linux- ja Windows-laitteilta, kunhan niihin on asennettu agentti.

Icinga hyödyntää agentteja hankkimaan rautatason tietoja Linux- ja Windows-laitteilta. Muut tiedot voidaan hankkia ilman agentteja, kuten verkkolatenssi ja SSL-sertifikaatin voimassaolo.

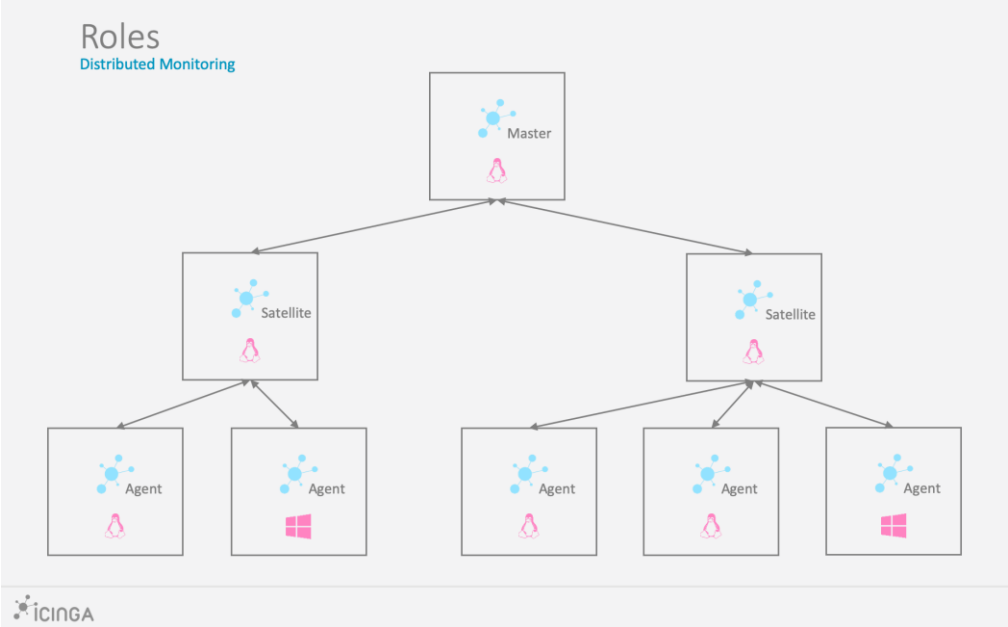
Icingalla voidaan myös asettaa komennoille raja-arvoja, jotka ylittäessä se lähettää hälytyksen. Hälytyksien tiheyttä ja kriittisyyksiä voidaan säätää raja-arvojen avulla. Kriittisyyden perusteella voidaan myös asettaa minne ja keille ilmoitus lähetetään.

3.2.1 Masteri-, satelliitti- ja agenttirakenne

Satelliitti voidaan asentaa pääpalvelimen ja agentin väliin (**Kuva 2.**). Satelliitin suurin etu on, että jos master on väliaikaisesti tavoittelematon, toimii satelliitti silti ja säilöö dataa ja, kun yhteys palautuu, puskee satelliitti kaiken datan takaisin masterille.[4]

Tässä työssä satelliitteja ei käytetty hyödyksi vaan käytettiin agentilta suoraan masterille lähestymistapaa (lisää otsikossa 3.3.3). Jos oltaisiin käytetty satelliitteja, oltaisiin se toteutettu siten, että myymälöiden palvelimet olisivat satelliitteja, joista sitten satelliitit lähettävät datan takaisin masterille.

[4] Icinga 2 Roles: Master, Satellites and Agents. Viitattu 26.4.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#roles-master-satellites-and-agents

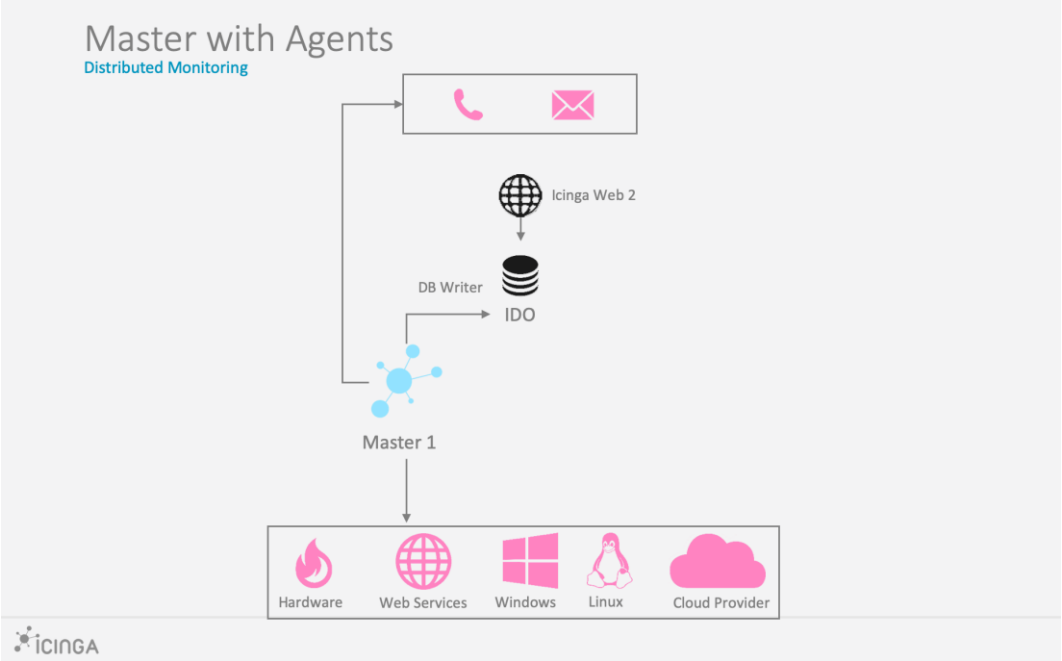


Kuva 2. Icingan hajautettu valvonta käyttäen satelliitteja[4]

3.2.2 Masteri- ja agenttirakenne

Masteri- ja agenttirakenteessa yksittäinen master-solmupiste ajaa tarkastuksen ajoitusohjelmaa, ilmoituksia ja IDO-tietokannan taustajärjestelmää ja suorittaa agenttien tarkistukset, milloin agentti palautuu. (**Kuva 3.**).[5]

[5] Icinga 2 Master with Agents. Viitattu 12.5.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#master-with-agents



Kuva 3. Icingan hajautetun valvonnan periaate pelkillä agenteilla ja masterilla[5]

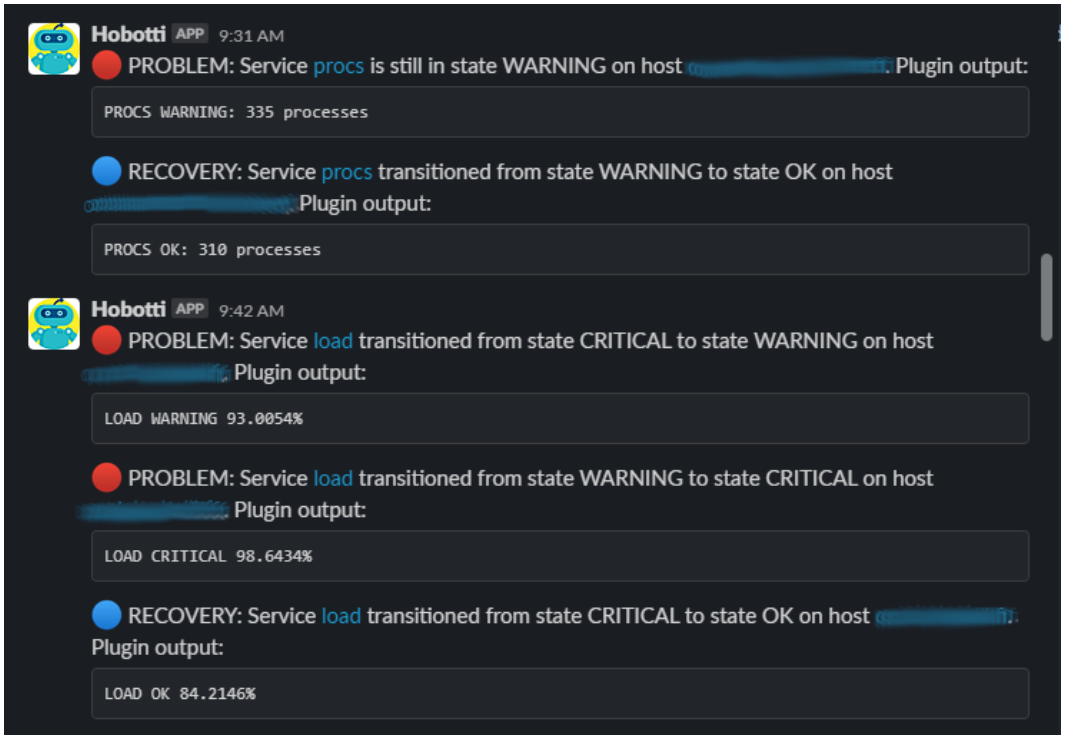
3.2.3 Ilmoitukset / Hälytykset

Icingalla pystytään seuraaman verkkolaitteiden resursseja ja tehdä hälytyksiä niille asetetuiden raja-arvojen perusteella. Tässä työssä käytetiin hälytyksiin sähköpostia ja Slackiä, joka on organisaatioiden viestintään suunnattu pikaviestintäohjelma.

Icinga tarjoaa dokumentaation hälytyksien käyttöönottoon, joka teki tästä prosessista yksinkertaista. Ohjeistuksen avulla oli myös helppoa säätää hälytyksien raja-arvoja.

Icingan yhteisöfoorumeilta löytyy ilmainen liitännäisohjelma, joka lähettää ilmoituksia aiemmin mainittuun Slack-pikaviestintäohjelmaan käyttäen Slackin webhookkeja (**Kuva 4.**).

Icingalla voidaan konfiguroida minkä tyyppisistä ilmoituksista lähtee viesti, tyyppejä ovat palautunut, varoitus ja kriittinen. Samalla tavalla voidaan konfiguroida liitännäinen. Haluttiin jokaisesta ilmoitustyypistä viestin, koska haluttin tietää myös milloinka agentti palautuu normaaliin tilaan.



Kuva 4. Icingan lähettämiä ilmoituksia Slackiin webhookkien avulla

Icinga tarjoaa myös mahdollisuuden lähettää SMS-viestejä, mutta tässä tapauksessa ei nähty tekstiviestijä tarpeellisiksi.

3.2.4 Komennot

Taulukossa 1 on listattu yleisimmät komennot, joita käytettiin. Windows ja Linux vaativat osittain eri komentoja niiden erojen takia.[6]

[6] Icinga 2 Template Library. Viitattu 20.8.2021. https://icinga.com/docs/icinga-2/latest/doc/10-icinga-template-library/

Taulukko 1. Agenteilla ajettavat komennot

Komennon nimi	Selitys
Hostalive	Sama kuten ping, eli testaa määritetyn laitteen saavutettavuutta.
Mem (Linux)	Tarkistaa keskusmuistin käytön. Palautetut arvot ovat käytetty, vapaana ja välimuistissa. Hälyttää jos asetetut raja-arvot ylittyvät.
Memory-windows	Tarkistaa keskusmuistin käytön. Palauttaa paljonko muistia on vapaana. Hälyttää jos asetetut raja-arvot ylittyvät.
Disk	Tarkistaa paljonko massamuistia on jäljellä. Hälyttää jos asetetut raja-arvot ylittyvät.
Http	Testaa onko HTTP-palvelu ylhäällä ja tarkistaa myös sisältääkö tietyn sanan tai lauseen. Hälyttää jos asetetut raja-arvot ylittyvät.
Users	Tarkistaa montako käyttäjää on kirjautunut kyseiseen järjestelmään. Hälyttää jos asetetut raja-arvot ylittyvät.
Procs	Tarkistaa montako prosessia on käynnissä. Hälyttää jos asetetut raja-arvot ylittyvät.
Http (http_check)	Tarkistaa sertifikaatin tiedot. Hälyttää jos asetetut raja-arvot ylittyvät.

3.3 Icinga Web 2

Icinga Web 2 on PHP-ohjelmistokehys. Icinga tarjoaa helppokäyttöisen verkkosivun kyseisen ohjelmistokehyksen päälle. Jotta saadaan enemmän toiminnallisuuksia, tarvitaan valvontamoduuli, jonka avulla saadaan käyttöliittymä valvontaan.[7]

3.4 Grafana

Grafana on Grafana Labsin luoma avoimen lähteen visualisointiohjelma, jonka avulla voidaan luoda kaavioita useiden datalähteiden, kuten InfluxDB:n avulla, jota käytettiin tässä työssä tallettamaan dataa.[8]

Grafanan avulla voidaan arvioida, milloin laitteiden hälytysraja-arvot alkavat lähestymään. Tästä on myös hyötyä tilanteissa, joissa ilmoitukset eivät kerkeä lähteä, mutta käyttäjät silti ovat ilmoittaneet hitauksista, joten voidaan tutkia alkuperää. Voidaan myös etsiä millä ajanjaksolla esimerkiksi prosessien määrä oli noussut ja sen avulla lähteä tutkimaan syvemmin mistä se voisi johtua.

3.5 SNMP-protokolla

SNMP eli Simple Network Management Protocol on protokolla, jolla kerätään ja muokataan tietoja TCP/IP-verkkojen laitteista. SNMP toimii UDP-protokollan päällä.[9] SNMP sallii laitteiden välisen kommunikaation, vaikka ne ovat eri laitteistoja ja käyttävät eri ohjelmistoja.

---

[7] Icinga Web 2. Viitattu 25.7.2021 https://icinga.com/docs/icinga-web-2/latest/doc/01-About/

[8] Icinga 2:n integraatio Grafana. Viitattu 25.7.2021 https://icinga.com/products/integrations/grafana/

[9] SNMP selityksiä. Viitattu 25.7.2021. https://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/SNMP.html

Nimellä managers tarkoitetaan palvelinta ja nimellä agentti tarkoitetaan laitetta, jolta kerätään data.

Agentit paljastavat datan hallittavista järjestelmistä muuttujina. Näitä muuttujia kutsutaan OID eli Object Identifiers. Käytettävät muuttujat on järjestetty hierarkioihin. Nämä hierarkiat tunnetaan nimellä MIB eli Management Information Base. MIB:t kuvaavat laitteen osajärjestelmän hallintatietojen rakenteen.

Käytetty liitännäinen, joka kyselee kytkimiltä niiden dataa käyttää vakiona SNMP:n versiota SNMPv2c. SNMPv2c määritellään IETF:n RFC:ssä RFC 3416.[10] Liitännäinen tukee myös SNMP:n versiota 3. SNMPv3 ei lisää tai muuta SNMP-protokollaa verrattuna SNMPv2c:hen. SNMPv3 kuitenkin tuo lisättyä kryptografiaturvallisuutta, mutta emme nähneet sitä kovin tarpeellisena työhön nähden, koska kaikki liikenne kulkee sisäverkossa.

3.5.1 SNMP POLLING

Pollaus tai kysely eli GET-viesti tarkoittaa, että manager lähettää kyselyn agenteille tietyin aikavälein. Hyödynnettiin SNMP pollausta tässä työssä kyselemään kytkimiltä niiden tiloja. Kuvasta 1 kohta SNMP.[9]

3.5.2 SNMP TRAP

Trap-viestillä tarkoitetaan tilannetta, jossa agentti lähettää managerille viestin muuttuneesta tilanteesta.[9] Tätä käytetään usein verkonvalvonnassa tilanteissa, joissa halutaan saada tieto heti, kun verkkolaite menee kriittiseen tilaan.

---

[10] Douglas R. Mauro & Kevin J. Schmidt. (2001). Essential SNMP (1st ed.). Sebas-topol, CA: O'Reilly & Associates. https://doc.lagout.org/network/Essential%20SNMP%202001.pdf

4 KEHITYSTYÖ

Työssä kehityksen kohteina oli lisätä kaikki verkkolaitteet eli palvelimet, reitittimet ja kytkimet valvontaan. Verkkolaitteet eivät olleet kattavasti keskitetyssä valvonnassa, joten piti selvittää, miten niistä saadaan tietoja ulos keskitettyyn sijantiin. Tähän löytyi lisäosa, joka käyttää SNMP-protokollaa kyselemään tietoja ja lähettämään ilmoituksia niiden perusteella.

Tarvittiin myös hyvä nimeämiskäytäntö verkkolaitteille. Todettiin, että työtä edeltävä nimeämiskäytäntö ei soveltunut tähän hyvin.

Haluttiin myös kehittää metriikkadatan visualisointia. Jatkettiin Grafanan käyttöä tähän, lisättiin eri näkymiä ryhmille ja yksittäisille palvelimille.

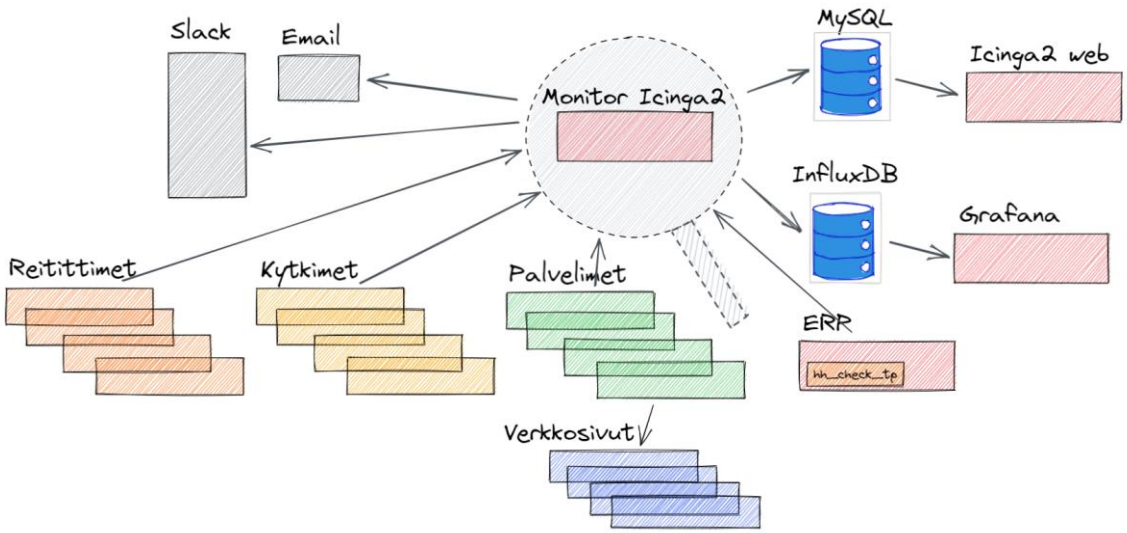
Merkittävin kehityksen kohde oli saada varoitusilmoituksia laitteista, kun ne käyttäytyvät epänormaalisti. Suurimmalla prioriteetilla oli kaikki palvelimet, joissa pyörii HalpaHallin sisäisiä palveluita ja pääliikenteen reitittimet.

4.1 Infrastruktuurin selvittäminen

Ensimmäisenä haasteena oli suunnitella hyvä nimeämiskäytäntö valvottaville laitteille. Palvelimet nimettiin itse palvelimen nimeämiskäytännön mukaan. Logistiikkakeskuksella hyödynnettiin kytkimien nimeämisessä niiden fyysistä sijaintia ja osaa laitteen nimestä. Myymälöiden kytkimet nimettiin myymälän numeron perusteella ja laitteen IP-osoitteen loppuosalla.

4.2 Arkkitehtuuri

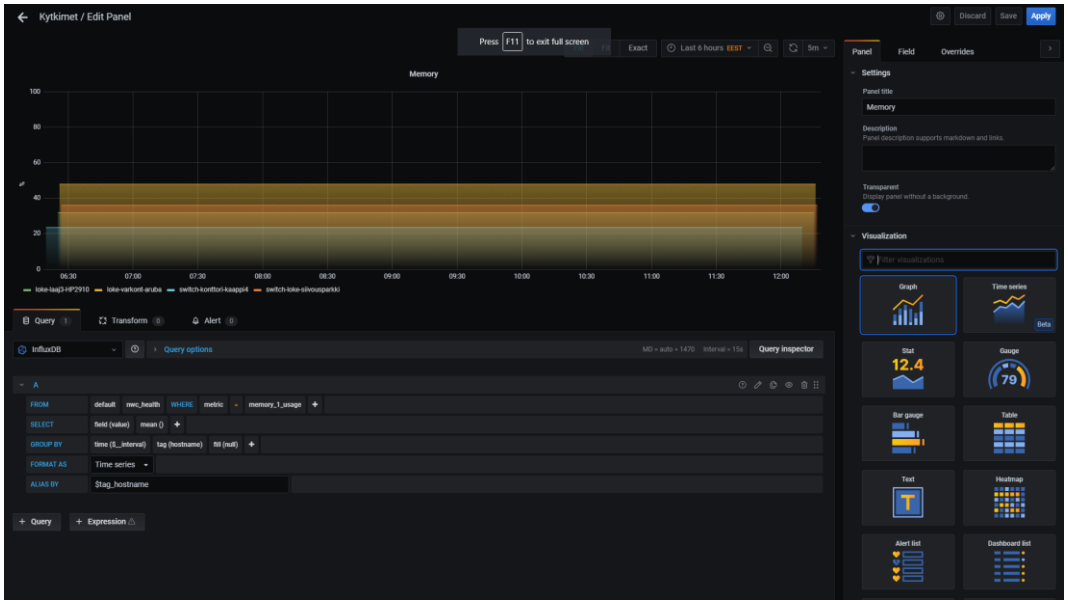
Kuvasta 5 nähdään, kuinka järjestelmä toimii kokonaisuudessaan. Laitteet, joille on asennettu agentti, lähettävät dataa masterille, josta masteri tekee päätökset mitä tehdään datalla. Data tallennetaan aina johonkin tietokantaan. Metriikkadata tallennetaan InfluxDBhen. Hälytykset ja ilmoitukset lähetetään tarpeen mukaan sähköpostiin ja Slackiin.



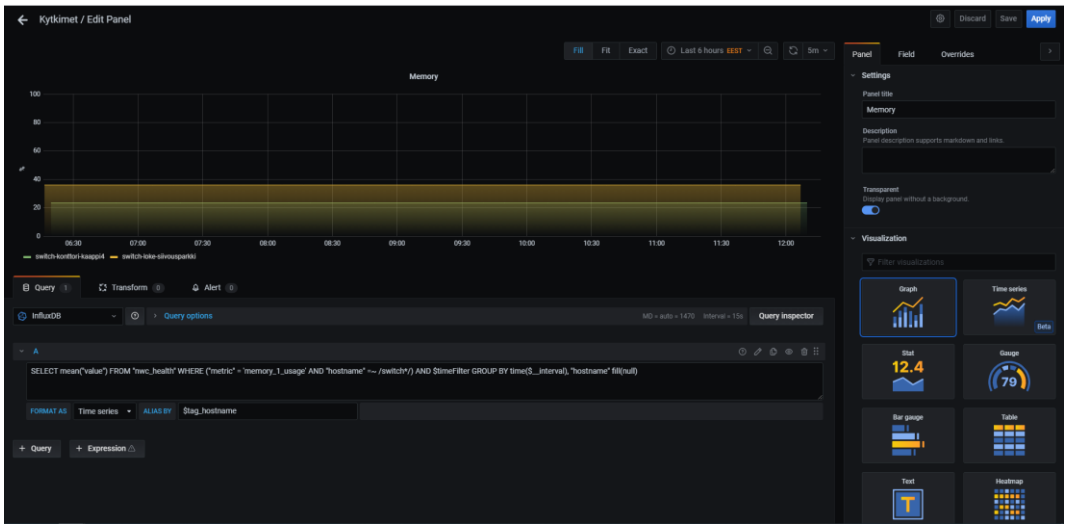
Kuva 5. Valvonnan arkkitehtuuri

4.3 Grafanan jatkokehitys

Käytettiin Grafanaa visualisoimaan dataa, joka löytyy InfluxDB-tietokannasta. Datan visualisointi toteutetaan tietokantakyseleillä. Grafana tarjoaa kyselyihin käyttöliittymässä valikon (**Kuva 6.)** tai tekstin monimutkaisimpia kyselyitä varten, joissa voidaan hyödyntää regex:iä. Kuten kuvassa 7 halutaan valita kaikki kytkimet, joista löytyy metriikkadataa muistin käytöstä ja nimessä on switch eli kytkin.



Kuva 6. Grafanan kantakysely valikolla



Kuva 7. Grafanan kantakysely tekstillä, joka tukee regexiä.

4.4 Ohjelmistojen asentaminen

Ohjelmien asentamiset olivat vaivattomia Icinga 2:n dokumentaation avulla. Icinga 2:n masterin ja agentin asentaminen palvelimelle eivät eroa paljoa toisistaan, koska tarvitsevat molemmat pohjana Icinga 2:n ja tarvittavat valvontalisäosat.

4.4.1 Icinga 2 Masterin asentaminen

Icinga 2:n masterin palvelimen käyttöjärjestelmä on pakko olla Linux-pohjainen. Icinga tukee useita Linux-jakelupaketteja eli distroja. Heidän tukemat jakelupaketit löytyvät asennusdokumentaatiosta. Tällä hetkellä tuettuja ovat Icinga 2 tukee Debian, Ubuntu, Raspbian, RHEL/CentOS, openSUSE ja SLES. Näiden lisäksi on yhteisö rakentanut tuen muutamille lisää, joista huomattavin ArchLinux. Tämän jälkeen valitaan sopiva jakelupaketti, jota halutaan käyttää. Tässä työssä valittiin Debian-paketin version 11 Bullseye.

Kun Icinga 2 on asennettu, pitää pääpalvelimelle asentaa liitännäiset, jotka ovat The Monitoring Plugins Project:n ylläpitämiä. Näiden liitännäisten paketti löytyy nimellä monitoring-plugins useilla distroilla.

Tiketin luonnissa luodaan CSR eli varmenteen allekirjoituspyyntö, joka authentikoidaan, kun käytetään tikettiä agentin asennusvaiheessa.[11]

Kun Icinga 2 ja tarvittavat liitännäiset on asennettu pitää Icinga 2 ottaa käyttöön ja käynnistää uudelleen komennoilla (**Kehys 1.**).

```
systemctl enable icinga2

systemctl restart icinga2
```

Kehys 1. Icinga 2:n palvelun käyttöönotto ja uudelleenkäynnistys

Luodaan salt eli suola, lisätään merkkijonoon ylimääräinen merkkijono myöhempiä agenttien lisäystä varten. Tämän avulla lasketaan masterin luoman asiakasohjelman tiketin tiiviste eli hash. (**Kehys 2.**)

[11] Icinga 2 Agent Setup on Linux. Viitattu 13.8.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#agentsatellite-setup-on-linux

```
openssl rand -base64 30
```

Kehys 2. Luodaan satunnainen kolmekymmentä merkkinen tiiviste

Lisätään suola Icinga 2:n vakioihin tiedostoon /etc/icinga2/constants.conf. (**Kehys 3.**)

```
const TicketSalt = ”…”
```

Kehys 3. Vakio muuttuja tiketin suolalle

Ajetaan Icinga 2:n node wizard-komento. Tämän vaiheen saa automatisoitua. (**Kehys 4.**)

```
icinga2 node wizard
```

Kehys 4. Icigan 2:n node wizardin aloitus

Tällä wizardilla konfiguroidaan masterin zone eli vyöhykkeen asetukset, kuten palvelimen nimi ja sertifikaatit yms.

Tämän jälkeen käynnistetään Icinga 2:n service eli palvelu uudelleen, jotta muutokset tulevat voimaan.

4.4.2 Icinga 2 Agentin asentaminen

Kuten masterin asentaminen, on myös agentin asentaminen yksinkertainen. Agentin asentamisessa on eroja riippuen kummalle käyttöjärjestelmälle, Windowsille vai Linuxille, agentti asennetaan. Huomattavin ero on, että Windowsilla agentti asennetaan käyttäen asennuspakettia, jossa on tarvittava Icinga 2 ja sen vaatimat liitännäiset. Linuxilla tehdään kuten masterin asentamisessa, eli ladataan Icinga 2:n paketti ja vaaditut liitännäiset.

Kun on aikaisemmat askeleet tehty, käydään tekemässä pääpalvelimella tiketti agentin liittämistä varten kehyksen 5 komennolla. Nimessä käytetään laitteen verkkonimeä.

```
icinga2 pki ticket --cn icinga2-agent1.localdomain
```

Kehys 5. Tiketin luonti agentille

Tiketistä lasketaan tiiviste suolan avulla. Otetaan talteen kyseisen komennon palauttama numerosarja ja syötetään se seuraavassa vaiheessa.

Tässä asennusvaiheessa tulee taas eroja Windowsin ja Linuxin välillä. Linuxilla ajetaan kehyksen 4 komento, joka aukaisee kehyksen 6 kyselyn. Noudetaan näitä asetuksia. Syötetään agentin verkkonimi ja masterin verkkonimi.

```
$ icinga2 node wizard

Please specify the common name (CN) [icinga2-agent1]: icinga2-agent1.localdomain

Master/Satellite Common Name (CN from your master/satellite node): master.localdomain

Parent certificate information:

 Version:          3

 Subject:          CN = icinga2-agent1

 Issuer:           CN = Icinga CA
```

Kehys 6. Agentilla ajettava wizardi

Syötetään masterilla luotu tiketin tiiviste. Tiiviste luodaan vihjeen mukaisella komennolla, joka on sama kuin kehyksen 5.

```
Please specify the request ticket generated on your Icinga 2 master (optional).

 (Hint: # icinga2 pki ticket --cn icinga2-agent1.localdomain): tiketin tiiviste
```

Kehys 7. Tiketin tiivisteen syöttäminen

Konfigurointien jälkeen hyväksytään ylemmän tason solmulta tulevat konfiguroinnit ja komennot eli tässä tapauksessa masterin tuomat konfiguroinnit ja komennot. (**Kehys 8.**)

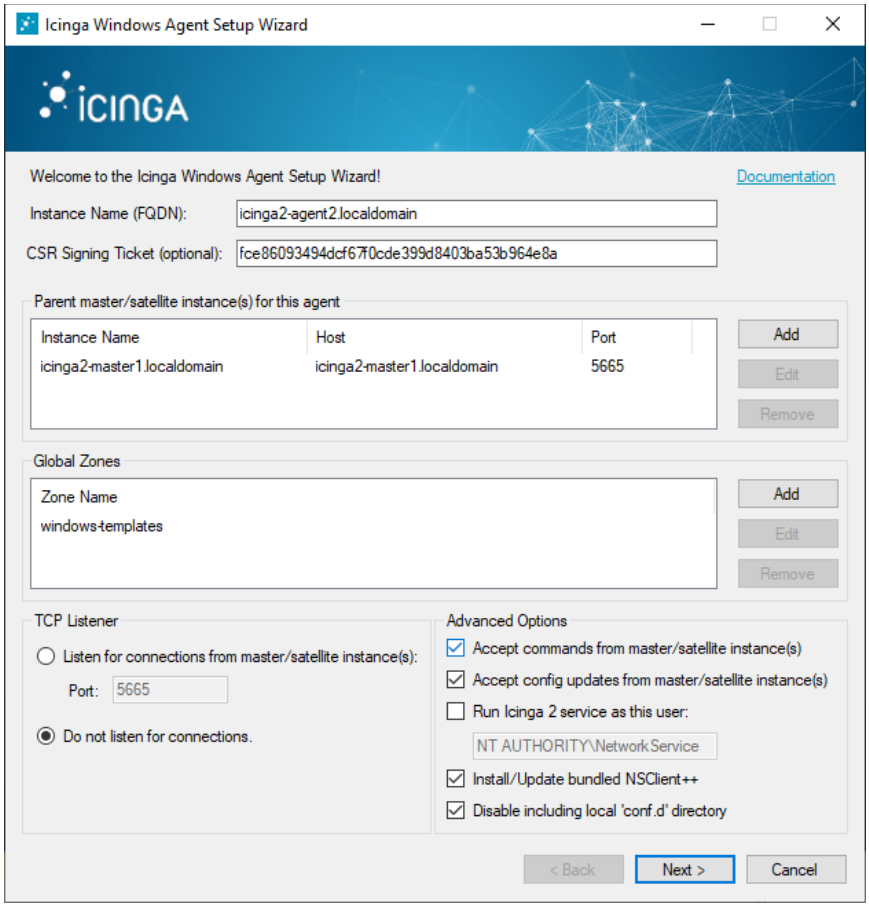
```
Accept config from parent node? [y/N]: y

Accept commands from parent node? [y/N]: y

Local zone name [icinga2-agent1.localdomain]: <enter>

Parent zone name [master]: <enter>

Default global zones: global-templates director-global

Do you want to disable the inclusion of the conf.d directory [Y/n]: <enter>

Disabling the inclusion of the conf.d directory...
```

Kehys 8. Masterin konfigurointien ja komentojen hyväksyminen

Kuten ohjeistetaan, käynnistetään palvelu uudelleen.

Windowsilla asennus toteutetaan käyttäen Icinga 2:n luomaa käyttöliittymää (**Kuva 8.**).[12] Annetaan instanssin nimi eli agentille haluttu nimi, masterilla luotu tiketti ja annetaan masterin osoite ja hyväksytään komennot, joita lähetetään. Agentin asentamisen jälkeen alkaa Icinga 2 automaattisesti Windows-palveluna.

[12] Icinga 2 Agent Setup on Windows. Viitattu 20.8.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#agent-setup-on-windows



Kuva 8. Icinga 2:n Windows-käyttöliittymä agentin asentamiseen[12]

4.4.3 Icinga Web 2 asentaminen

Asentaminen vaatii tietokantaan asennettuna joko MySQL:n tai PostgreSQL:n ja sen päälle on asennettava IDO-moduuli. Tässä työssä käytettiin MySQL-tietokantaa. IDO-moduuli huolehtii kaikkien konfiguraatio- ja tilatietojen tallettamisesta tietokantaan.[13]

Asennetaan MySQL ja IDO-moduuli kehyksen 9 komennolla.

---

[13] Icinga 2 Setting up Icinga Web 2. Viitattu 25.7.2021. https://icinga.com/docs/icinga-2/latest/doc/02-installation/#setting-up-icinga-web-2

```
apt-get install mariadb-server icinga2-ido-mysql
```

Kehys 9. Ladataan tarvittavat paketit MySQL-tietokantaa varten Icinga Web 2:lle

Luodaan dokumentaation ohjeistuksella kehyksen 10 tapaan tarvittu tietokanta ja annetaan sille tarvitut ominaisuudet. Tässä tapauksessa luodaan taulu root käyttäjällä.[13]

```
# mysql -u root -p

CREATE DATABASE icinga;

GRANT SELECT, INSERT, UPDATE, DELETE, DROP, CREATE VIEW, INDEX, EXECUTE
ON icinga.* TO 'icinga'@'localhost' IDENTIFIED BY 'icinga';
```

Kehys 10. Luodaan tietokanta ja annetaan tarvittavat oikeudet sille.

Taulun luonnin jälkeen ajetaan Icinga 2 IDO kaavio tauluun. (**Kehys 11.**)

```
mysql -u root -p < /usr/share/icinga2-ido-mysql/schema/mysql.sql
```

Kehys 11. Icinga 2 IDO:n skeeman ajo.

Otetaan IDO-palvelu käyttöön ja käynnistetään Icinga-palvelu uudelleen. (**Kehys 12.**)

```
icinga2 feature enable ido-mysql

systemctl restart icinga2
```

Kehys 12. IDO-palvelun käyttöönotto

Näiden asennuksien jälkeen pystyteen verkkopalvelin ja käynnistetään se. Suositeltu verkkopalvelin on Apache. Vaihtoehtona on myös Nginx, mutta valittiin Apache.

```
apt-get install apache2
```

Kehys 13. Apache 2-verkkopalvelimen asennus

Icinga Web 2 ja muut web-käyttöliittymät vaativat REST APIa toimiakseen. REST APIa käytetään toimintojen lähettämiseen, aikataulujen tarkistukseen ja kohteen tietojen kyselyyn. Asennetaan REST API, luodaan käyttäjä api-users.conf-tiedostoon ja käynnistetään palvelu uudelleen. (**Kehys 14.**)

```
$ icinga2 api setup

$ vim /etc/icinga2/conf.d/api-users.conf

object ApiUser "icingaweb2" {

  password = "…"

  permissions = [ "status/query", "actions/*", "objects/modify/*", "objects/query/*" ]

}

$ systemctl restart icinga2
```

Kehys 14. Icinga 2 APIn asennus

4.5 Tietokannat

Konfiguroitiin Icinga 2 käyttämään kahta tietokantaa eri käyttötarkoituksiin. MySQL on Icinga Web 2:n käyttöliittymää varten, jonne talletetaan käyttäjätunnukset, muistiinpanot, suunnitellut alhaalla oloaika ja vastaavaa. InfluxDB:ssä säilytetään laitteista kerättyä metriikkadataa.

4.5.1 MySQL

MySQL asennettiin pääosin Icinga Web 2:n takia. Icinga 2 tarvitsee myös tietokannan heidän REST API:a varten, jota Icinga Web 2 käyttää. Icinga hyödyntää tietokantaa heidän IDO-moduulinsa avulla, josta aikaisemmin jo mainittu. Lyhyesti kerrattuna huolehtii se kaikkien konfiguraatioiden ja tilatiedostojen puskemisen tietokantaan.

4.5.2 InfluxDB

Asennetaan InfluxDB ja sen asiakasohjelma pääpalvelimelle. (**Kehys 15.**)

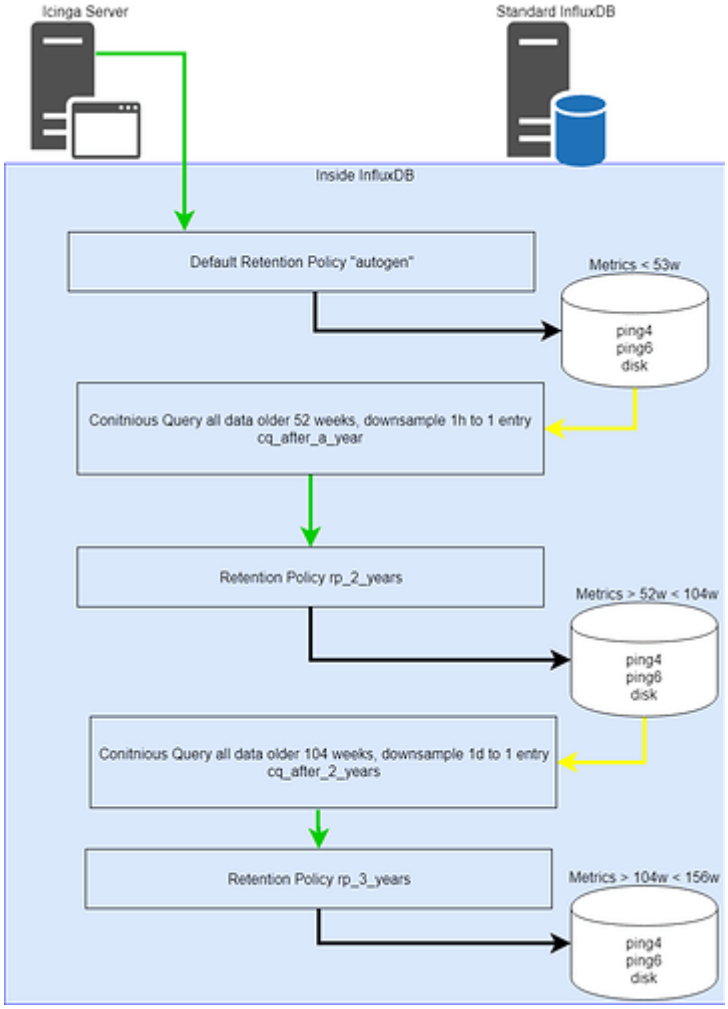
```
apt install influxdb influxdb-client
```

Kehys 15. InfluxDBn asennus

InfluxDB pyörii pääpalvelimella ja säilyttää dataa seuraavien konfiguraatioiden perusteella. Seuraavaksi luodaan taulut, joihin data säilytetään tietyllä säilytyspolitiikalla. Löydettiin tämä säilytyspolitiikka Icingan yhteisösivuilta.[14] Metriikkadataa ei haluttu säilyttää rajattomasti, joten pitää tehdä säätöjä tietokantaan. Metriikkadatasta ei ole tuntitasolla hyötyä kuukausien päästä.

Tällä politiikalla kuten kuvasta 9 voidaan päätellä, ajetaan kantaan alle 53 viikkoisen datan Icinga 2:n perussäilytyspolitiikalla eli yksi tunti per lokitiedosto. Tämän jälkeen, kun datalla on ikää yli 52 viikkoa ja alle 104 viikkoa ajetaan aikaisempi data pienennettynä tauluun yhden päivän lokitiedostoina. Tämän jälkeen ajetaan data pienennettynä tauluun yhtenä lokitiedostona, kunnes datalla on ikää 156 viikkoa, jonka jälkeen se poistetaan. (**Kehys 16.**)

[14] Icinga 2:n säilytyspolitiikka InfluxDBhen. Viitattu 21.08.2021. https://community.icinga.com/t/retention-policies-and-continuous-queries-made-simple/117



Kuva 9. InfluxDBn metriikkadatan säilytyspolitiikka[14]

```
> CREATE DATABASE icinga2;

> CREATE USER icinga2 WITH PASSWORD 'xxx'

> USE icinga2

> CREATE RETENTION POLICY "rp_2_years" ON "icinga2" DURATION 104w2d REPLICATION 1

> CREATE RETENTION POLICY "rp_3_years" ON "icinga2" DURATION 156w REPLICATION 1
```

```
> CREATE CONTINUOUS QUERY "cq_after_1_year" ON "icinga2" BEGIN SELECT mean(value) AS value,mean(crit) AS crit,mean(warn) AS warn INTO "icinga2"."rp_2_years".:MEASUREMENT FROM "icinga2"."autogen"./.*/ WHERE time < now() -52w GROUP BY time(1h),* END

> CREATE CONTINUOUS QUERY "cq_after_2_year" ON "icinga2" BEGIN SELECT mean(value) AS value,mean(crit) AS crit,mean(warn) AS warn INTO "icinga2"."rp_3_years".:MEASUREMENT FROM "icinga2"."rp_2_years"./.*/ WHERE time < now() -104w GROUP BY time(1d),* END

> ALTER RETENTION POLICY "autogen" ON "icinga2" DURATION 52w1d REPLICATION 1 SHARD DURATION 168h DEFAULT
```

Kehys 16. InfluxDBn tietokanta ja säilytyskonfigurointi

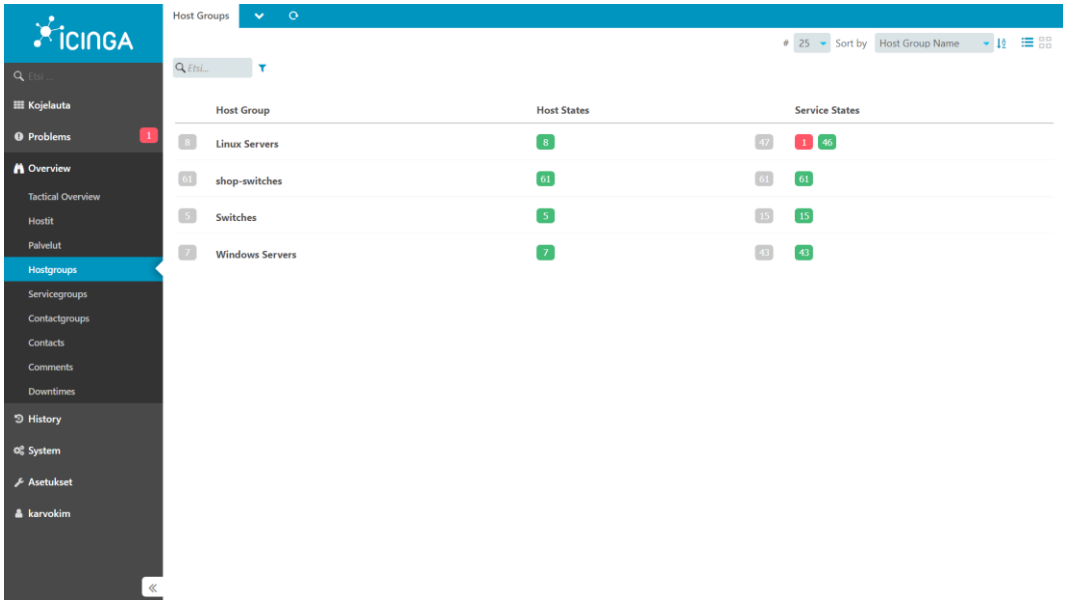
4.6 Icinga Web 2

Otettiin käyttöön Icinga Web 2, jotta voimme helposti seurata käyttöliittymän avulla mitkä laitteet ovat alhaalla ja nopeasti nähdä menikö konfiguroinnit oikein. Käyttöliittymä myös helpottaa ilmoituksien testaamista.

Jaettiin laitteet eri ryhmiin. Katso kuvasta 10 jaottelu. Ryhmät helpottavat yleisien asetuksien määrittämisen. Ryhmät määritellään kehyksen 17 tapaan. Tässä konfiguroidaan hostgroup eli isäntäryhmä nimeltä linux-servers.

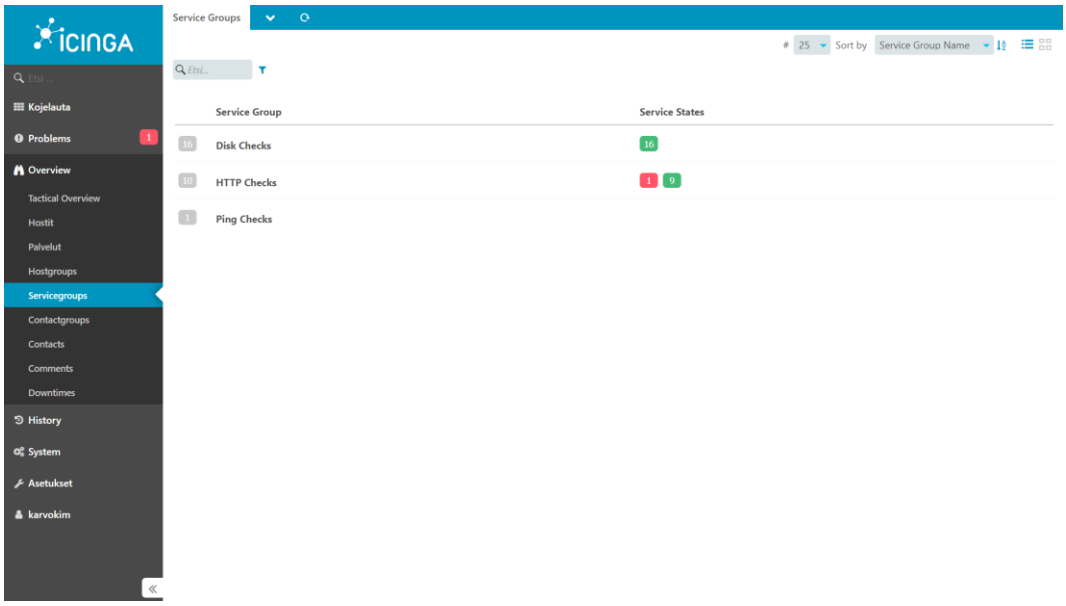
```
object HostGroup "linux-servers" {
  display_name = "Linux Servers"
  assign where host.vars.os == "Linux"
}
```

Kehys 17. Icinga hostgroup konfigurointi



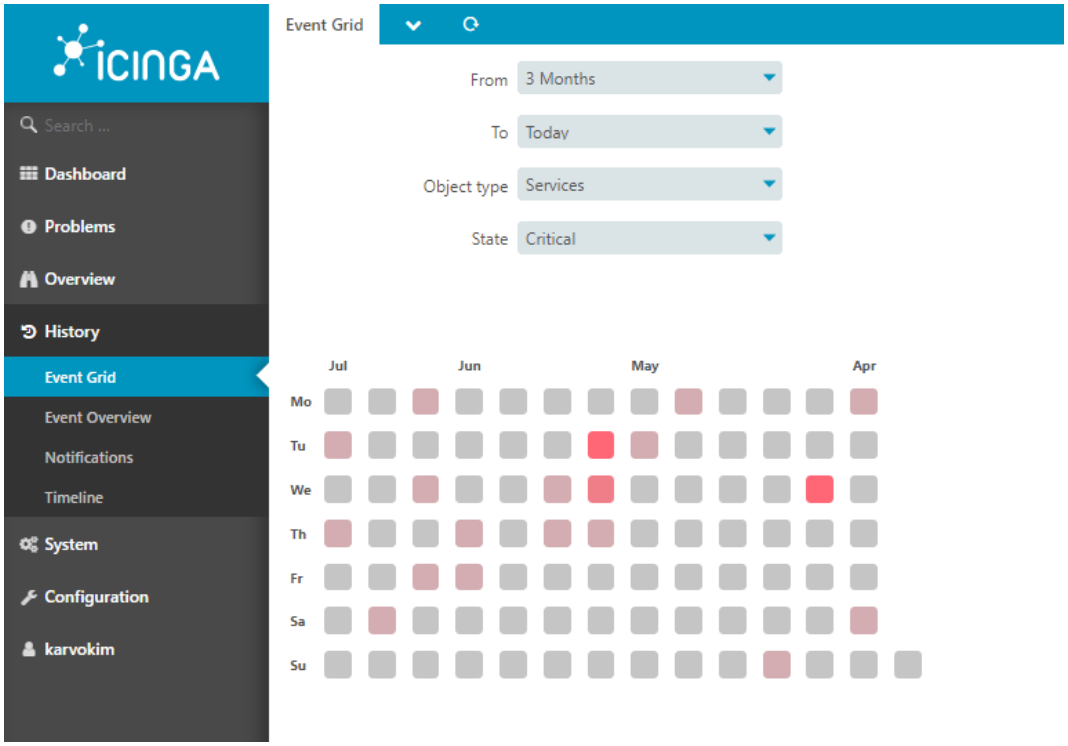
Kuva 10. Icinga Web 2 Hostgroups

Ryhmitettiin myös muutama Service eli palvelu, jotta niille on helpompi määrittää ylimmäntason tiedot. Katso kuvasta 11 jaottelut.



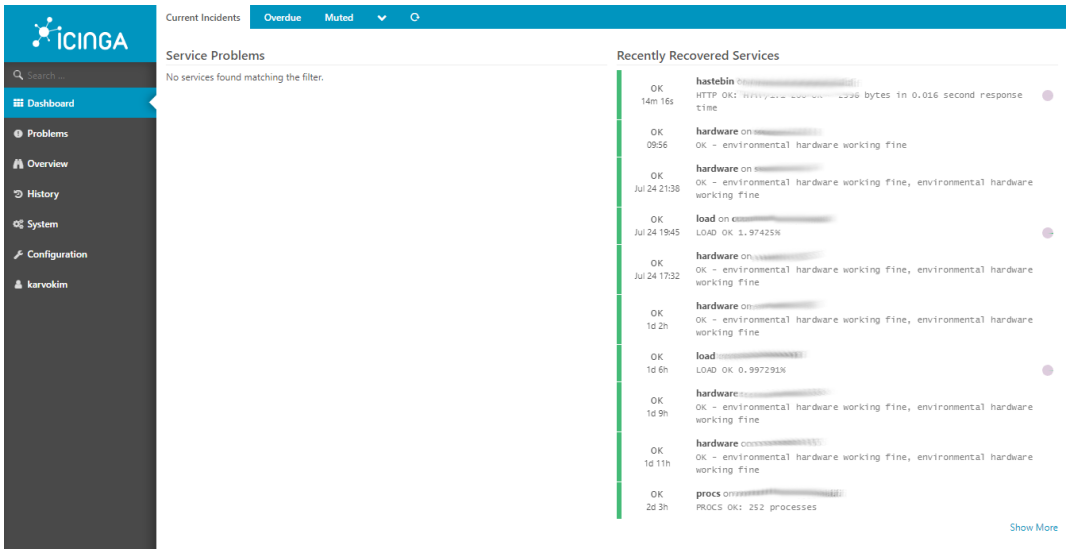
Kuva 11. Icinga Web 2 Servicegroups

Käyttöliittymä tarjoaa historianäkymän virhetiloista, jonka avulla on helppo selata tapahtuneita tapahtumia. (**Kuva 12.**).



Kuva 12. Icinga Web 2 History Event Grid

Käyttöliittymällä näkee reaaliaikaisia tapahtumia, kun käskyjä ajetaan. Etusivulla näkee mitkä palvelut ovat alhaalla ja mitkä ovat palautuneet (**Kuva 13.**).



Kuva 13. Icinga Web 2 Index Dashboard

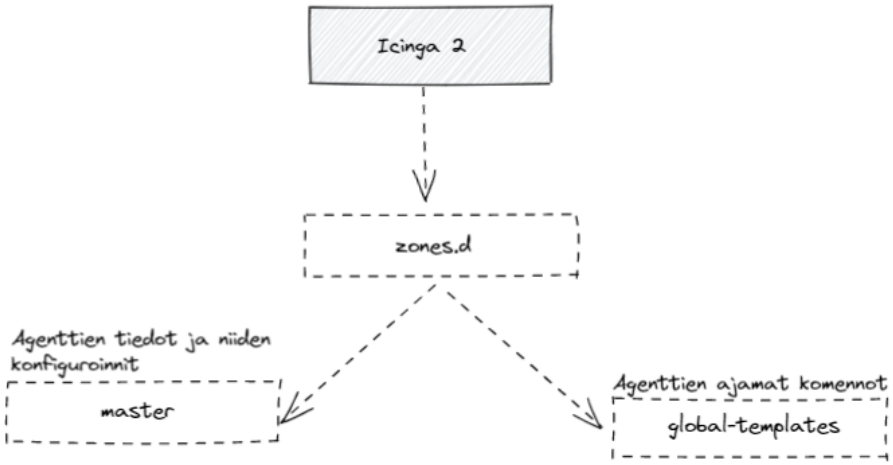
4.7 Icinga 2:n rakenne ja ilmoituksien raja-arvojen konfigurointi

Icinga 2 lukee ainoastaan /etc/icinga2/icinga2.conf tiedostoa. Kyseiseen tiedostoon sisällytetään tarvitut konfigurointitiedostot ja lisäosat kuten monitoring-plugins, jotka aikaisemmin ladattiin. Kun otetaan käyttöön Icinga Web 2 tai Icingan lisäosa, jossa tarvitaan web-käyttöliittymää, pitää sisällyttää conf.d kansion alta api-users.conf.

4.7.1 Icinga 2:n rakenne

Master-to-agent toteutustavassa kaikkien agenttien tiedot löytyvät zones.d-hakemiston alla olevasta master-hakemisto (**Kuva 14.)**. Paras käytäntö on hajauttaa laitteet niille parhaaksi nähtyihin ryhmiin, kuten aikaisemmista luvuista näimme, ryhmitettiin agentit palvelimiin, reitittimiin ja kytkimiin.

Agenteille määritetään useita muuttujia, ja voidaan niitä muokata joko master-hakemistossa olevissa konfigurointitiedostoissa, jotka ovat tarkkoja, tai voidaan niille asettaa yleisiä muuttujia global-templates-hakemistossa, jossa ne eivät ole niin tarkkoja, vaan yleisempiä.



Kuva 14. Icinga 2:n rakenne master-to-agent toteutuksessa.

4.7.2 Icinga 2:n raja-arvojen konfigurointi

Käytiin kohdassa 4.7.1 läpi mitenkä Icinga 2:n konfiguroinnit toteutetaan master-to-agent toteutustavassa. On useita erityyppisiä agentteja, joten on niillä myös erilaiset konfigurointitiedostot.

Global-templates-hakemistossa konfiguroidaan komentoja ja palveluita, joita ajetaan agenteilla. Hakemistossa on myös käyttäjätiedot API:a varten. Hakemisto sisältää myös ilmoituksien konfiguroinnit niiden lähetystä varten (**Kuva 15.**)

```
/etc/icinga2/zones.d/global-templates# ls -l | grep -v "~$"

root root 6212 Mar 26 13:49 commands.conf
root root   71 Aug 24  2020 constants.conf
root root  859 May 27 13:59 groups.conf
root root  677 Feb  9  2021 notifications.conf
root root 1279 Feb  4  2021 notifications.conf.save
root root 4768 May 27 14:18 services.conf
root root 4732 Apr 29 13:15 services.conf.save
root root 6311 Feb  4  2021 slack-notifications-command.conf
root root 1813 Feb 10  2021 slack-notifications-configuration.conf
root root  708 Feb  9  2021 slack-notifications-user-configuration.conf
root root 2605 May 27 11:43 templates.conf
root root 1044 Mar 26 15:02 timeperiods.conf
root root  538 Feb  9  2021 users.conf
```

Kuva 15. Icinga 2 global-templates konfigurointitiedostot

Templates.conf-tiedostossa määritellään mallit hosteille ja palveluille, jonka avulla voidaan määrittää muuttujia yleisellä tasolla agenteilla (**Kuva 16.**). Nämä asetukset eivät kuitenkaan ole korkeimman tason, eli voidaan ne ylikirjoittaa myöhemmin agenttien omissa konfigurointitiedostoissa. Kuvassa 16 määritellään mallille, kuinka tiheästi lähetetään kyselyä tilasta, ja jos on virhetila, niin tihennetään aikajaksoa. Jos virhetila ei ole mennyt ohi, kun on tehty määritetty määrä uudelleenyrityksiä, lähetetään ilmoitus hosteista ja palveluista Slackiin. Ainoastaan hosteista lähetetään ilmoitus sähköpostiin.

```
template Host "generic-host" {
  max_check_attempts = 3
  check_interval = 3m
  retry_interval = 30s
  vars.notification["mail"] = {
        groups = ["icingaadmins"]
  }
  vars.slack_notifications = "enabled"
}

template Service "generic-service" {
  max_check_attempts = 5
  check_interval = 3m
  retry_interval = 30s
  vars.slack_notifications = "enabled"
}
```

Kuva 16. Icinga 2 hostien ja palveluiden konfigurointi.

Malleja käytetään tuomalla ne erillisiin palveluihin, joissa voidaan ylikirjoittaa mallien muuttujat tarpeen mukaan. Erilliset palvelut ovat vielä tarkempia verrattuina malleihin, jotka ovat hyvin laajoja ja epätarkkoja. Näissä palveluissa määritellään tarkasti mihinkä laitteeseen tai osaan kyseistä palvelua tullaan käyttämään. Määritetään komento mitä halutaan palvelun ajavan ja niiden muuttujat (**Kuva 17.**). Palvelulla, joka ajaa disk-komentoa, on määritetty raja-arvoiksi varoitus 10 % ja kriittinen 5 %. Procs-palvelussa ei määritellä raja-arvoja, vaan määritellään ne agentin konfigurointitiedostossa (**Kuva 19.**). Load-palvelu tarkkailee prosessin kuormitusta kolmella eri aikatasolla 1-, 5- ja 15-minuutin aikavälillä. Tässä olemme asettaneet jokaiselle aikavälille saman kuormituksen varoitusrajat.

```
apply Service "disk" {
  import "generic-service"
  check_command = "disk"
  check_interval = 10m
  vars.disk_wfree = "10%"
  vars.disk_cfree = "5%"
  //enable_notifications = false
  enable_notifications = true
  command_endpoint = host.vars.agent_endpoint
  assign where host.vars.agent_endpoint
}

apply Service "procs" {
  import "generic-service"
  check_command = "procs"
  command_endpoint = host.vars.agent_endpoint
  assign where host.vars.agent_endpoint
}

apply Service "load" {
  import "generic-service"
  check_command = "load"
  vars.load_wload1 = 8
  vars.load_cload1 = 10
  vars.load_wload5 = 8
  vars.load_cload5 = 10
  vars.load_wload15 = 8
  vars.load_cload15 = 10
  command_endpoint = host.vars.agent_endpoint
  assign where host.vars.agent_endpoint && host.vars.os == "Linux"
}
```

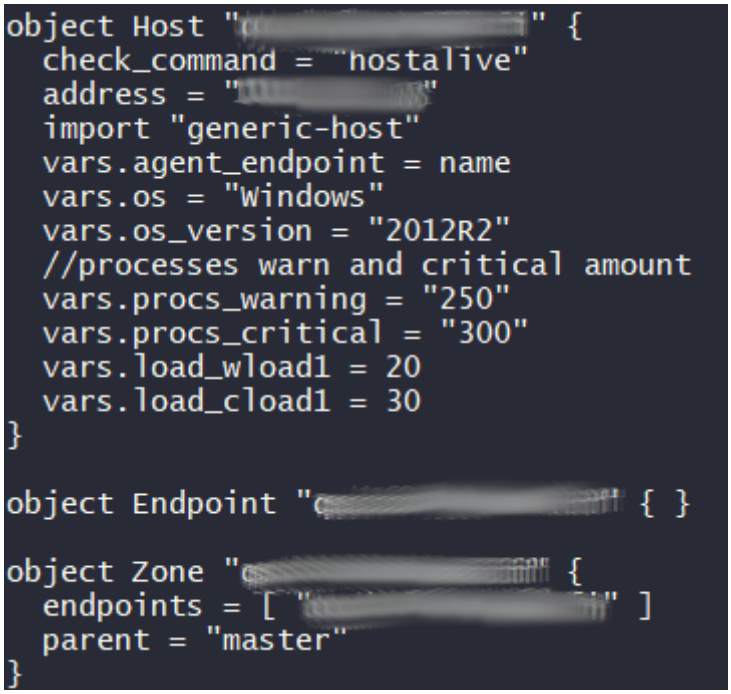
Kuva 17. Icinga 2 Sääntöjen soveltaminen malleilla.

Jaetaan hostit ja palvelut erillisiin ryhmiin, jotta niitä on myöhemmin helpompi analysoida (**Kuva 18.**). Icinga Web 2 erityisesti hyötyy tästä ryhmittämisestä katso kuvat 10–11. Ryhmiä voidaan määritellä monella eri tapaa esimerkiksi niiden muuttujien arvoilla ja hostin eli agentin nimen mukaan.

```
/**
 * Host group examples.
 */

object HostGroup "linux-servers" {
  display_name = "Linux Servers"

  assign where host.vars.os == "Linux"
}

object HostGroup "windows-servers" {
  display_name = "Windows Servers"

  assign where host.vars.os == "Windows"
}

object HostGroup "switches" {
  display_name = "Switches" // overwrites HostGroup name

  assign where host.vars.device == "switch"
}

object HostGroup "shop-switches" {
        assign where host.vars.device == "shop-switch"
}

/**
 * Service group examples.
 */

object ServiceGroup "ping" {
  display_name = "Ping Checks"

  assign where match("ping*", service.name)
}

object ServiceGroup "http" {
  display_name = "HTTP Checks"

  assign where match("http*", service.check_command)
}

object ServiceGroup "disk" {
  display_name = "Disk Checks"

  assign where match("disk*", service.check_command)
}
groups.conf (END)
```

Kuva 18. Icinga 2 hostien ja palveluiden ryhmittäminen.

Kaikkea yllä olevaa hyödynnetään itse hostilla eli agentilla. Tässä alla olevassa kuvassa (**Kuva 19.**) konfiguroidaan palvelimelle ylimääräiseksi komennoksi ”hostalive” eli tarkistetaan vastaako laite pingiin. Lisäksi tuodaan ”generic-host”-malli, josta tulee millä aikavälillä palvelinta tarkistetaan ja lähetäänkö ilmoituksia. Määritellään laite Windows-pohjaiseksi ryhmitystä varten. Koska laite kuuluu Windows-ryhmään, ajetaan sille Windows-pohjaisia komentoja, jotka määritellään apply:lla eli soveltamisella (**Kuva 17**). Määritetään myös tarkat arvot, jotka ylittyessä lähetetään ilmoitukset, jos ne on sallittu.



Kuva 19. Palvelimen konfigurointi.

4.8 Verkkolaitteet

Verkkolaitteisiin kuuluvat palvelimet, reitittimet ja kytkimet. Näistä valvotaan eri tietoja riippuen mitä niistä voidaan valvoa. Kuten aikaisemmista luvuista nähdään, valvotaan palvelimilta perustietokoneen komponentteja kuten prosessoria, muistia ja talletustilaa ja niihin liittyviä prosesseja.

Tässä työssä hyödynnettiin SNMP-protokollaa, jotta saatiin tietoa kytkimistä ja reitittimistä (**Kuva 1.**). Tähän käytettiin Icinga 2:n foorumeilta löytyvää lisäosaa, joka toimii suurimmalla osaa reitittimistä ja kytkimistä. Harvinaisessa tapauksessa, jos liitäntä ei tue laitetta, voidaan valmistajan sivuilta etsiä laitteeseen vastaava MIB ja rakentaa oma komento hankkimaan tietoa kyseiseltä laitteelta.

5 TULOKSET

Työn tuloksena on hajautettu valvontajärjestelmä, jolla valvotaan verkkolaitteiden tilaa. Osittain valvotaan myös palveluita, kuten verkkosivuja. Työn toteutukseen käytettiin työkaluna Icinga 2:sta ja sen tarjoamia moduuleja kuten Icinga Web 2:sta ja Grafanaa. Valvottavia laitteita on yhteensä lähes satakunta. Valvottaviin laitteisiin kuuluvat palvelimet, reitittimet ja kytkimet. Kaikille laitteille ei voida asentaa Icingan agenttia, joten hankitaan niistä tietoa käyttäen SNMP-protokollaa.

Lisäksi kollega on rakentanut komennon valvomaan muutaman myymälän verkkoliikennettä ja eräälle palvelimelle tiedonsiirtoa. Tiedonsiirtojen valvonta vaatii erittäin hyvää tietämystä, mitenkä tietojen kuuluu kulkea, ja mistä nähdään ovatko ne kulkeneet oikein. Laitteen verkkoliikennettä voidaan valvoa, jos se koetaan tarpeelliseksi. Toteutettiin testaustarkoituksiin verkkoliikenteen valvonta, jotta nähdään, onko tarvetta nostaa nopeuksia. Muutamia kehityskohteita ilmaantui työn aikana. Haluttiin enemmän laitteistoa valvontaan.

5.1 Metriikkadatan visualisointi

Kuten kuvasta 20 selviää, tarkastellaan palvelimen käyttöä viimeisen kolmenkymmenen päivän tapahtumista. Tämän tapaisilla visualisoinneilla luotiin tämänhetkiset raja-arvot, joiden avulla ilmoitukset lähtevät. Grafana tukee myös ilmoituksien lähettämisen, jos tietyt raja-arvot ylittyvät, mutta halusimme keskittää kaiken hallintaan liittyvän yhteen paikkaan eli Icinga 2:n masteri. Hyödynnettiin kuitenkin raja-arvoja asettamalla graafeihin varoitus- ja kriittiset arvot, jotta on helposti nähtävissä, jos raja-arvot lähestyvät, eikä niitä tarvitse muistella tai käydä katsomassa erillisestä paikasta.

HalpaHallin logistiikkakeskuksen IT-osaston huoneeseen on asennettu TV, jossa pyörii Grafanan tarjoama esitystila, joka pyörittää Grafanaan luotuja sivuja. Tämäkin helpottaa huomattavuutta, kun tulee esille sivu, jossa on kaikki kytkimet ja vihreän joukossa näkyy keltaista tai punaista, eli varoitus- ja kriittinen tila.

Kuva 20. Palvelin x:n datan visualisointi

5.2 Varoitusilmoitukset

Varoitusilmoitukset laukeavat, kun asetetut raja-arvot ylittyvät. Raja-arvoja voidaan konfiguroida usealla tasolla eli voidaan kaikille kytkimille antaa yleinen vasteaika ja sitten korvata arvo yksittäisen kytkimen konfigurointi tiedostossa.

Varoitusilmoitukset ovat olleet jo hyödyksi muutamaan otteeseen tämän työnteon aikanakin. Slackiin on tullut ilmoituksia Hobotilta webhookkien avulla (**Kuva 4.**). Ilmoitukset ovat tulleet, myös sähköpostiin, mutta reagointi on ollut nopeinta Slackin suhteen. Osasyynä on, että sähköpostit tulevat kahdelle henkilölle, eikä koko IT-osastolle.

Yhdellä kytkimellä oli mennyt tuuletin rikki ja siitä tuli ilmoitus, joka myöhemmin todettiin todeksi lähettämällä kysely myymälään, joten on työkalu osoittautunut

jo hyödylliseksi. Muita varoitusilmoituksia ovat olleet muun muassa muistin ja talletustilan lähestyminen täyttä. Nämäkin tulevat ongelmat saatiin hyvissä ajoin ratkaistua.

6 JOHTOPÄÄTÖKSET

Työn tarkoituksena oli saada verkonvalvontajärjestelmä, jolla on helppo valvoa nykyistä ja mennyttä. Mennyttä halutaan seurata, koska voidaan siitä tehdä johtopäätöksiä, milloin resursseja alettiin käyttämään enemmän, ja sen perusteella tehdä johtopäätöksiä. Ilmoitukset ovat myös suuri osa nykyistä ja tulevaa nähden. Varoitusilmoitukset auttavat arvioimaan kriisejä, joita tulee vastaan tulevaisuudessa, ellei näihin asioihin puututa. Kriittiset ilmoitukset varoittavat nykyhetkessä tapahtuvia ongelmia, jotka pitää hoitaa heti.

Tässä työssä ei perehdytty paljoa sen valvontaan mitä verkkoliikennettä liikkuu ja liikkuuko se oikein, vaan keskityttiin laitteiden valvontaan. Tietoliikenteen valvonta keskitettyyn paikkaan jää tulevaisuuden projektiksi.

On käyty keskustelua, onko tarpeen liittää UPS: eli varavirtalähteet ja laitteiden tukiasemat valvonnan piiriin. HalpaHallin käyttämät varavirtalähteet vaativat erillisen verkkokortin, joka liitetään varavirtalähteeseen, jotta niitä voitaisiin valvoa. Varavirtalähteet, jotka vastaavat keskeisimpien palvelimien ylläpidosta, kun verkkovirta katkeaa, olisi hyvä saada valvontaan.

LÄHTEET

1 SNMP selityksiä. Viitattu 25.7.2021. https://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/SNMP.html

2 Nagiosin toimintaperiaate esitettynä kuvassa. Viitattu 22.4.2021. https://upload.wikimedia.org/wikipedia/commons/1/1a/Monitoring.png

3 Mikä on Icinga 2? Viitattu 22.4.2021. https://icinga.com/docs/icinga-2/latest/

4 Icinga 2 Roles: Master, Satellites and Agents. Viitattu 26.4.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#roles-master-satellites-and-agents

5 Icinga 2 Master with Agents. Viitattu 12.5.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#master-with-agents

6 Icinga 2 Template Library. Viitattu 20.8.2021. https://icinga.com/docs/icinga-2/latest/doc/10-icinga-template-library/

7 Icinga Web 2. Viitattu 25.7.2021 https://icinga.com/docs/icinga-web-2/latest/doc/01-About/

8 Icinga 2:n integraatio Grafana. Viitattu 25.7.2021 https://icinga.com/products/integrations/grafana/

9 SNMP selityksiä. Viitattu 25.7.2021. https://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/SNMP.html

10 Douglas R. Mauro & Kevin J. Schmidt. (2001). Essential SNMP (1st ed.). Sebastopol, CA: O'Reilly & Associates. https://doc.lagout.org/network/Essential%20SNMP%202001.pdf

11 Icinga 2 Agent Setup on Linux. Viitattu 13.8.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#agent-satellite-setup-on-linux

12 Icinga 2 Agent Setup on Windows. Viitattu 20.8.2021. https://icinga.com/docs/icinga-2/latest/doc/06-distributed-monitoring/#agent-setup-on-windows

13 Icinga 2 Setting up Icinga Web 2. Viitattu 25.7.2021. https://icinga.com/docs/icinga-2/latest/doc/02-installation/#setting-up-icinga-web-2

14 Icinga 2:n säilytyspolitiikka InfluxDBhen. Viitattu 21.08.2021. https://community.icinga.com/t/retention-policies-and-continuous-queries-made-simple/117