jamk

Verkonvalvontasovellusten vertailu

Jere Issakainen

Opinnäytetyö, AMK
Kesäkuu 2024
Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Issakainen Jere

Verkonvalvontasovellusten vertailu

Jyväskylä: Jyväskylän ammattikorkeakoulu. Kesäkuu 2024, 54 sivua

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Opinnäytetyö tehtiin toimeksiantona TNNet Oy:lle. Tavoitteena oli selvittää vaihtoehtoja nykyiselle verkonvalvonta järjestelmälle. Syy selvitystyölle oli nykyaikaisten ominaisuuksien puuttuminen nykyisestä verkonvalvontajärjestelmästä sekä vanhentunut sovellusversio, joka vaatisi joka tapauksessa päivitystä.

Työ toteutettiin vertailemalla kahta verkonvalvontasovellusta. Vertailun osa-alueet valittiin etukäteen ennen vertailun tekemistä. Vertailtavat sovellukset olivat Checkmk ja Nagios XI. Vertailu toteutettiin pystyttämällä molempiin sovelluksiin testausympäristö, jonka avulla sovelluksien ominaisuuksia testattiin. Tämän pohjalta eri osa-alueet pisteytettiin, jonka perusteella näistä kahdesta sovelluksesta saatiin selville parempi vaihtoehto.

Tutkimuksen tuloksen perusteella Checkmk on verkonvalvontasovellus, joka sopii paremmin mahdollisesti käyttöönotettavaksi. Vertailun pohjalta selviksi eroiksi muodostuivat hinta ja käyttökokemus.

Työssä tuli esille myös puutteet nykyisessä verkonvalvontajärjestelmässä sekä miten nykyaikaisella verkonvalvontasovelluksella saadaan lisäarvoa yritystoimintaan. Työn pohjalta toimeksiantajayritys voi tehdä päätöksen, halutaanko yritykselle ottaa käyttöön kaupallinen verkonvalvontasovellus.

Avainsanat (asiasanat)

Verkonvalvontasovellus, Verkonvalvonta, Checkmk, Nagios XI,

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Issakainen Jere

Comparison of network monitoring software

Jyväskylä: JAMK University of Applied Sciences, June 2024, 54 pages

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

Permission for open access publication: Yes/No

Language of publication: Finnish

Abstract

This study was employed by TNNet Ltd. The goal was to find alternative solutions to the current network monitoring system. The reason behind this study was the lack of modern features in the current network monitoring system and its old software version, which requires updating.

The study was done by comparing two different networking monitoring software. The comparison was divided into different topics, which were determined beforehand. The software that were compared were Checkmk and Nagios XI. The comparison was done by making the same testing environment in both systems. With these environments the features were tested, and the topics of comparison were scored. Based on this score and testing the better software was chosen.

The result was that Checkmk is the better software out of these two options. The main differences were the price and user experience.

The lack of features in the current network monitoring system stood up, and how a modern network monitoring software can add value to business. The employer can make decisions based on this study, whether it's worth to start using a commercial network monitoring software.

Keywords/tags (subjects)

Network monitoring system, Network monitoring Checkmk, Nagios XI

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

1 Johdanto

1.1 Verkonvalvonta yleisesti

Verkonvalvonnalla tarkoitetaan verkossa olevien laitteiden jatkuvaa seurantaa. Tarkoituksena on saada käsitys siitä, mitä verkossa tapahtuu ja havaita ongelmia. Valvonta toteutetaan keräämällä tietoa valvottavista laitteista. Tätä varten tarvitaan sovellus, joka suorittaa tiedon keräämisen, eli verkonvalvontasovellus. Verkonvalvonta toteutetaan tietoliikenneprotokollia ja valvontatyökaluja hyödyntäen. Osapuolina on hallintasovellus eli itse valvontapalvelin, joka käsittelee dataa, jota kerätään verkosta, ja agenttisovellus, joka sijaitsee valvottavilla laitteilla ja jonka tehtävä on välittää kerätty data hallintasovellukselle. (What is network monitoring? n.d.)

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli selvittää vaihtoehtoja nykyiselle verkonvalvontajärjestelmälle. Nykyinen asiakaslaitteiden valvonta on toteutettu pääosin Nagios Core 3 -valvontamoottorilla, jolle on tehty oma käyttöliittymä. Syynä uudistukselle on nykyisen järjestelmän vanhempi versio ja nykypäivän tarpeita vastaavien ominaisuuksien puuttuminen. Työssä vertaillaan täysin uutta sovellusta, sekä Nagioksen kaupallista verkonvalvontasovellusta. Vertailussa halutaan kiinnittää erityisesti huomiota sovellusten lisäominaisuuksiin pelkän valvonnan lisäksi, joilla voidaan luoda lisäarvoa erityisesti asiakkaille. Lisäominaisuuksilla tarkoitetaan esimerkiksi visualisointi- ja hallintaominaisuuksia.

Huomioitavaa on myös, että nykyinen järjestelmä on avoimeen lähdekoodiin perustuva ja siten yritykselle täysin ilmainen. Vertailtavista ohjelmista on myös saatavilla ilmaisversio, tai ilmainen avoimen lähdekoodin versio, joka poikkeaa hieman maksullisista versioista. Ilmaisversioissa on kuitenkin rajoituksia joko skaalautuvuuden tai ominaisuuksien suhteen, joten vertailuissa käytettiin kokeiluversioita maksullisista tuotteista.

1.3 Toimeksiantaja

Tämän opinnäytetyön toimeksiantajana on TNNet Oy. TNNet on vuonna 2002 perustettu yritys, joka tarjoaa monipuolisesti IT-infrastruktuuripalveluja. Palveluihin kuuluvat esimerkiksi omasta ko-

nesalista tuotetut virtuaalipalvelimet, tietoliikenneyhteydet, sisäverkkoratkaisut sekä tietoturvapalvelut. TNNet työllistää 14 henkilöä ja yrityksen liikevaihto oli vuonna 2023 3,7 miljoonaa euroa. (Tietoja meistä n.d.) Verkonvalvontajärjestelmää käytetään yrityksen omien palvelimien ja laitteiden valvontaan sekä asiakkaiden palveluiden ja laitteiden valvontaan. Yleisimmät valvottavat kohteet ovat asiakkaiden päätelaitteet ja virtuaalipalvelimet. Asiakkaiden palvelutaso liittyy oleellisesti verkonvalvontaan, joten verkonvalvontajärjestelmän täytyy myös sen suhteen tukea yrityksen toimintaa.

1.4 Tutkimusasetelma

Tutkimusongelmana on yrityksen verkonvalvontakokonaisuuden parantaminen. Tarkoituksena on vertailla vaihtoehtoisia ohjelmia ja vertailun avulla parantaa nykyistä verkonvalvontaa.

1.4.1 Tutkimuskysymykset ja -menetelmä

Tutkimusongelmasta voidaan johtaa seuraavat tutkimuskysymykset:

- Vastaako nykyinen ratkaisu nykyhetken tarpeita verkonvalvonnan suhteen?
- Onko verkonvalvonnan uusimisesta merkittävää hyötyä yritykselle sekä asiakkaille?
- Miten verkonvalvontaa on mahdollista toteuttaa nykyajan sovelluksilla?

Tutkimusmenetelmänä on kehittämistutkimus. Työssä on tunnistettu ongelma, johon on kehittämistarve. Tutkimuksen tavoitteissa on tullut esille kehittämistavoitteet, ja näiden pohjalta on tehty kehittämissuunnitelma, jota testataan ja arvioidaan. (Pernaa 2013)

2 Verkonvalvonta

2.1 Valvonnan osa-alueet

On tärkeää ymmärtää, miksi valvontaa tehdään, mitä valvotaan ja minkä takia. Verkonvalvontaa voidaan lähestyä ITIL-viitekehyksen näkökulmasta, joka vastaa näihin kysymyksiin. ITIL palvelunhallintakäytänteiden avulla voidaan verkonvalvonta jakaa eri osa-alueisiin: saatavuuden hallinta, suorituskyvyn hallinta, vikojen hallinta sekä valvonnan ja tapahtumien hallinta. (ITIL Foundation 2019.)

Saatavuuden hallinta

Saatavuuden hallinnalla tarkoitus on varmistaa, että asiakkaalle toimitettu palvelu on toiminnassa. Palvelun saatavuus on suoraan riippuvainen siitä, kuinka usein palvelun toimitus keskeytyy ja kuinka pitkäksi aikaa. Asiakkaalle merkityksellistä on, että esimerkiksi heidän virtuaalipalvelimellansa toimiva sovellus on toiminnassa. Todellisuudessa palvelu koostuu useammista toiminnoista, kuin pelkkä virtuaalipalvelin ja siinä toimiva sovellus. (ITIL Foundation 2019.)

TNNetin palvelut tarjotaan samalla kun ne tuotetaan, eli verkonvalvonnan tehtävänä on havaita mahdolliset ongelmat tuotannossa, mielellään niin, että vika saadaan käsiteltyä ennen kuin asiakas sitä edes huomaa.

Suorituskyvyn ja kapasiteetin hallinta

Suorituskyvyn ja kapasiteetin hallinnalla tarkoitetaan, että palvelu saavuttaa odotetun tai sovitun suorituskyvyn. Tämä pitää sisällään itse asiakkaan palvelut sekä yrityksen infrastruktuurin, jonka päällä nämä palvelut toimivat. Täytyy siis tietää, että millainen on nykyinen vaatimus kapasiteetin suhteen ja osata myös ennustaa tulevaisuuteen vaatimusten suhteen. Palvelujen skaalautuvuus liittyy myös olennaisesti tähän. Valvonnalla halutaan nähdä nykyisen infrastruktuurin riittävyys sekä havaita mahdollisia puutteita asiakkaan palvelujen suorituskyvyssä. (ITIL Foundation 2019.)

Valvomalla suorituskykyä ja kapasiteettia, voidaan asiakkaan palvelulle määrittää halutut raja-arvot, joilla voidaan todeta, että suorituskyvyssä tai palvelun resursseissa on puutteita. Esimerkiksi

voidaan seurata, jos palvelimen muisti uhkaa jatkuvasti loppua tai varoittaa levytilan loppumisesta. Molemmissa tapauksissa varoitukseen voidaan reagoida etukäteen joko lisäämällä resurssia tai muulla muutoksella.

Vikojen hallinta

Vialla tarkoitetaan odottamatonta keskeytystä palvelussa tai sen laadun heikkenemistä. Vioista ja niiden ratkaisemisista tulisi jäädä jälki organisaation järjestelmiin, jotta vanhoihin vikoihin voidaan palata saman- tai samankaltaisen vikojen ilmetessä uudelleen. Viat voidaan jakaa ryhmiin, sen mukaan minkälaisia toimenpiteitä ne vaativat ja kenen toimesta ne voidaan korjata. (ITIL Foundation 2019.)

Odottamattomiin keskeytyksiin täytyy reagoida palvelutason mukaan priorisoiden. Hälytyksistä tulisi jäädä jälki esimerkiksi organisaation tikettijärjestelmään, jotta nähdään, onko vastaavia vikoja ollut aiemmin ja kuinka paljon. Ratkaistuissa vioissa tulisi olla kuvaus viasta ja vaadituista korjaustoimenpiteistä.

Valvonnan ja tapahtumien hallinta

Valvonnan hallinnalla tarkoitetaan palvelujen jatkuvaa automatisoitua monitorointia, jotta voidaan havaita mahdollisia palveluihin vaikuttavia poikkeamia. Nämä poikkeamat halutaan erotella niiden kriittisyyden ja vaadittavien toimenpiteiden mukaan. Valvonnan havaitsemat tapahtumat voivat olla informatiivisia, varoituksia tai poikkeuksia. Näistä vain varoituksista ja poikkeuksista halutaan ilmoituksia, koska niillä on suora vaikutus palveluihin. Varoitukset ennakoivat mahdollisia ongelmia, ja niiden perusteella korjaustoimenpiteet voidaan aloittaa, ennen kuin suurempaa vikaa kerkeää tapahtumaan. Poikkeukset ovat tapahtumia, joissa tilanteesta mukaan vika voi jo näkyä käyttäjälle. Poikkeusiin reagoidaan palvelutason tai valvottavan kohteen kriittisyyden mukaan. (ITIL Foundation 2019.)

Valvonnan ja tapahtumien hallinta liittyy suoraan käytettyyn verkonvalvontaohjelmistoon, jonka tehtävänä on havaita poikkeamia. Lähtökohtaisesti kaikesta, jota valvotaan, halutaan saada ilmoituksia. Jos jostain valvonnasta saadusta ilmoituksesta ei ole mitään hyötyä, tulisi kyseinen valvonta poistaa.

3 Verkkolaitteet

Verkkolaitteita, kuten palomuureja, kytkimiä tai reitittimiä valvotaan yleensä SNMP:llä tai ping-tarkistuksella. Näihin sekä valvonta-agentteihin liittyvät oleellisesti TCP, IP ja UDP protokollat.

3.1 TCP

TCP (Transmission Control Protocol) on tietoliikenneprotokolla, joka mahdollistaa pakettien liikkumisen esimerkiksi palvelimen ja yksittäisen käyttäjän välillä. TCP on yhteydellinen protokolla, jota käytetään, kun halutaan, että data liikkuu luotettavasti. TCP luo aluksi yhteyden palvelimen ja käyttäjän välille käyttämälle kolmisuuntaista kättelyä, jossa osapuolet synkronoivat ja kuittaavat, että tiedonsiirto voidaan aloittaa. Yhteyden päättämiseen käytetään FIN-viestiä. TCP sisältää virheenkorjaus-, vuonhallinta ja ruuhkanhallinta mekanismeja, joiden ansiosta tiedonsiirto on luotettavaa. Pakettien täytyy mennä perille ennalta sovitussa järjestyksessä, ja jos jokin paketti tippuu, se lähetetään uudelleen. TCP paketti pitää sisällään aiempien mekanismien lisäksi tiedon lähde- ja kohdeportista, joiden avulla löydetään oikea kohde tiedonsiirrolle. (What is Transmission Control Protocol TCP/IP? n.d; RFC793:1981.)

3.2 UDP

UDP (User Datagram Protocol) on tietoliikenneprotokolla, jota hyödynnetään matalaa latenssia vaativissa sovelluksissa. UDP lähettää datagram paketteja kohteelle, jotka sisältävät tiedon lähde- ja kohdeportista. UDP protokollan matala latenssi perustuu siihen, että toisinkuin TCP protokollassa, se ei luo yhteyttä kohteen ja lähettäjän välille, eikä siinä ole virheenkorjaus- tai vuonhallinta-ominaisuuksia. Käytännössä lähettäjä ei tiedä, meneekö paketit perille asti. (What is User Datagram Protocol (UDP)? n.d.)

3.3 ICMP

ICMP eli on OSI-mallin kolmannella kerroksella eli verkkokerroksella toimiva protokolla. ICMP protokollaa käytetään yleensä virheiden löytämiseen tietoliikenteessä. IP protokolla itsessään ei varmista, että paketit menevät perille asti. Mahdollisessa virhetilanteessa ICMP ilmoittaa ainoastaan paketin lähteelle virheestä, koska IP paketti pitää sisällään vain tietoa lähde- ja kohdeosoitteesta. ICMP viesti on kapseloituna IP paketin dataosiossa. Yleisimpiä ICMP sovelluksia ovat ping ja

Tracert. Näistä pingiä hyödynnetään verkonvalvonnassa, koska sen avulla voidaan helposti todentaa, että valvottava kohde on tavoitettavissa. Ping hyödyntää ICMP protokollan echo request viestiä, lähdelaiteen echo request viestiin tulee kohdelaitteelta echo reply viesti, jos paketti tavoittaa kohteen virheettömästi. Tavoitettavuuden lisäksi pingillä testataan latenssia sekä hukkuuko osa paketeista matkan aikana. (Xiang 2021.)

3.4 SNMP

Verkkolaitteissa on yleensä tuki SNMP:lle. Jos laitteella on SNMP agentti, puhutaan yleensä hallitusta laitteesta. SNMP protokollaa käytetään hyödyksi, kun laitteelle ei ole mahdollista asentaa valvontasovelluksen omaa agenttia. SNMP toimii asiakas - palvelin mallilla, eli tässä yhteydessä valvontasovellus toimii palvelimena ja valvottavat kohteet, joilla on SNMP agentti asennettuna ovat asiakkaita. Valvontasovellus voi joko lähettää SNMP agentille kyselyjä tai SNMP agentti voidaan määritellä lähettämään valvontasovellukselle tietoja. Laitteen tiedot löytyvät Management Information Basesta (MIB). MIB sisältää Object Identifiereitä (OID), jotka ovat osoitteita laitteella mitkä viittaavat johonkin tietoon, kuten lämpötilaan tai laitteen käyttöaikaan. Valvontasovellus tekee SNMP kyselyjä agentilta eri komennoilla, kuten SNMP Get. SNMP agentti vastaa tähän SNMP Response:lla. Valvonnassa voidaan hyödyntää myös SNMP trap komentoja, joiden avulla voidaan määrittää SNMP agentti ilmoittamaan valvontasovellukselle välittömästi, kun laitteella tapahtuu jotain. Esimerkkitapahtumia voivat olla kytkimen portin tilan muutos tai virtalähteen sammuminen. (SNMP Monitoring Overview n.d.) SNMP trappien käyttäminen ei ole kuitenkaan aina suotavaa, sillä ne ei kerro valvottavan palvelun nykyisestä tilanteesta mitään. Kriittisissä tapauksissa, kuten virtalähteen sammumisesta on hyvä tulla tieto heti, eikä pahimmassa tapauksessa useita minuutteja myöhässä, riippuen valvontasovelluksen tarkistusvälistä.

SNMP:tä on myös mahdollista käyttää Linux järjestelmissä. Fioren (2022) mukaan SNMP käyttö Linuxilla ei ole järkevää. SNMP on nykypäivän standardeilla valvontakäytössä hidas protokolla, joka on jäänyt kehityksessä jälkeen ominaisuuksien suhteen. Ongelmaksi hän nostaa myös tietoturvan sekä UDP:n käytön kuljetusprotokollana. UDP on yhteydetön protokolla, eli pakettien perillemenoa ei voida varmistaa. Vertauksena TCP protokolla, joka varmistaa pakettien perillemenon eri mekanismeja hyödyntäen. Vaihtoehto SNMP:lle on valvonta-agentti. Yleensä jokaisella valvonta-

sovelluksella on heidän itse kehittämänsä agenttisovellus. Valvonta-agenttien etu on niiden suorituskyvyssä ja ominaisuuksien määrässä. Valvonta-agentti sovelluksia myös kehitetään huomattavasti enemmän ja ne on suunniteltu nykyajan laitteille. (Fiore 2022.)

4 Palvelimet

Palvelimien valvonnalla tarkoitetaan palvelimella olevien prosessien ja toimintojen seuraamista ja mittaamista. Palvelimia halutaan valvoa, koska yksittäisen palvelimen kaatuminen tai hitaus voi vaikuttaa koko yrityksen toimintaan, varsinkin jos sillä ajetaan jotain kriittistä palvelua. Kun valvontaohjelma havaitsee poikkeaman tai ongelman valvottavassa kohteessa, tulisi aloittaa käsittely kappaleessa 3 mainittujen prosessien mukaan. (What is server monitoring? n.d.)

Yleisimmät palvelut, joita palvelimella halutaan valvoa, ovat CPU:n käyttöaste, käytetyn muistin määrä ja levytila. Nämä liittyvät aiemmassa kappaleessa mainittuun suorityskyvyn ja kapasiteetin hallintaan, eli näiden valvonnalla halutaan havaita mahdollisia pullonkauloja suorituskyvyssä ja resursseissa sekä havaita mahdolliset ongelmat ennen vian syntymistä. Myös eri palveluita, kuten Apachea tai MySQL tietokantaa voidaan monitoroida. Esimerkiksi web-palvelimen osalta voidaan seurata HTTP pyyntöjen ja vastausten viivettä tai vastaako web-palvelin näihin pyyntöihin ollenkaan. (What is server monitoring? n.d.)

Palvelimien hallintaan on myös olemassa erilaisia hallintasovelluksia, jotka mahdollistavat esimerkiksi päivitysten asentamisen palvelimille tai uusien palvelimien asentamisen. Näissä on myös monesti oma agenttisovellus, joka mahdollistaa myös valvontaominaisuuksien käytön. Valvontasovelluksella voidaan kuitenkin nähdä palvelimen ohjelmien päivitystiedot, joten poislukien päivitysten ajamisen sekä uusien palvelimien luonnin saadaan valvontasovelluksella toteutettua myös monia hallintaan liittyviä tehtäviä. (What is server monitoring? n.d.)

4.1 Valvonta-agentti

Valvonta-agentti on sovellus, joka on asennettu valvottavalle laitteelle ja kerää valvontatarkoitukseen tietoa kyseiseltä laitteelta. Tieto, johon päästään käsiksi paikallisesti valvottavalla laitteella, voidaan välittää agentille. Agentin tehtävä on välittää kerätty data valvontapalvelimelle. Määrityksistä riippuen joko agentti välittää tämän tiedon valvontapalvelimelle tai valvontapalvelin itse kysyy tätä tietoa agentilta. Tapaa, että agentti välittää tiedon valvontapalvelimelle käytetään yleensä vain, kun valvontapalvelimella ei ole pääsyä kohdelaitteen verkkoon. (LaFlamme N.d; Monitoring Agents 2023.)

4.2 Agentiton valvonta

Agentittomalla valvonnalla tarkoitetaan monitorointia hyödyntäen standardisoituja tietoliikenneprotokollia. Yleisimmät valvonnassa hyödynnetyt protokollat ovat SNMP, ICMP ja HTTPS / HTTPS. SNMP vaatii kyllä agentin, joka on yleensä etukäteen asennettu verkkolaitteille. SNMP on kuitenkin standardisoitu protokolla, jolle on määritelty käytettäväksi UDP portit 161 ja 162 (RFC 1157:1990, 15). Agentittoman valvonnan etu on, että valvonta voidaan tehdä verkon yli ilman, että täytyy asentaa erillisiä sovelluksia, joka vähentää resurssien vaadetta kohdelaitteella. (LaFlamme n.d.)

Agentitonta valvontaa hyödynnetään yleensä, kun halutaan vain tietää, onko laite tai verkkosivusto saavutettavissa pingiä ja HTTP/HTTPS hyödyntäen. Jos kohteeseen ei saada yhteyttä, aloitetaan selvitystyö mistä tämä johtuu.

5 Vertailun pohjustus

Työssä vertaillaan kahta eri verkonvalvonta ohjelmistoa; Checkmk ja Nagios XI. Vaatimus on, että ohjelma on on-premises. Ohjelman tulee toimia täysin yrityksen omalla laitteistolla, eikä ohjelma ole esimerkiksi hostattu jonkun toisen yrityksen pilvessä.

Vertailussa halutaan kiinnittää huomiota seuraaviin asioihin:

Hinta

Onko kyseessä maksullinen vai täysin ilmainen palvelu. Miten mahdollinen hinta määräytyy, eli määräytyykö hinta esimerkiksi valvottavien palveluiden määrän mukaan. Mahdolliset eri hintaluokan versiot tuotteista ja erot niiden välillä.

Tuki

Millainen tukipalvelu tuotteella on ja onko rahaa vastaan mahdollista saada eri tason tukipalvelua. Millainen dokumentaatio tuotteella on. Millainen yhteisö tuotteella on sekä kuinka aktiivinen.

Käyttöönotto ja käyttökokemus

Kuinka helppo palvelu on ottaa käyttöön. Kuinka palveluun lisätään valvottavia kohteita ja onko mahdollisuus automatisoida esimerkiksi tietyn verkkoalueen sisällä kohteiden lisääminen. Millainen käyttöliittymä tuotteella on ja onko se helppokäyttöinen.

Valvontaominaisuudet

Miten ohjelma käytännössä suorittaa palveluiden valvomisen eri tilanteissa. Esimerkiksi soittaako agentti palvelimelle vai palvelimelle. Millaiset mahdollisuudet valvonnalle ilman agenttia.

Yhteensopivuus

Mitä kohteita ja palveluita on mahdollista valvoa ja mihin eri käyttöjärjestelmiin agentti on mahdollista asentaa. Onko mahdollisuus asentaa lisäosia, millaisia sekä kuinka laajasti niitä on saatavilla.

Järjestelmään pääsy

Onko asiakkailla mahdollisuus päästä järjestelmään niin, että näkymä on rajattu vain asiakkaan omiin palveluihin (multitenant).

Ominaisuudet

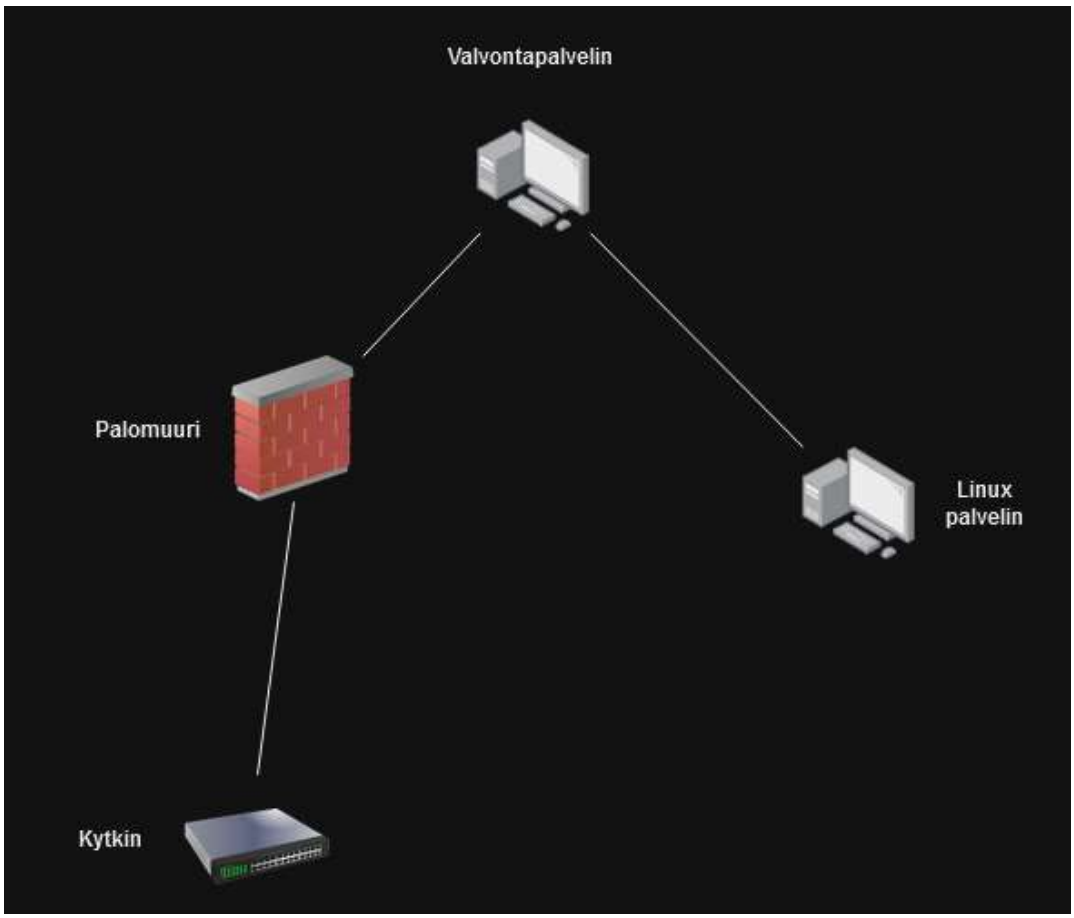
Ominaisuudet, kuten visualisointimahdollisuudet, automatisointimahdollisuudet, integraatiomahdollisuudet, tietoturva.

Merkittävät lisäominaisuudet

Onko tuotteella joitain merkittäviä lisäominaisuuksia, joita ei mahdollisesti vertailtavilla tuotteilla ole. Esimerkiksi konsolipääsy valvottavalle palvelimelle suoraan valvontaohjelman järjestelmästä.

6 Testaus

Testausta varten jokaiseen ohjelmaan lisätään valvottavaksi palomuuri, kytkin ja virtuaalipalvelin. Virtuaalipalvelimelle asennetaan MySQL tietokantasovellus ja mallitietokanta. Palomuurina toimii pfSense, jonka takana on kytkin. Kytkintä valvotaan SNMP:n avulla, koska agenttisovellusta ei ole mahdollista yleensä asentaa verkkolaitteisiin. Valvontapalvelin sekä valvottava virtuaalipalvelin sijaitsee TNNetin omalla virtuaalipalvelinalustalla. (Ks. kuvio 1.)



Kuvio 1 Testausympäristö

Testausta varten palomuurille täytyi lisätä sallintasäännöt liikenteelle valvontapalvelimelta, sekä porttiohjaus kytkimelle SNMP:tä varten, koska kytkin ja valvontapalvelin eivät ole samassa verkossa. Valvontasovelluksessa täytyy kytkimen valvonnalle määritellä eri SNMP portit kuin oletuksena, tässä tapauksessa portti 8845. Kuten kuviossa 3 nähdään, palomuurin julkisen IP-osoitteen porteista 8845 ja 8846 liikenne ohjautuu kytkimen SNMP portteihin. (Ks. kuvio 2) Kytkimeltä täytyi myös laittaa SNMP päälle sekä luoda käyttäjä, jolla on pääsy SNMP tietoihin. (Ks. kuvio 3).

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
WAN	UDP	[redacted]	*	WAN address	8845	10.52.170.20	162 (SNMP-Trap)	extreme snmp trap
WAN	UDP	[redacted]	*	WAN address	8846	10.52.170.20	161 (SNMP)	extreme snmp

Kuvio 2 Porttiohjaukset

```
jere-sw.2 # show configuration | include snmp
configure snmp sysName "jere-sw"
configure snmp sysLocation "koti"
configure snmp sysContact "Jere"
# Module snmpMaster configuration.
configure snmpv3 add user "checkmk" engine-id 80:00:07:7c:03:00:04:           authentication md5 auth-e
ncrypted localized-key 23:fc:23:88:23:              23:ff:23:03:5e:4e:37:23:e4:23:cc:79:23:a4:23:f3:7e
configure snmpv3 add group "valvonta" user "checkmk" sec-model usm
configure snmpv3 add access "valvonta" sec-model usm sec-level authnopriv read-view "defaultAdminView" w
rite-view "defaultAdminView" notify-view "defaultAdminView"
disable snmp access snmp-v1v2c
disable snmpv3 default-group
disable snmpv3 default-user
jere-sw.3 #
```

Kuvio 3 SNMP asetukset kytkimellä

7 Checkmk

Checkmk on IT-infrastruktuurin monitorointiin tarkoitettu sovellus. Checkmk:sta on saatavilla neljä eri versiota: Raw, Enterprise, Cloud ja MSP. Raw on ilmainen open source versio, joka käyttää Nagios Corea valvontamoottorina. Enterprise, Cloud ja MSP (Managed Services Edition) ovat kaupallisia versioita, joissa on käytössä Checkmk:n oma Checkmk Micro Core (CMC) valvontamoottori. Cloud versio on suunnattu yrityksille, joiden valvottavat hostit sijaitsevat pilvipalveluissa, kuten Microsoft Azuressa tai Amazon Web Servicessä. (Checkmk Pricing n.d; Setting up Checkmk 2023.)

MSP-versio mahdollistaa useiden asiakkuuksien lisäämisen niin, että heillä on omat eriytetyt järjestelmät. Useiden asiakkuuksien luominen on mahdollista myös muissa versioissa, mutta hallinta tapahtuu silti central palvelimelta ja kaikki data jaetaan kaikkien asiakkuuksien kesken. Ainoastaan tietojen näkyvyyttä voidaan rajoittaa käyttäjä tai ryhmäkohtaisesti. Checkmk Managed Services Editionilla voidaan luoda aidosti eriytettyjä asiakkuuksia, joissa jokaisella asiakkuudella on omat konfiguraatiodatat ja pääsyt vain tälle omalle sivustolle. Ainoastaan palveluntarjoajalla on pääsyt central palvelimelle, josta se voi hallita kaikkia sivustoja keskitetysti. (The Managed Services Edition 2024.)

Kaupallisissa versioissa kuukausihinta määräytyy hostien ja valvottavien palveluiden määrän mukaan. Checkmk:n laskurilla yhdellä hostilla olisi valvottavana 30 palvelua, joka on mielestäni ylimitoitettu reilusti. Palvelutason mukaan määrä on yleensä 1–10 valvottavaa palvelua per host. Hinta enterprise versiolle laskurin mukaan 1000 hostilla ja 30 000 palvelulla olisi 750 € kuukaudessa. (Checkmk Pricing n.d.)

Checkmk:n luvataan olevan yhteensopiva lähes kaikkien yleisimpien käyttöjärjestelmien kanssa eli eri Linuxien ja Windowsin, sekä esimerkiksi FreeBSD:n kanssa. (Ks. kuvio 4.)

```
OMD[valvonta]:~/share/check_mk/agents$ ls
CONTENTS                                check_mk_caching_agent.linux*
cfg_examples/                           linux/
check-mk-agent-2.2.0p24-1.noarch.rpm    mk-job*
check-mk-agent_2.2.0p24-1_all.deb       mk-job.aix*
check_mk_agent.aix*                     mk-job.solaris*
check_mk_agent.freebsd*                 mk-remote-alert-handler*
check_mk_agent.hpux*                    plugins/
check_mk_agent.linux*                   sap/
check_mk_agent.macosx*                  scripts/
check_mk_agent.netbsd*                  special/
check_mk_agent.openbsd*                 waitmax*
check_mk_agent.openvms*                 windows/
check_mk_agent.openwrt*                 z_os/
check_mk_agent.solaris*
```

Kuvio 4 Checkmk agentit

7.1 Asennus

Checkmk käyttää Open Monitoring Distributionia, jonka avulla saa yhdellä DEB tai RPM packagella asennettua valmiin monitorointijärjestelmän kaikilla tarvittavilla komponenteilla valmiiksi konfiguroituna. (Ks. kuvio 5.) OMD mahdollistaa esimerkiksi useiden asiakkuuksien ajamisen rinnakkain samalla palvelimella. (The Open Monitoring Distribution n.d.)

```
OMD[valvonta]:~$ omd status
agent-receiver: running
mkeventd:       running
liveproxyd:     running
mknotifyd:      running
rrdcached:      running
cmc:            running
apache:         running
dcd:            running
redis:          running
crontab:        running
----------------------
Overall state:  running
```

Kuvio 5 Checkmk komponentit

Asennus tapahtuu lataamalla Checkmk:n sivuilta asennuspaketti, tässä tapauksessa DEB paketti, koska valvontapalvelin on Ubuntu, joka on Debian pohjainen. Asennuksen jälkeen varmistetaan, että se on onnistunut. Tämän jälkeen luodaan OMD sivusto ja käynnistetään se. Alla komennot, jotka ajettiin:

```
wget https://download.checkmk.com/checkmk/2.2.0p24/check-mk-cloud2.2.0p24_0.jammy_amd64.deb
sudo apt update
sudo apt install ./check-mk-cloud-2.2.0p24_0.jammy_amd64.deb
omd version
sudo omd create valvonta
sudo omd start valvonta
```

Tämän jälkeen valvontasovelluksen graafiseen käyttöliittymään pääsee osoitteesta: http://palveli-menip/valvonta

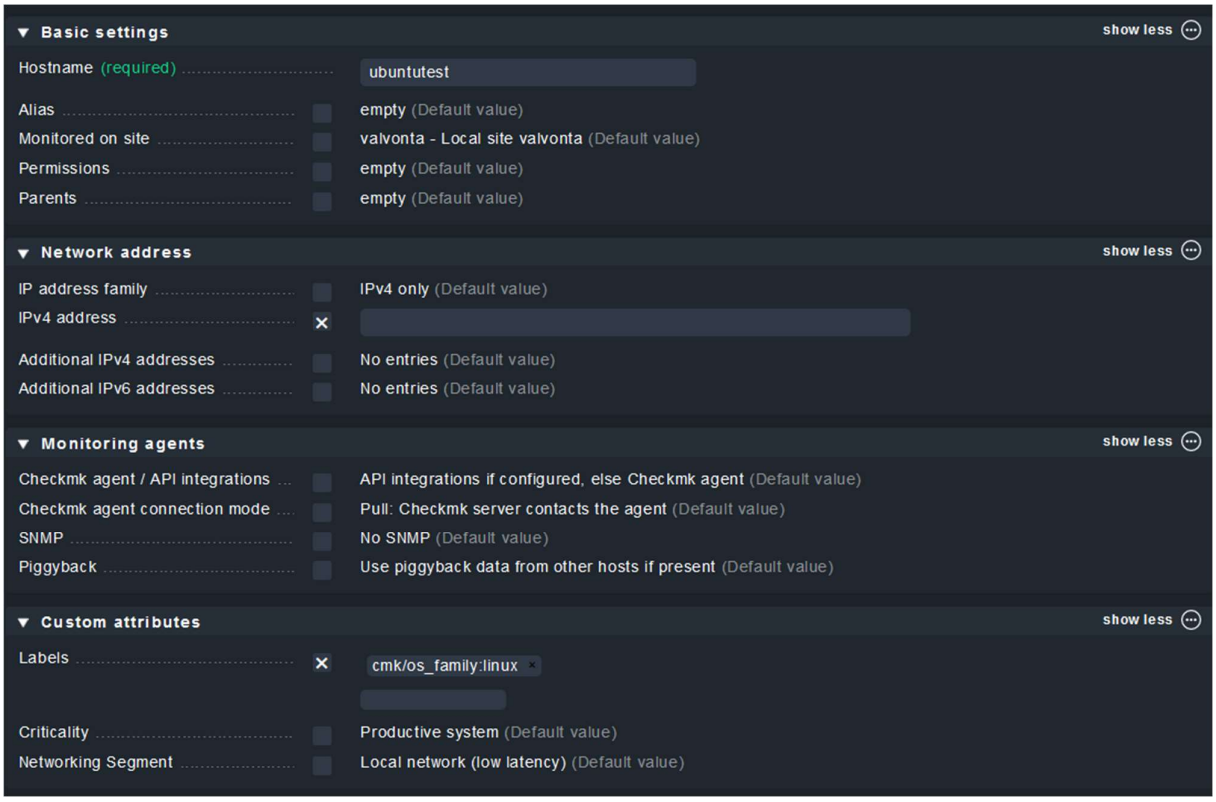
Checkmk agenttisovellus asennetaan valvottavalle Ubuntu virtuaalipalvelimelle sekä pfSense palo-muurille. PfSense on FreeBSD pohjainen, joten agentti on myös mahdollista asentaa sille.

7.2 Agentin asennus Ubuntu palvelimelle

Agentin asennus asennus tapahtuu seuraavilla komennoilla:

```
sudo wget http://<palvelimenip>/testmonitoring/check_mk/agents/check-mk-agent_2.2.0p9-1_all.deb
sudo dpkg -i check-mk-agent_2.2.0p9-1_all.deb
```

Valvottava palvelin pitää lisätä valvontajärjestelmään. Tässä annetaan hostille nimi sekä sen IP-osoite. Muita säädettäviä asetuksia on esimerkiksi, käytetäänkö valvonta-agenttia, SNMP:tä vai jotain muuta. Tässä kohtaa voi myös laittaa hostille tunnisteita, joiden avulla voidaan esimerkiksi lisätä sääntöjä tämän tunnisteen mukaan. Tunnisteita voi luoda vapaasti, kunhan ne ovat muotoa ”key:value”. (Ks. kuvio 6.)



Kuvio 6 Checkmk hostin lisäys

Agentin rekisteröinti valvontapalvelimelle, ajetaan seuraava komento valvottavalla palvelimella:

*cmk-agent-ctl register --hostname ubuntutest *
*--server <valvontapalvelimenip> --site valvonta *
--user cmkadmin --password 'salasana'

Agentin onnistunut asennus ja yhteys valvontapalvelimelle varmistetaan komennolla (Ks. kuvio 7.):

cmk-agent-ctl status

```
Version: 2.2.0p24
Agent socket: operational
IP allowlist: any


Connection:             /valvonta
        UUID: eddcbbaa-af03-4375-a781-c4d2f794421c
        Local:
                Connection mode: pull-agent
                Connecting to receiver port: 8000
                Certificate issuer: Site 'valvonta' agent signing CA
                Certificate validity: Tue, 09 Apr 2024 07:18:42 +0000 - Mon, 09
Apr 2029 07:18:42 +0000
        Remote:
                Connection mode: pull-agent
                Hostname: ubuntutest
```

Kuvio 7 Checkmk agentin tila palvelimella

7.3 Agentin lisääminen palomuurille

Checkmk agentti on mahdollista asentaa myös FreeBSD käyttöjärjestelmälle. Asennus PfSenselle vaati kuitenkin hieman manuaalista työtä. Aluksi PfSenselle pitää asentaa bash, koska agentti sisältää syntaksia, joka ei ole suoraan yhteensopiva FreeBSD:n käyttämän Bourne Shellin kanssa. FreeBSD agenttia kutsutaan xinetd superserverin kautta. (Monitoring FreeBSD, 2022.) Bashin asennus onnistuu komennolla:

pkg install bash

Agentti ladataan Checkmk valvontapalvelimelta komennolla:

wget -0/opt/bin/check_mk_agent.freebsd http://<palvelimenip>/valvonta/check_mk/agents/check_mk_agent.freebsd

Xinetd konfiguraatiolla (Ks. liite 1) luodaan oma tiedosto polkuun: /opt/etc/xinetd.d/check_mk.

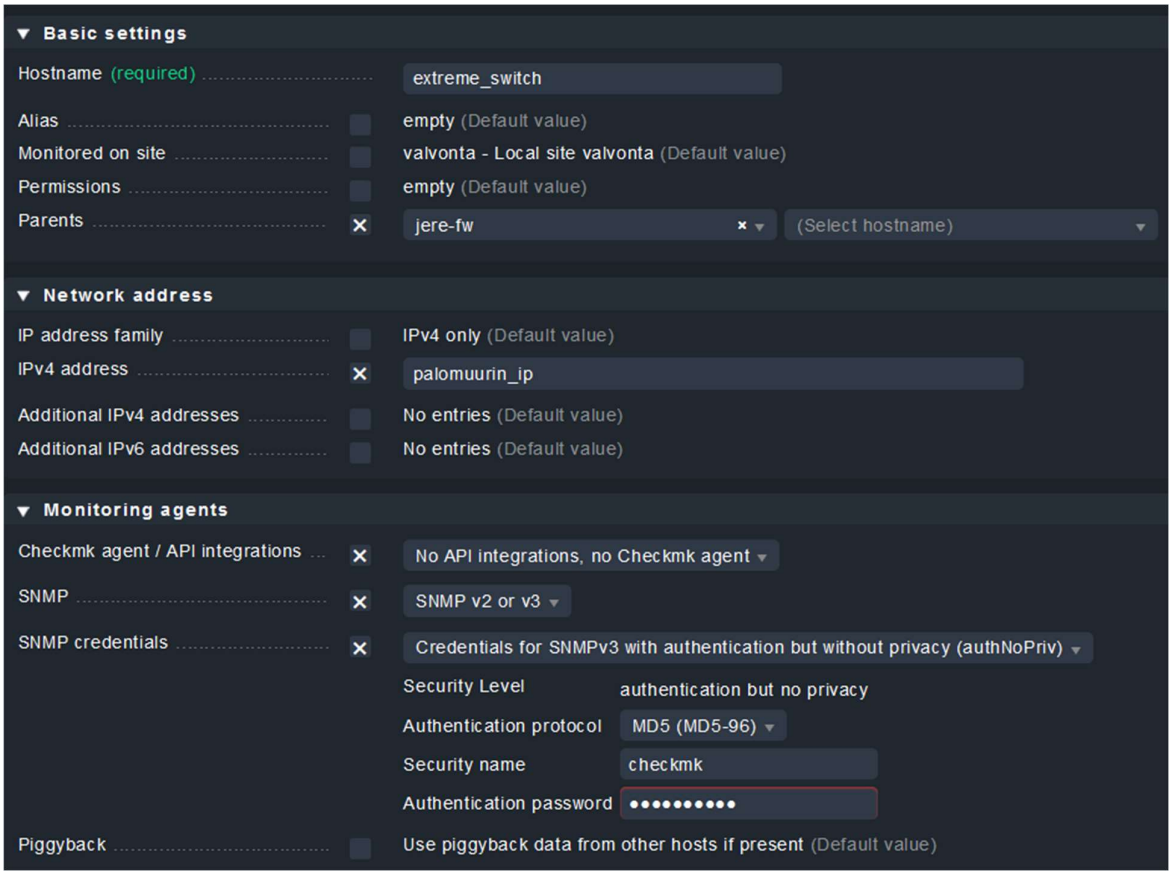
Tämä tiedosto sisällytetään PfSensen filter reload toimintoon kohtaan, jossa generoidaan uusi xinetd.conf tiedosto, koska muuten aina kun PfSensellä tehdään muutos, xinetd konfiguraatiotiedosto generoidaan uudelleen ja muualla kuin oletuspoluissa olevat konfiguraatiot jätetään huomioimatta. Lisätään polussa /etc/inc/filter.inc tiedostoon rivi:

fwrite($xinetd_fd, "includedir /opt/etc/xinetd.d");

Nyt palomuuri voidaan lisätä valvontaan samalla periaatteella, kuin aiemmin lisätty Ubuntu palvelin.

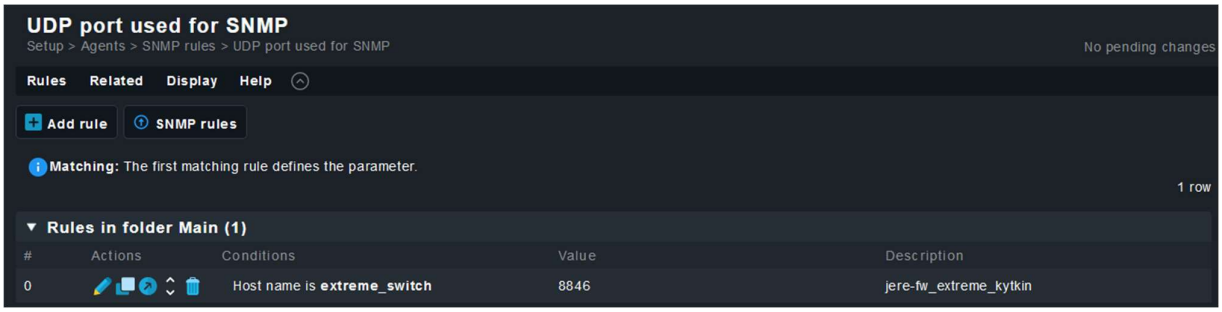
7.4 Kytkimen lisääminen valvontaan (SNMP valvonta)

SNMP:llä valvottava laite lisätään samalla tavalla kuin aiemmin näytetty Ubuntu palvelin, jota valvottiin Checkmk agentilla. Valvonta-agentiksi määritellään vain SNMP agentti sekä täytetään aiemmin kytkimelle kuviossa 4 määritellyt tunnukset ja salasana SNMP käyttöä varten. (Ks. kuvio 3 ja 8)



Kuvio 8 SNMP:llä valvottavan laitteen lisäys

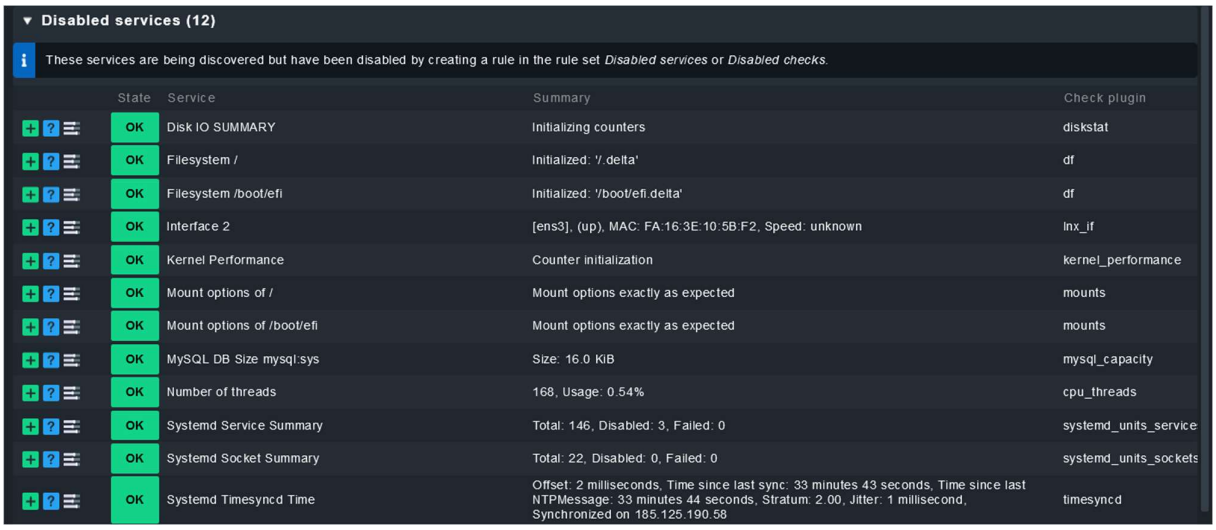
Tämän lisäksi lisätylle hostille pitää lisätä sääntö, jossa määritetään mitä UDP porttia SNMP käyttää, koska kytkin sijaitsee palomuurin takana. (Ks. kuvio 9) Kytkimelle oli tehty palomuurilla porttiohjaus palomuurin julkisesta IP-osoitteesta portista 8846 kytkimen IP-osoitteen porttiin 161.



Kuvio 9 UDP portin määritys SNMP:lle

7.5 Käyttö

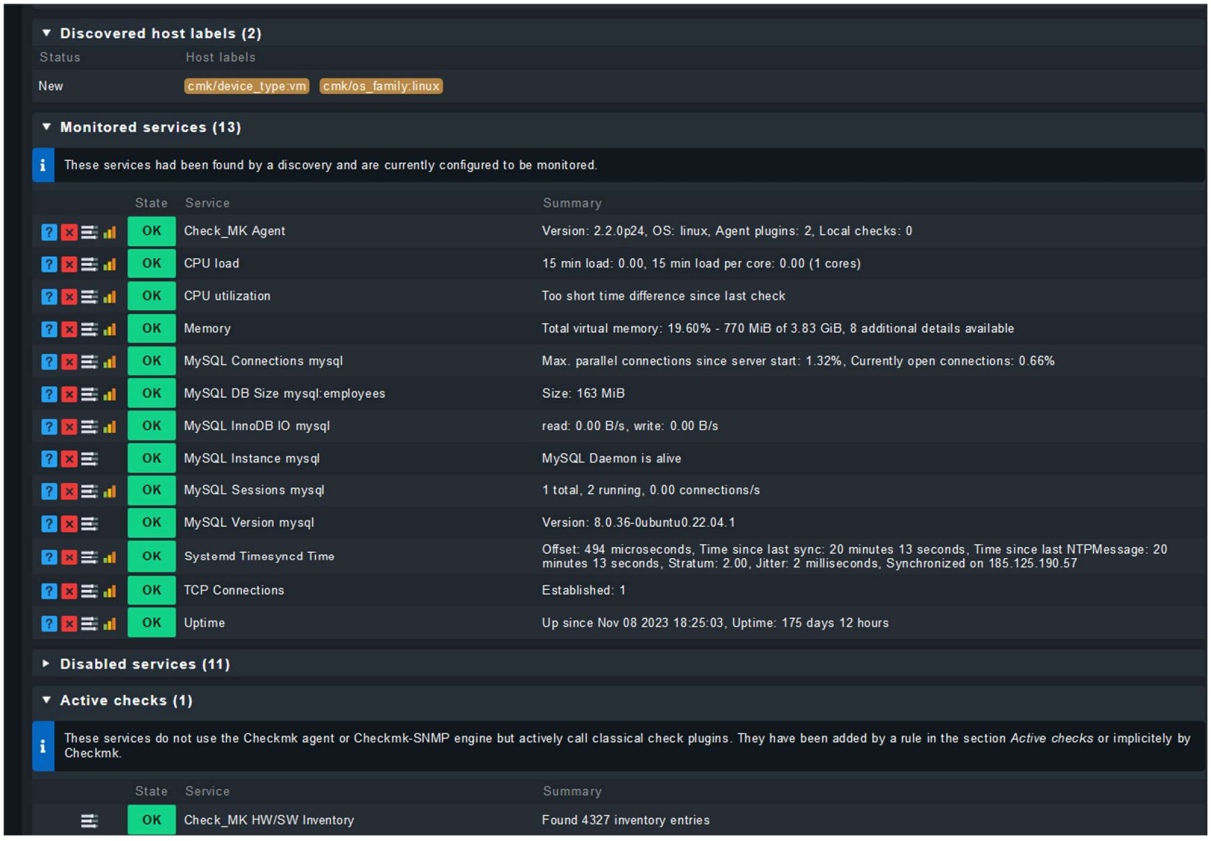
Agentin lisäämisen jälkeen agentti havaitsee automaattisesti palveluita, kuten CPU:n, muistin ja levytilan käyttö. Tässä kohtaa voi poistaa ylimääräisiä palveluita valvonnasta, jolloin ne siirtyvät kohtaan ”Disabled services”. (Ks. kuvio 10.)



Kuvio 10 Valvonnasta poistetut palvelut

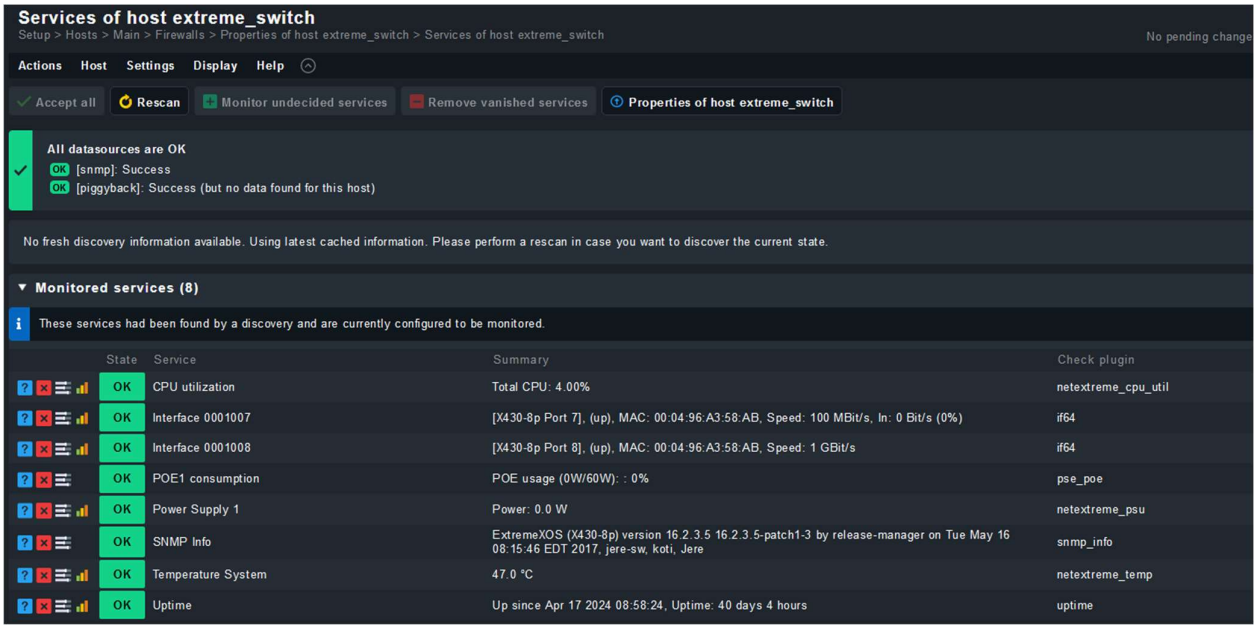
Muita palveluita voidaan lisätä myös sääntöjen ja lisäosien avulla. Valvottavalla Ubuntu palvelimella on asennettu MySQL tietokanta sekä sinne käyttäjä, jolla on oikeudet valita ja lukea tietokantoja. Tämän valvontaa varten pitää palvelimelle ladata mk_mysql -lisäosa valvontapalvelimelta komennolla: wget http://<palvelimenip>/valvonta/check_mk/agents/plugins/mk_mysql. Tämä tiedosto siirretään palvelimella kansioon /usr/lib/check_mk_agent/plugins. Tämän jälkeen täytyy

vielä tehdä konfiguraatiotiedosto polkuun /etc/check_mk/mysql.cfg, jonne määritellään tietokantakäyttäjä ja salasana. Nyt kun ajetaan service discovery uudelleen, pitäisi sieltä löytyä MySQL palveluja, joita voidaan lisätä valvontaan. (Ks. kuvio 11.)



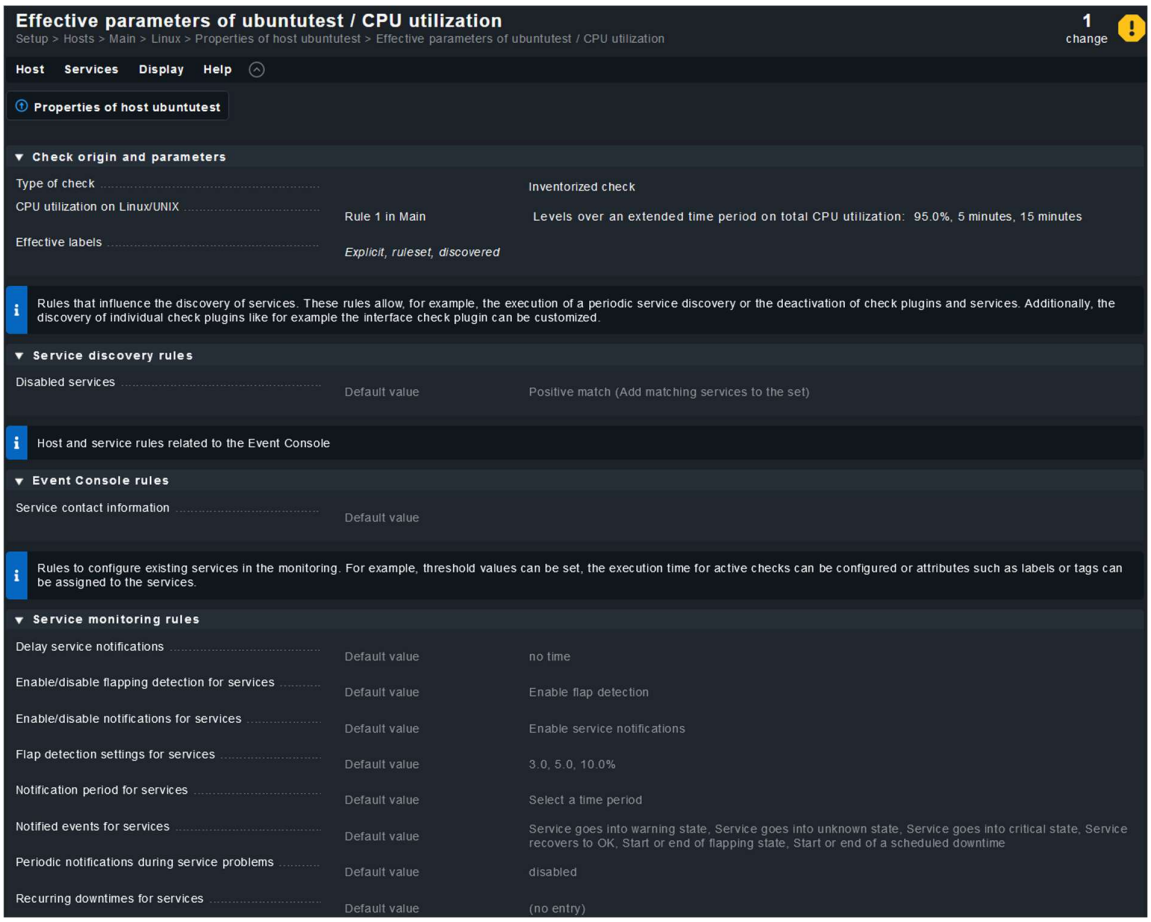
Kuvio 11 Ubuntu palvelimen valvottavat palvelut

SNMP:llä löydetyt palvelut eroavat Checkmk agentin löytämistä palveluista. Oletuksena Checkmk lisää valvontaan vain portit, joissa on linkki aktiivisena. (Ks. kuvio 12)



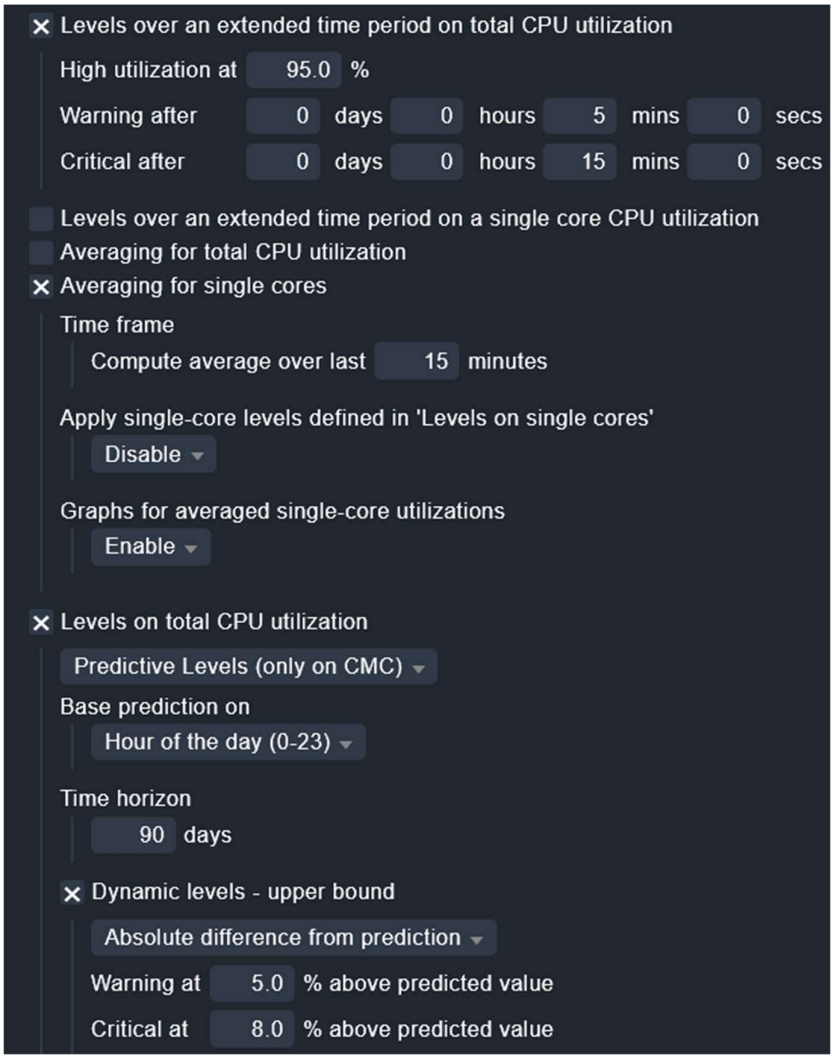
Kuvio 12 Checkmk SNMP palvelut

Palveluiden parametrejä pääsee tarkastelemaan ja muokkaamaan menemällä näkymään, josta näkyy kaikki hostin valvotut palvelut tai menemällä service monitoring rules -kohtaan. Parametrien muokkaus tapahtuu sääntöjen avulla. Kuviosta 14 nähdään osa CPU käytölle määritellyistä parametreista. Suurin osa on oletusarvolla, mutta esimerkiksi CPU:n käyttöasteen raja-arvoa on muutettu. (Ks. kuvio 13.)



Kuvio 13 Checkmk palvelun parametrit

Raja-arvoksi on määritelty 95 %, jos CPU käyttö on 95 % viiden minuutin ajalta, menee palvelu varoitustilaan ja 15 minuutin jälkeen palvelu menee kriittiseen tilaan. Checkmk CMC valvontamoottorilla on myös mahdollista määritellä ennustettu taso CPU käyttöasteelle, joka voidaan asettaa esimerkiksi tunti- tai päiväperusteiseksi. Jos käyttö poikkeaa tästä ennusteesta, menee palvelu varoitus- tai vikatilaan. (Ks. kuvio 14.) Kaikkia parametrien sääntöjä voidaan muuttaa joko hostkohtaisesti tai esimerkiksi ryhmän mukaan.



Kuvio 14 Checkmk palveluiden valvonnan sääntöjen muokkausta

Kaikille valvottaville kohteille lisättiin myös Check_MK HW/SW Inventory, tällä saadaan tietoa valvottavan kohteen ohjelmistoista ja laitteistoista. Kaikki tiedot voidaan katsoa laitekohtaisesti yhdeltä sivulta tai filteröidä esimerkiksi jonkun tietyn sovelluksen versiotiedot kaikilta laitteilta. (Ks. kuvio 15.)

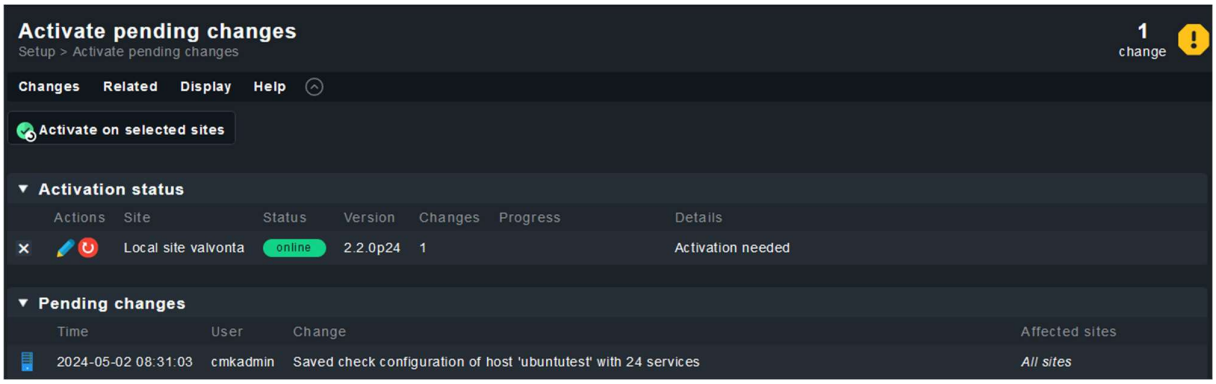
Kuvio 15 Ubuntu palvelimen inventory

Kytkimeltä saadaan HW/SW inventory -palvelulla näkyviin esimerkiksi tiedot kytkinporttien tilasta ja kytkimelle konfiguroiduista VLANeista (Virtual LAN). (Ks. kuvio 16.)

Host	Index	Description	Alias	Operational Status	Administrative Status	Port Usage	Speed	Last Change	Type	Phys
extreme_switch	1001	X430-8p Port 1		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1002	X430-8p Port 2		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1003	X430-8p Port 3		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1004	X430-8p Port 4		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1005	X430-8p Port 5		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1006	X430-8p Port 6		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1007	X430-8p Port 7		up	up	used	100 Mbit/s		6 - ethernetCsmacd	00:04
extreme_switch	1008	X430-8p Port 8		up	up	used	1 Gbit/s		6 - ethernetCsmacd	00:04
extreme_switch	1009	X430-8p Port 9		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1010	X430-8p Port 10		down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1011	Management Port	MgmtPort	down	up	used	0 bit/s		6 - ethernetCsmacd	00:04
extreme_switch	1000001	VirtualRouter0		up	up		0 bit/s		53 - propVirtual	
extreme_switch	1000002	VirtualRouter1		up	up		0 bit/s		53 - propVirtual	
extreme_switch	1000003	VirtualRouter2		up	up		0 bit/s		53 - propVirtual	
extreme_switch	1000004	VLAN 00001 (Default)		up	up		0 bit/s		53 - propVirtual	
extreme_switch	1000005	VLAN 04095 (Mgmt)	Management VLAN	down	up		0 bit/s		53 - propVirtual	
extreme_switch	1000010	rtif(10.52.170.20/24)		up	up		0 bit/s		53 - propVirtual	00:04
extreme_switch	1000011	VLAN 00400 (testi)		down	up		0 bit/s		53 - propVirtual	

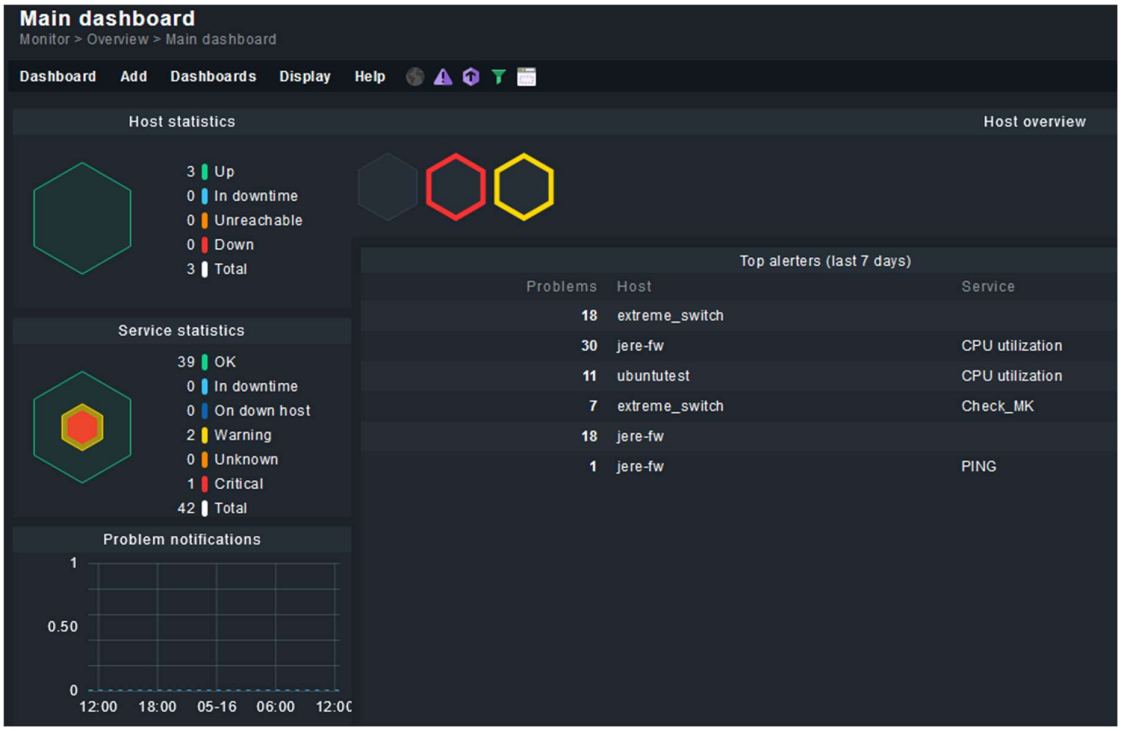
Kuvio 16 Kytkimen rajapinnat

Muutosten jälkeen muutokset eivät mene suoraan tuotantoon, vaan ne ovat avoimena, kunnes ne aktivoidaan. Konfiguraatiomuutosten jälkeen sivun oikeaan yläkulmaan tulee ilmoitus muutoksesta, jota painamalla pääsee aktivointisivulle. (Ks. kuvio 17.)



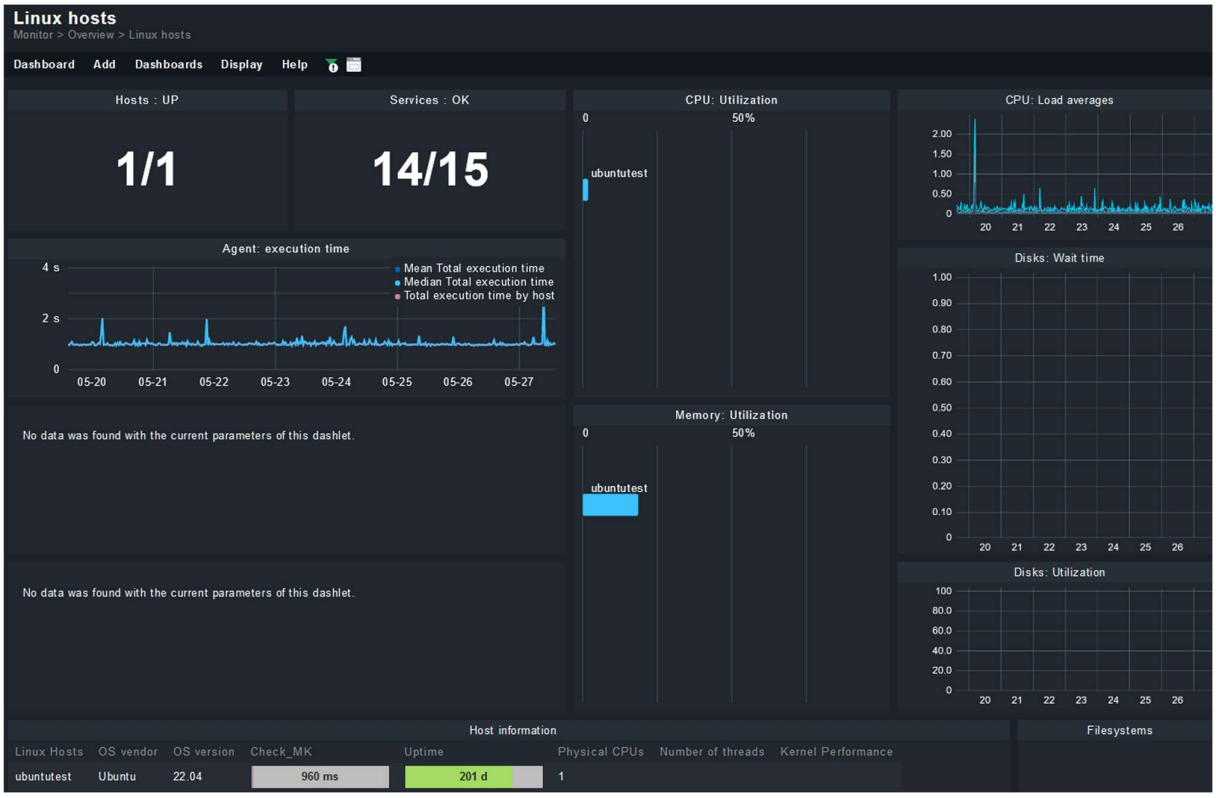
Kuvio 17 Checkmk näkymä avoimista muutoksista

Nyt testausympäristö on kokonaisuudessaan lisätty valvontasovellukseen. Etusivulta nähdään oletusnäkymästä, että valvontasovelluksella on kolme hostia ja yhteensä 42 palvelua valvonnassa. (Ks. kuvio 18)



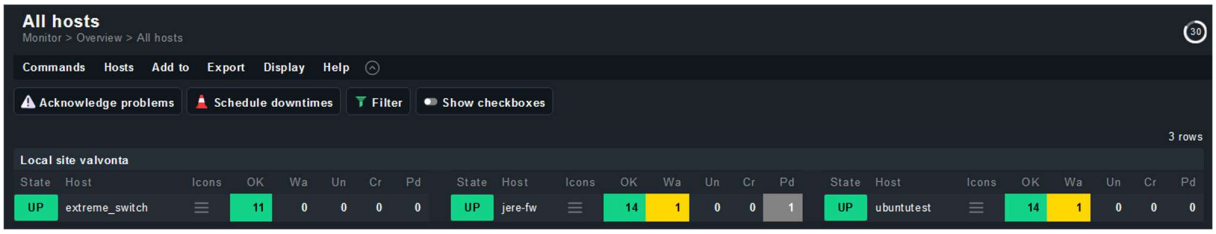
Kuvio 18 Checkmk etusivunäkymä

Dashboard näkymiä on myös mahdollista muokata sekä luoda omille ryhmille omat dashboardit. Esimerkiksi Ubuntu testipalvelin on lisätty Linux ryhmään ja tälle ryhmälle on tehty oma dashboard näkymä. (Ks. kuvio 19) Avaamalla dashboard näkymästä yksittäisen hostin, avautuu sille samanlainen näkymä, johon voi muokata näkymään esimerkiksi graafeja eri palveluista.



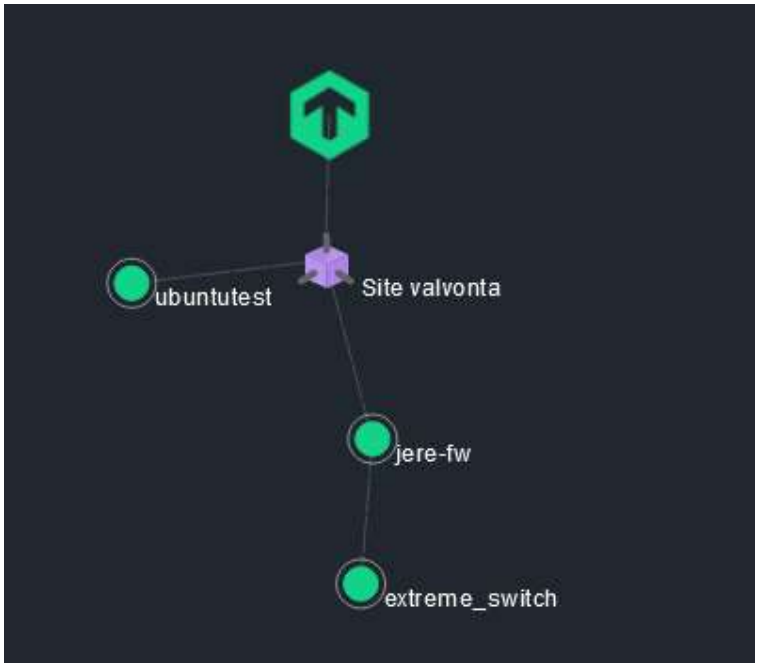
Kuvio 19 Checkmk Linux hosts dashboard

All hosts -välilehdeltä nähdään hostkohtaisesti niiden tila. Tästä näkymästä nähdään tiivistetysti, onko host ylhäällä sekä mikä on hostin valvottujen palveluiden tilanne. Painamalla keltaisella taustalla olevaa varoitusilmoitusta, avautuu kaikki sen hostin palvelut, jotka ovat kyseisessä tilassa. (Ks. Kuvio 20.) Problem dashboardilta nähdään kaikki hostit ja palvelut, jotka ovat joko varoitus- tai vikatilassa.



Kuvio 20 Checkmk hostien tila

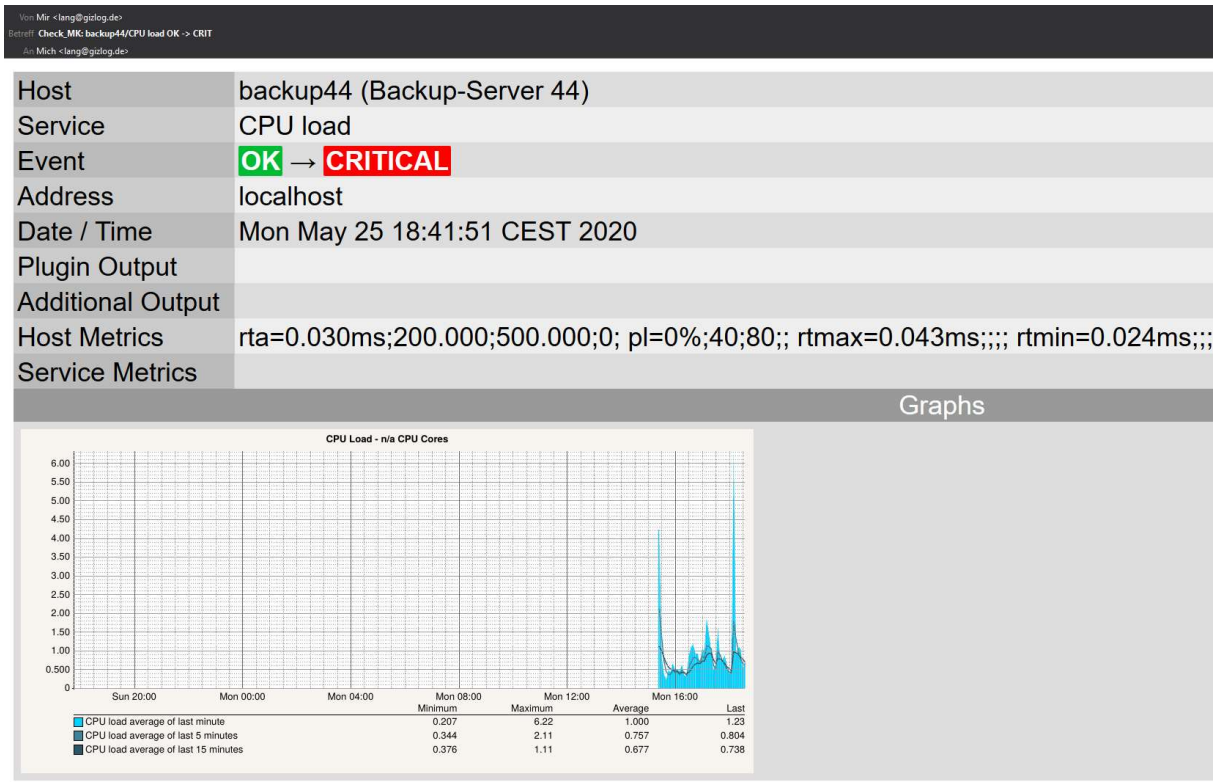
Kaikki valvonnassa olevat hostit voidaan esittää verkkotopologiana. Topologia esitetään valvontapalvelimen näkökulmasta ja se perustuu parent – child suhteeseen. Hostin lisäämisen yhteydessä sille voidaan manuaalisesti määrittää yksi tai useampi vanhempi. Tämä voidaan tehdä myös automaattisella skannauksella. Parent scan -ominaisuus suorittaa tracerouten, jonka perusteella katsotaan, mikä on viimeinen yhdyskäytäväosoite valvontapalvelimen näkökulmasta, tai hostilta katsottuna sen oletusyhdyskäytävä. Jos tämä löydetty yhdyskäytävä ei ole jo lisättynä valvontaan, luodaan tälle automaattisesti uusi host, jota valvotaan pelkällä pingillä. Jos hostilla on julkinen ip-osoite, kuten testiympäristössä palomuurilla, niin automaattinen skannaus lisää valvottavaksi internet palveluntarjoajan yhdyskäytävän Tämän valvominen pingillä ei ole tarpeellista, koska kyseisen laitteen toimintaan ei voida vikatilanteessa vaikuttaa. (Ks. kuvio 21.)



Kuvio 21 Checkmk Valvontaympäristön topologia

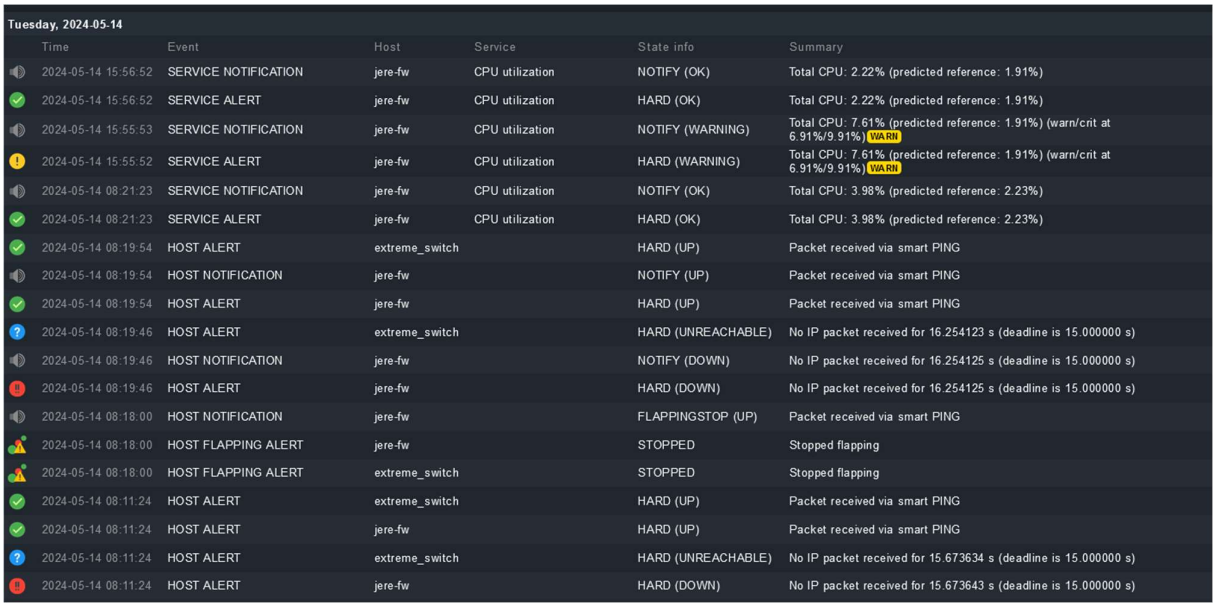
7.6 Tapahtumat, ilmoitukset ja raportointi

Yksi valvontasovelluksen tärkeimmistä ominaisuuksista on tapahtumien ja ilmoitusten hallinta. Jatkuva tapahtumien seuraaminen valvontasovelluksen käyttöliittymästä ei ole mahdollista tai järkevää, joten vioista ja varoituksista täytyy tulla ilmoituksia halutuille henkilöille. Checkmk:lla ilmoituksia on mahdollista lähettää sähköpostilla ja tekstiviestillä. Ilmoituksia on myös mahdollista lähettää keskusteluohjelmiin kuten Microsoft Teamsiin tai eri tikettijärjestelmiin. Kuviosta 22 nähdään esimerkki Checkmk:n lähettämästä ilmoituksesta. Ilmoituksia on mahdollista hallita monipuolisesti sääntöjen avulla. Esimerkiksi lähetetäänkö ilmoituksia, kun palvelu varoitustilassa tai millä ajanjaksolla ilmoituksia lähetetään. Palvelukohtaisesti ilmoituksia voidaan myös viivästyttää, esimerkiksi jos tiedetään, että jokin palvelu menee vikatilaan usein, mutta palautuu hetken kuluttua. Jos palvelulle on asetettu ilmoituksen lähetykseen minuutin viive ja se palautuu tämän aikana, ilmoitusta ei lähetetä, jos vika on edelleen aktiivinen minuutin jälkeen, lähtee ilmoitus eteenpäin.



Kuvio 22 Checkmk esimerkki sähköposti-ilmoituksesta (Notifications, n.d.)

Host & service events -välilehdeltä nähdään kaikki tapahtumat. Tapahtumia ovat esimerkiksi hälytykset, lähetetyt ilmoitukset ja palveluiden tai hostien palautumiset. Historiassa näkyy ”flapping” tapahtumia, jolla tarkoitetaan, että palvelun tai hostin tila hyppii tilasta toiseen. Checkmk tunnistaa tämän automaattisesti ja lopettaa ilmoitusten lähettämisen, kunnes flapping loppuu. (Ks. kuvio 23.)



Tuesday, 2024-05-14

Time	Event	Host	Service	State info	Summary
2024-05-14 15:56:52	SERVICE NOTIFICATION	jere-fw	CPU utilization	NOTIFY (OK)	Total CPU: 2.22% (predicted reference: 1.91%)
2024-05-14 15:56:52	SERVICE ALERT	jere-fw	CPU utilization	HARD (OK)	Total CPU: 2.22% (predicted reference: 1.91%)
2024-05-14 15:55:53	SERVICE NOTIFICATION	jere-fw	CPU utilization	NOTIFY (WARNING)	Total CPU: 7.61% (predicted reference: 1.91%) (warn/crit at 6.91%/9.91%) WARN
2024-05-14 15:55:52	SERVICE ALERT	jere-fw	CPU utilization	HARD (WARNING)	Total CPU: 7.61% (predicted reference: 1.91%) (warn/crit at 6.91%/9.91%) WARN
2024-05-14 08:21:23	SERVICE NOTIFICATION	jere-fw	CPU utilization	NOTIFY (OK)	Total CPU: 3.98% (predicted reference: 2.23%)
2024-05-14 08:21:23	SERVICE ALERT	jere-fw	CPU utilization	HARD (OK)	Total CPU: 3.98% (predicted reference: 2.23%)
2024-05-14 08:19:54	HOST ALERT	extreme_switch		HARD (UP)	Packet received via smart PING
2024-05-14 08:19:54	HOST NOTIFICATION	jere-fw		NOTIFY (UP)	Packet received via smart PING
2024-05-14 08:19:54	HOST ALERT	jere-fw		HARD (UP)	Packet received via smart PING
2024-05-14 08:19:46	HOST ALERT	extreme_switch		HARD (UNREACHABLE)	No IP packet received for 16.254123 s (deadline is 15.000000 s)
2024-05-14 08:19:46	HOST NOTIFICATION	jere-fw		NOTIFY (DOWN)	No IP packet received for 16.254125 s (deadline is 15.000000 s)
2024-05-14 08:19:46	HOST ALERT	jere-fw		HARD (DOWN)	No IP packet received for 16.254125 s (deadline is 15.000000 s)
2024-05-14 08:18:00	HOST NOTIFICATION	jere-fw		FLAPPINGSTOP (UP)	Packet received via smart PING
2024-05-14 08:18:00	HOST FLAPPING ALERT	jere-fw		STOPPED	Stopped flapping
2024-05-14 08:18:00	HOST FLAPPING ALERT	extreme_switch		STOPPED	Stopped flapping
2024-05-14 08:11:24	HOST ALERT	extreme_switch		HARD (UP)	Packet received via smart PING
2024-05-14 08:11:24	HOST ALERT	jere-fw		HARD (UP)	Packet received via smart PING
2024-05-14 08:11:24	HOST ALERT	extreme_switch		HARD (UNREACHABLE)	No IP packet received for 15.673634 s (deadline is 15.000000 s)
2024-05-14 08:11:24	HOST ALERT	jere-fw		HARD (DOWN)	No IP packet received for 15.673643 s (deadline is 15.000000 s)

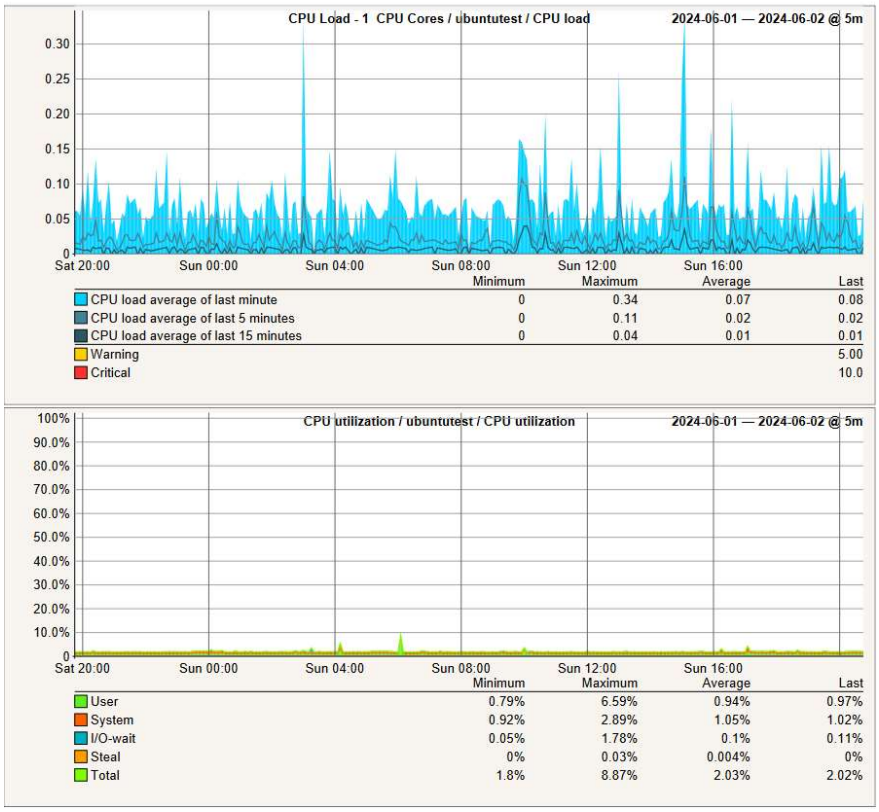
Kuvio 23 Checkmk valvontatapahtumia

Hosteilta on mahdollista nähdä tietoja raporttimuodossa. Yleisraportti näyttää PDF-muodossa viimeisimmät tapahtumat hostilla sekä palveluiden saatavuuden, myös pelkät saatavuustiedot voidaan näyttää raporttimuodossa. Hostin suorituskykyraportti näyttää graafimuodossa statistiikkaa kaikista valvotuista palveluista. (Ks. kuvio 24.)

Report of Host Performance Graphs ubuntutest

Report created 2024-06-02 20:47:38 by cmkadmin (cmkadmin)
Timerange: Today - from 2024-06-02 00:00:00 until 2024-06-02 20:47:38

Last 25 hours



Kuvio 24 Checkmk Hostin suorituskykyraportti

8 Nagios XI

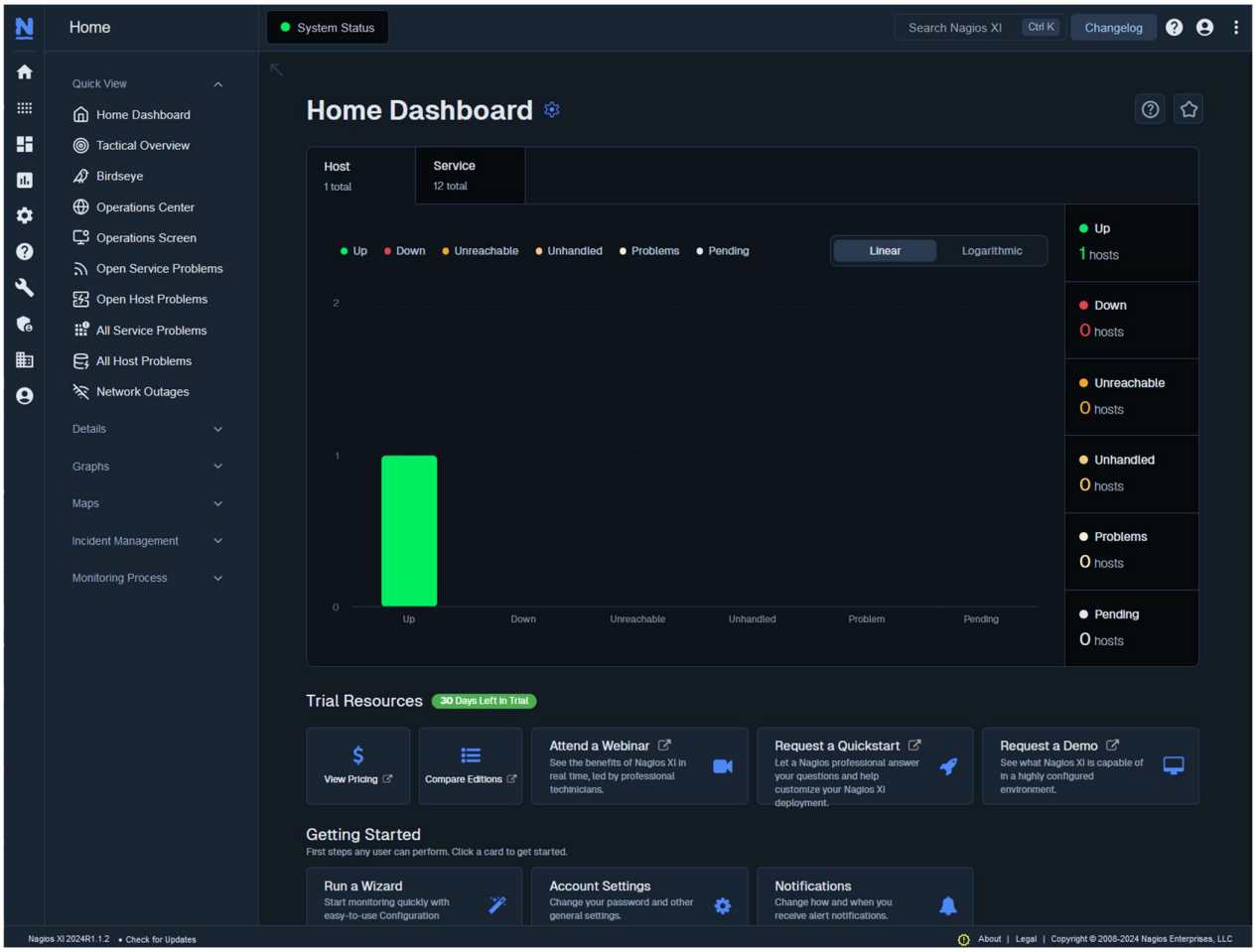
Nagios XI on verkkonvalvontasovellus, joka perustuu Nagios Core 4 valvontamoottoriin. Sovellus sisältää valvonnan lisäksi ominaisuuksia kuten graafisen web-käyttöliittymän, hallintatyökaluja sekä datan visualisointityökaluja. Nagios XI:stä on saatavilla neljä eri versioita: Free, Standard, Enterprise ja Sitewide. Ilmaisversio sisältää 7 valvottavaa hostia tai 100 valvottavaa palvelua sekä melkein kaikki ominaisuudet seuraavasta Standard versiosta. Standard versiosta puuttuu lähinnä hallintaominaisuuksia verrattuna Enterprise versioon. Standard ja Enterprise lisenssit sallivat kolme asennusta; itse tuotantopalvelin, backup/failover palvelin sekä testausympäristön. Sitewide lisenssillä saa useita rajoittamattomia asennuksia. Kaikki lisenssit ovat kertamaksullisia, Standard lisenssi 500 hostilla maksaa 8495 dollaria ja Enterprise lisenssi 500 hostilla 10490 dollaria. Rajoittamattomilla hostien määrillä hinnat ovat 23995 ja 25990 dollaria. (Nagios XI n.d; Nagios XI // Licensing Policy n.d.)

8.1 Asennus

Nagios XI:n asennus tapahtuu seuraavilla komennoilla:

```
wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
tar xzf xi-latest.tar.gz
cd nagiosxi
sudo ./fullinstall
```

Kun asennusskripti on valmis, tulee siitä ilmoitus, jonka jälkeen web käyttöliittymään pääse osoitteesta: http://<palvelimenip>/nagiosxi. Kuviossa 16 näkyy oletusnäkymä tuoreelle asennukselle. Valvontaan on lisätty oletuksena localhost, eli itse valvontapalvelin. (Ks. kuvio 25)

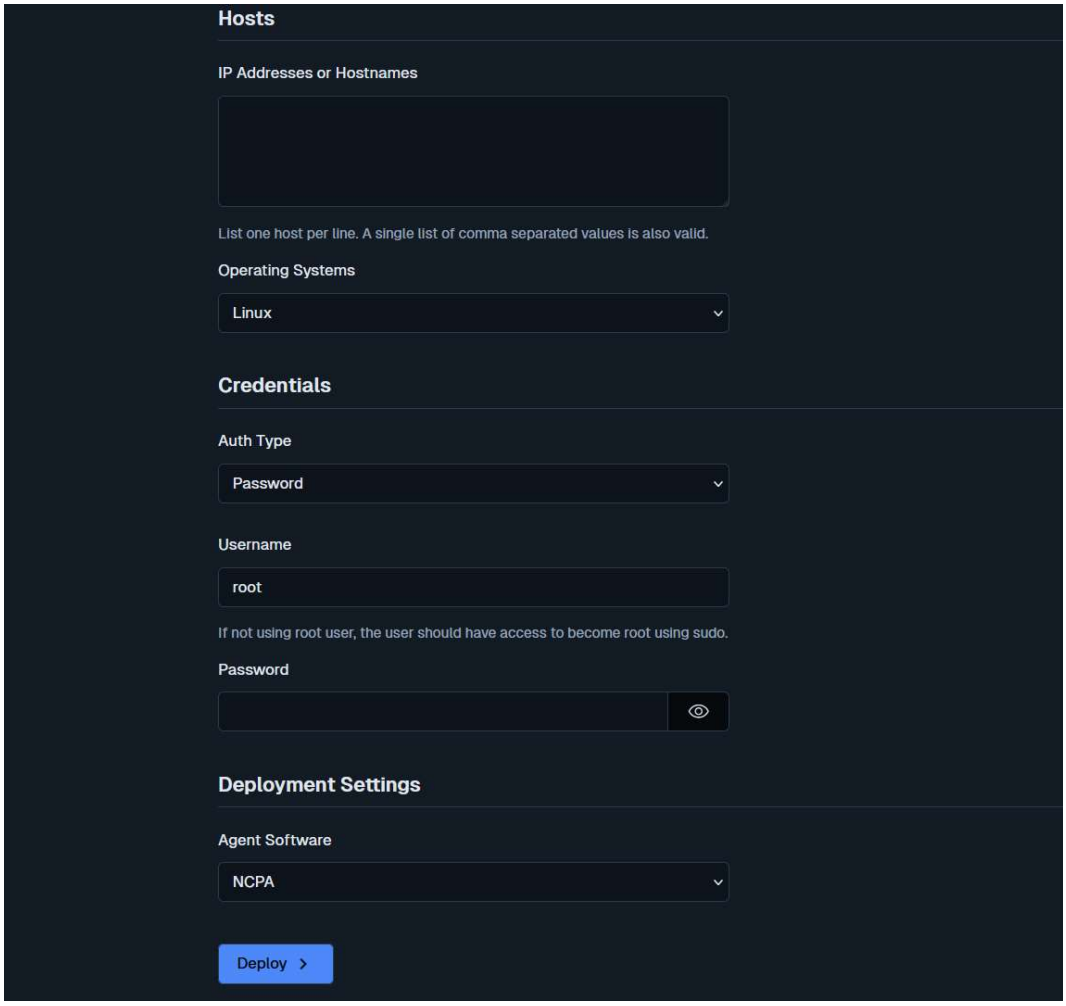


Kuvio 25 Nagios oletusdashboard etusivulla

8.2 Agentin asennus

Nagios XI käyttää oletuksena NCPA (Nagios Cross-Platform Agent) agenttia, josta on saatavilla virralliset versiot seuraaville käyttöjärjestelmille: Windows, MacOS sekä RHEL ja Debian Linux jakelut. NCPA on Python pohjainen, eli käytännössä se kykenee toimimaan melkein millä tahansa käyttöjärjestelmällä. (Nagios Cross-Platform Agent n.d.)

NCPA asennetaan samalle Ubuntu testipalvelimelle, jota käytettiin Checkmk:n kanssa. Nagios XI:llä on mahdollista ottaa agentti automaattisesti käyttöön käyttöliittymän kautta. (Ks. kuvio 26) Tässä näkymässä ei kuitenkaan ollut mahdollista määrittää SSH-avainpareja, niin asennus tehtiin manuaalisesti.



Kuvio 26 Agentin asennus käyttöliittymän kautta

Manuaalinen asennus onnistuu lataamalla NCPA valvottavalle palvelimelle. Asennus tehtiin DEB paketin avulla seuraavilla komennoilla:

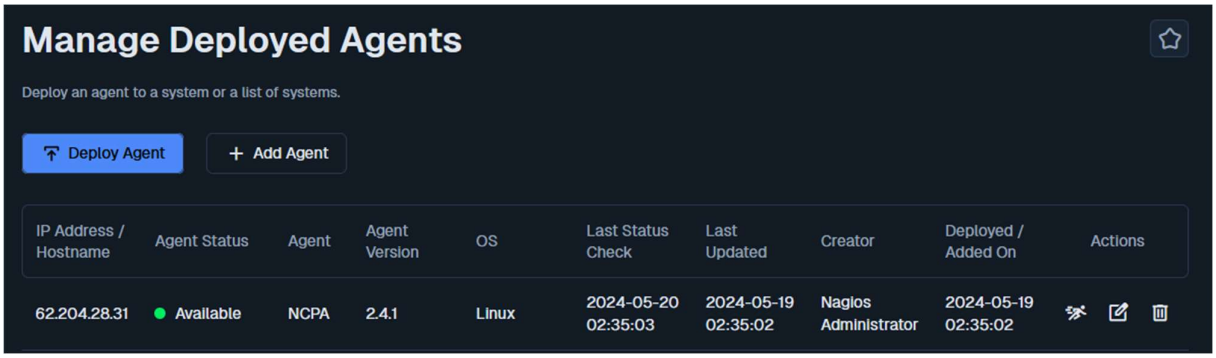
sudo wget https://assets.nagios.com/downloads/ncpa/ncpa-latest.u22.amd64.deb

sudo dpkg -i ./ncpa-latest.u22.amd64.deb

Konfiguraatiomuutoksia pitää tehdä vain yksi: /usr/local/ncpa/etc/ncpa.cfg -tiedostoon muutetaan community_string kohtaan oikea NCPA token, joka löytyy käyttöliittymästä Deployment Settings kohdasta. Tämän jälkeen vielä käynnistetään ncpa_listener palvelu uudelleen:

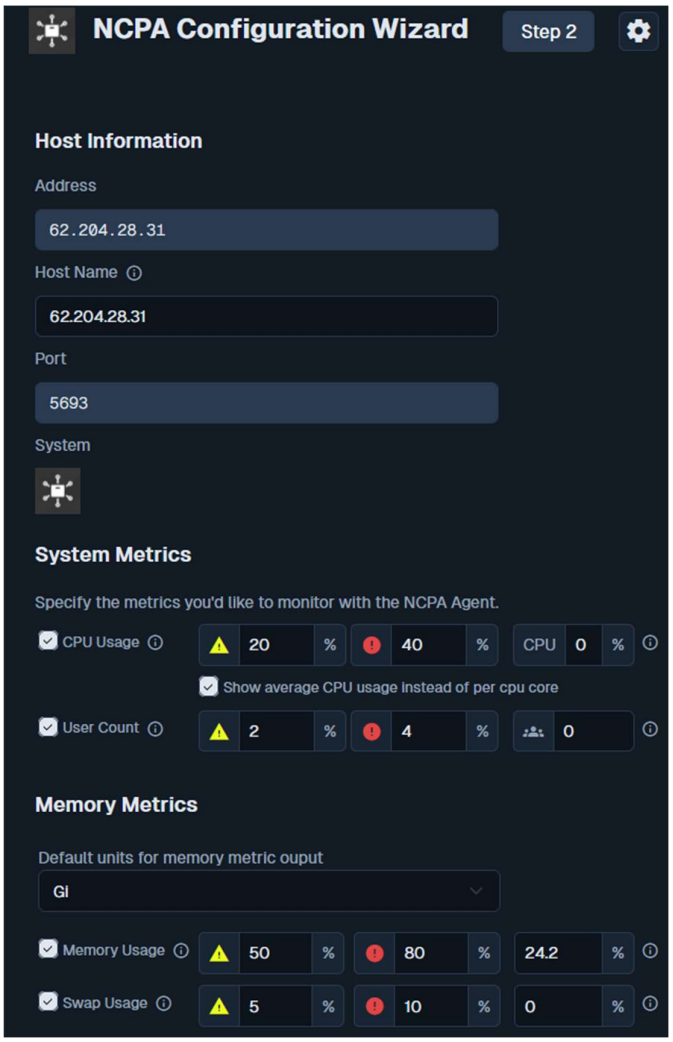
sudo service ncpa_listener restart

Tämän jälkeen agentti pitää lisätä vielä valvontapalvelimelle, käyttöliittymästä löytyy valikko Manage Deployed agents. Add Agent -kohdasta lisätään agentti antamalla siihen palvelimen IP-osoitteen ja NCPA token -merkkijono. Nyt agentin pitäisi näkyä tässä valikossa. (Ks. kuvio 27)



Kuvio 27 Nagios XI asennetut agentit

Nyt voidaan Actions kohdasta painaa Run Wizard -napista, josta voidaan määritellä valvottavia palveluja, sekä näille eri raja-arvoja. Kuviosta 19 nähdään, että esimerkiksi CPU käytön suhteen varoitusraja-arvo on 20 % ja kriittinen taso 40 %. Seuraavilla sivuilla configuration wizardissa voidaan määrittää, kuinka usein tarkastuksia tehdään normaalitilanteissa sekä vikatilanteissa ja kenelle vioista menee ilmoituksia. Myös ryhmä sekä mahdolliset parent hostit voidaan määritellä tässä vaiheessa. (Ks. kuvio 28)



Kuvio 28 Valvottavien palvelujen valinta

8.3 SNMP asennus

Kytkimen lisääminen valvontaan onnistuu käyttöliittymän kautta valmiilla Configuration Wizardilla. Configuration Wizards -valikosta löytyy Network Switch / Router Configuration Wizard. Kytkimelle on avattu eri portti SNMP:lle Nagios valvontapalvelimelta, muuten tähän määritellään samat asetukset kuin Checkmk asennuksessa. Seuraavassa vaiheessa valitaan mitkä rajapinnat halutaan valvontaan. Myös porttien kaistankäyttöä on mahdollista valvoa, sekä määritellä raja-arvot kaistankäytön valvonnalle. Tässä vaiheessa kannattaa myös vaihtaa porttien kuvaus johonkin selkeämpään. (Ks. kuvio 29.) Seuraavat vaiheet ovat samat, kuin aiemmassa agentin asennuksessa, eli määritellään tarkastusvälit, ilmoitusasetukset sekä ryhmäasetukset.

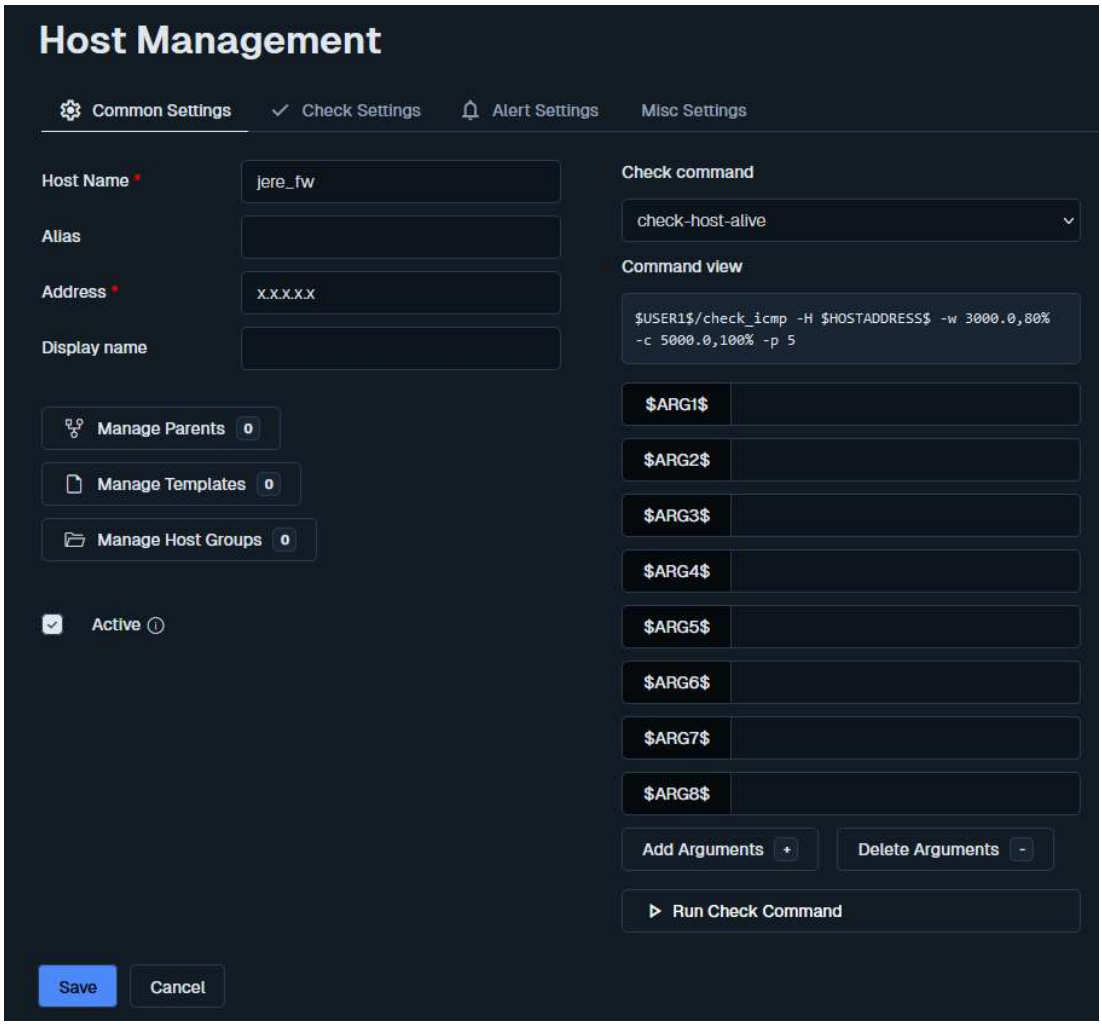
Kuvio 29 SNMP valvottavien palveluiden valinta

8.4 Palomuurin valvonta

Palomuurille ei ole suoraan mahdollista asentaa NCPA agenttia. Palomuuria valvotaan pelkällä icmp valvonnalla. PfSenselle on kuitenkin mahdollista asentaa NRPE (Nagios Remote Plugin Executor) agentti, joka mahdollistaa Nagios pluginien ajamisen palomuurilla.

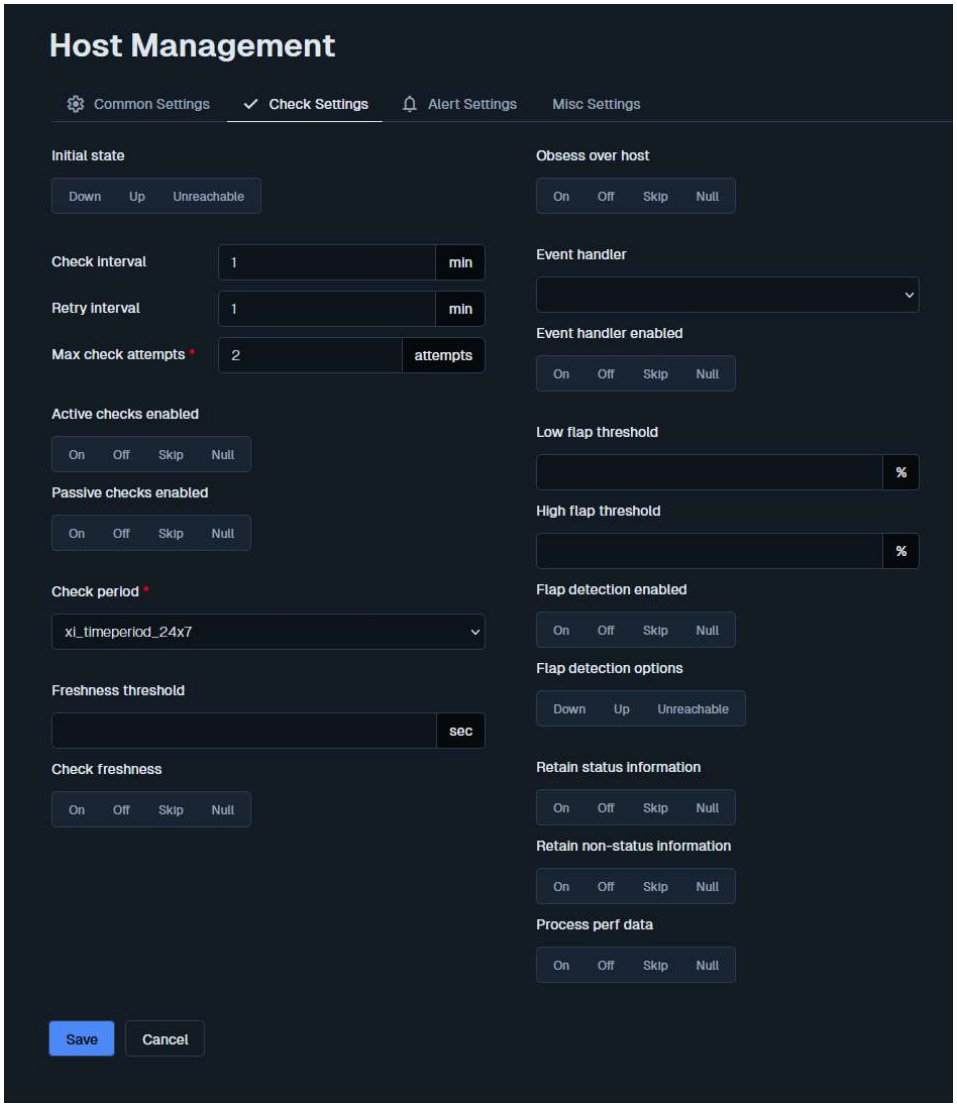
Palomuurin lisäämiseksi ping valvontaa tarvitsee vain lisätä uusi Host valvottavaksi. Tämä onnistuu Core Config Managerin kautta, joka on käytännössä web-käyttöliittymä Nagios Core -valvontamoottorille. Kohdasta Hosts lisätään uusi valvottava kohde. Tähän määritellään hostille nimi ja IP-osoite. Tarkistekomennoksi valitaan check-host-alive, joka on käytännössä check_icmp tarkiste,

johon on määritelty valmiiksi argumentit. (Ks. kuvio 30) Tässä voisi myös käyttää check-ping tarkistetta, joka on käytännössä sama kuin check-icmp eli lähettää kohteelle echo-request ICMP paketteja, mutta käytää ping sovellusta.



Kuvio 30 Nagios XI hostin lisääminen

Muut pakolliset kohdat löytyvät check settings -välilehdeltä, johon täytyy määritellä maksimi tarkistusmäärä, jonka jälkeen host tai palvelu menee hard tilaan, joka käytännössä tarkoittaa ilmoitusten lähettämistä vikatilanteesta ja mahdollisen event handlerin suorittamista. Myös palautimen vikatilanteesta on hard tila, jolloin tästäkin lähtee ilmoitukset. Toinen pakollinen kohta on check period, joka määrittää millä ajanjaksolla tarkistuksia tehdään ja milloin ei. Ajanjaksoille on mahdollista myös itse tehdä mallipohjia. Tarkistevälillä tarkoitetaan, kuinka usein Nagios tekee tarkistuksen ja uudelleenyritysväli, kuinka usein tarkiste tehdään vikatilanteessa. (Ks. kuvio 31)



Kuvio 31 Nagios XI tarkisteasetukset

Palomuurille lisätään palveluna kytkimelle ping valvonta NRPE:n avulla. Palomuurille on asennettu NRPE lisäosa, johon on määritelty check_sw nimellä seuraava check_ping tarkiste:

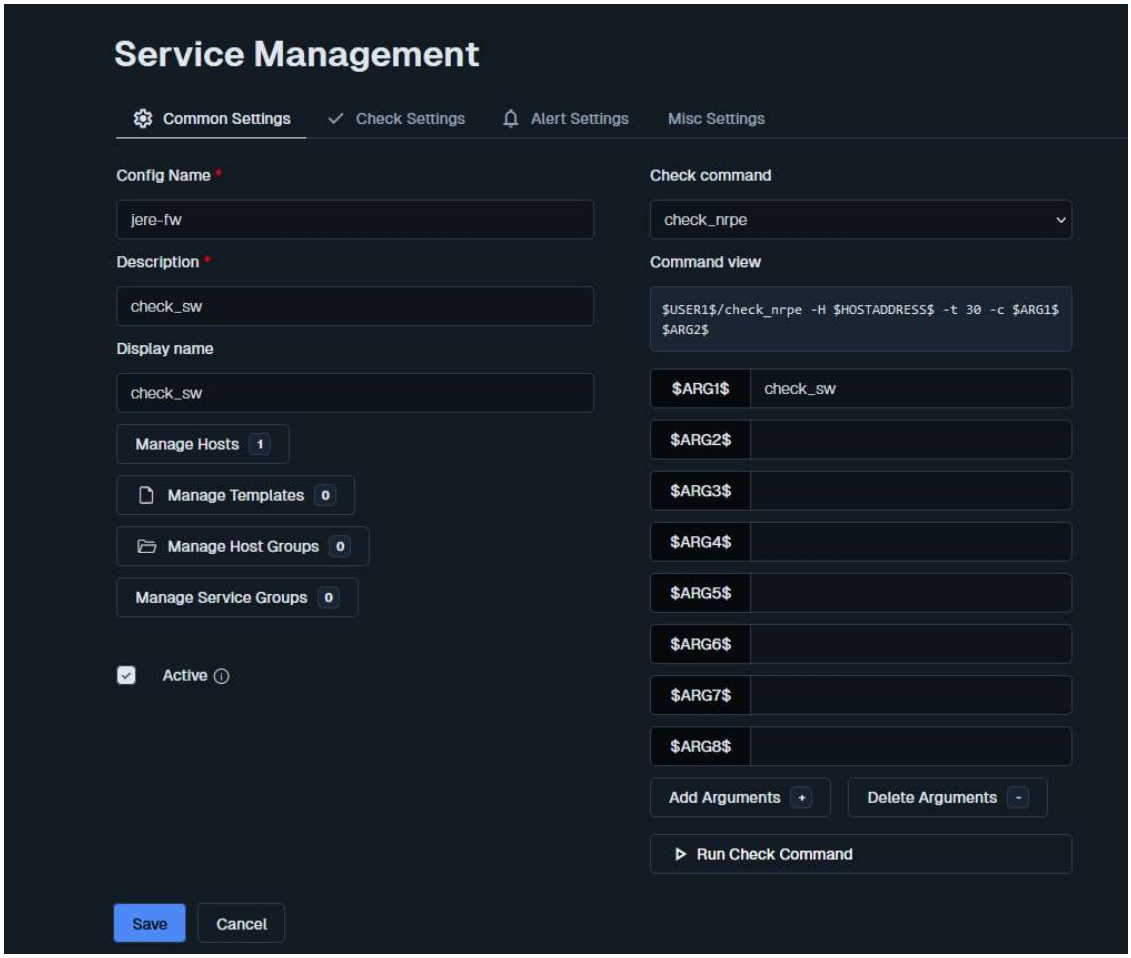
check_ping -H 10.52.170.20 -w 100,60% -c 500,100%

Komennon -H parametri on host, eli kytkimen IP osoite, -w varoitusraja-arvo ja -c kriittisen tilan raja-arvo. Ensimmäinen numero tarkoittaa RTA:ta (Round-trip Average), eli keskiarvoa millisekunneissa sille, kuinka kauan echo-requestin lähettämisen jälkeen kesti saada echo-reply. Toinen luku tarkoittaa packet lossia prosentteina.

Seuraavaksi lisätään Nagios XI core config managerin kautta uusi service. Config nimeksi laitetaan sama kuin hostin nimi ja description kentään esimerkiksi check_sw. Kohdasta manage hosts pitää myös valita millä hostilla valvottava palvelu on, eli valitaan aiemmin luotu jere-fw hostiksi. Tarkistekomennoksi valitaan check_nrpe. Parametriksi tarvitsee lisätä vain check_sw, kokonaisuudessaan tarkistekomento näyttää siis tältä:

/usr/local/nagios/libexec/check_nrpe -H <palomuurin_ip> -t 30 -c check_sw

Valvontapalvelimelta ajetaan check_nrpe plugin, joka kutsuu palomuurilta NRPE:lle määriteltyä check_sw komentoa. (Ks. kuvio 32)



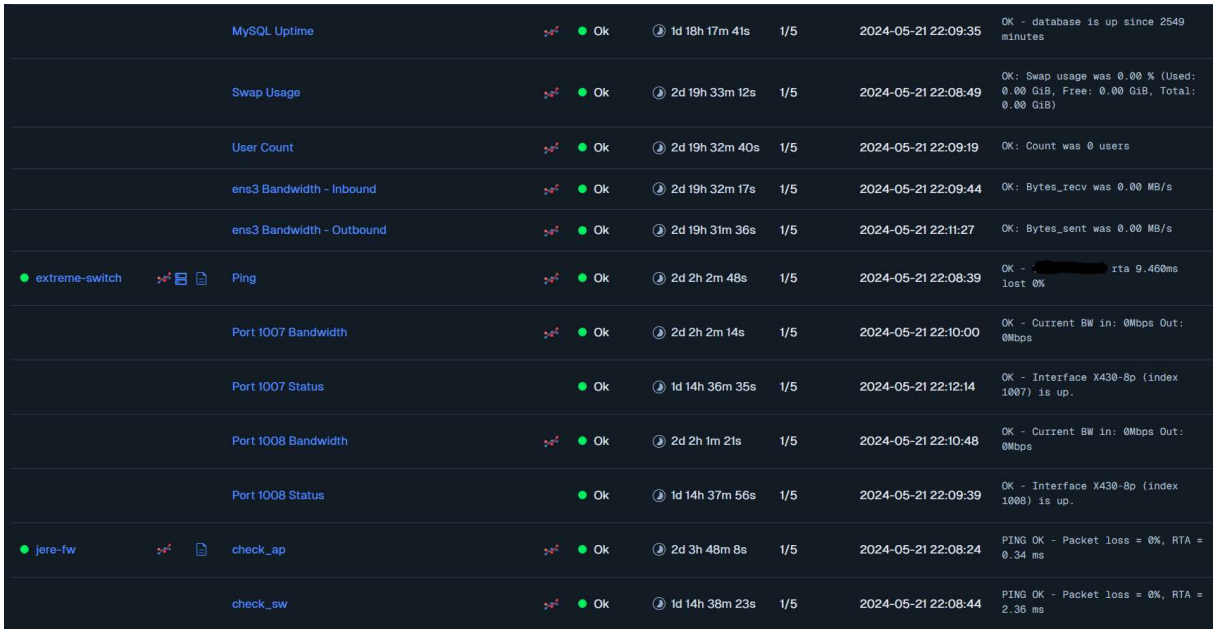
Kuvio 32 Nagios XI check_nrpe service

8.5 Käyttö

Nyt testiympäristö on lisätty Nagios XI:lle kokonaisuudessaan. Etusivulla näkyy nyt kaikki lisätyt hostit ja niiden palvelut sekä tiivistettynä niiden tila (Ks. kuvio 33)

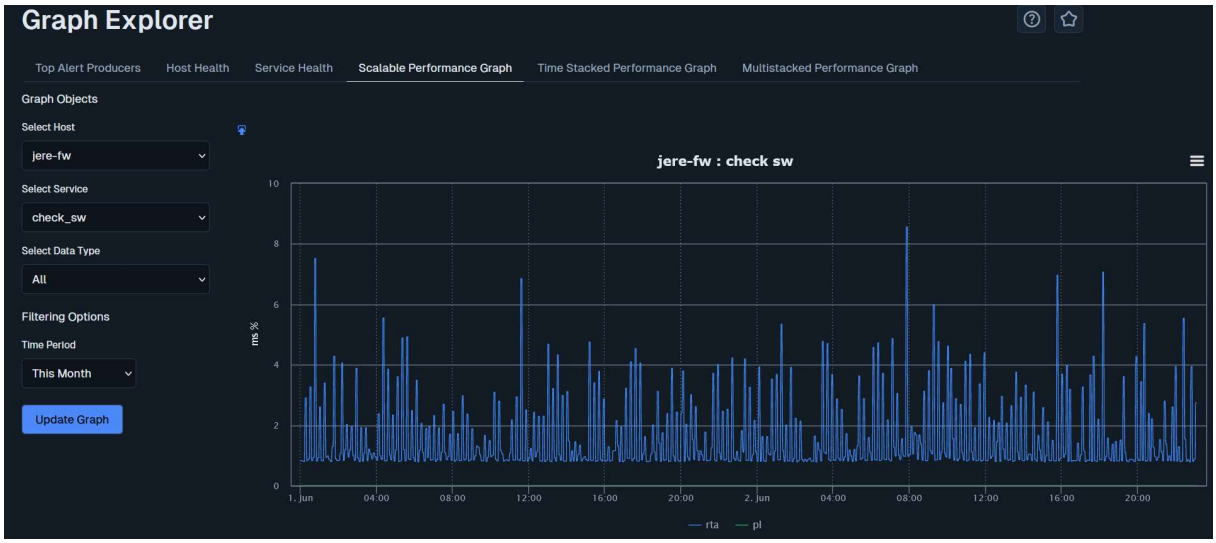
Kuvio 33 Nagios XI dashboard

Kaikki palvelut nähdään service status -välilehdeltä ja hostit host status -välilehdeltä. Kuviosta 34 nähdään palveluiden tilanne.



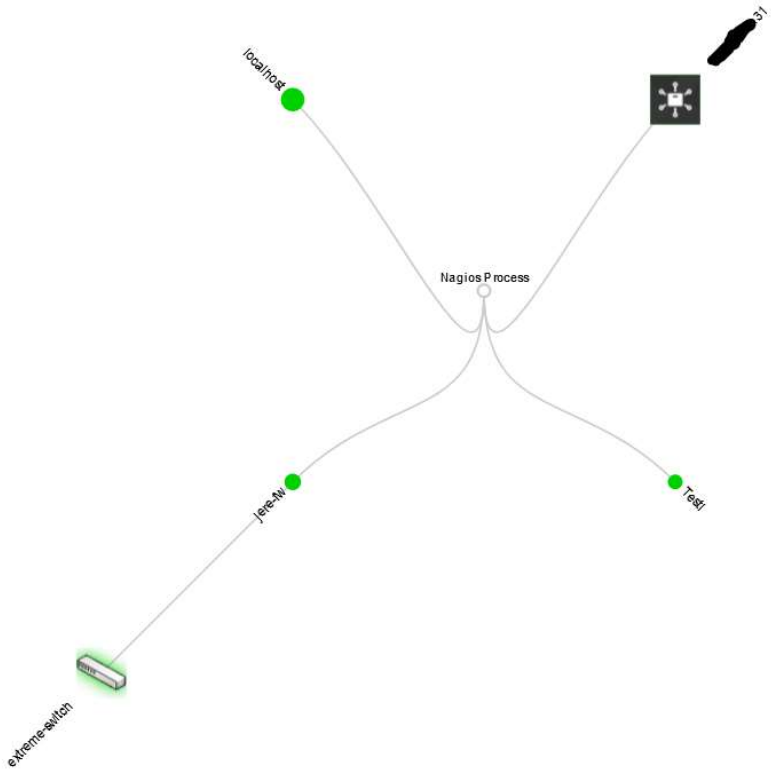
Kuvio 34 Nagios XI palvelut välilehti

Graph Explorer työkalulla pystytään tarkastelemaan palvelu kerrallaan eri palveluiden suorituskykyä. Kuviosta 35 nähdään graafi check_sw palvelulle palomuurilta. Kyseessä on check-ping -tarkiste, eli graafista nähdään vastauksen saamiseen kulunut aika echo request -paketille.



Kuvio 35 Nagios XI palvelun graafi

Verkkotopologian saa myös näkyviin Nagioksella, mutta tätä ei ole mahdollista tehdä automaattisesti, vaan hosteille pitää luoda manuaalisesti vanhemmuussuhteet, samalla tavalla kuin Checkmk:lla. Kuviosta 36 nähdään verkkotopologia Nagioksessa valvontapalvelimen näkökulmasta.



Kuvio 36 Nagios XI verkkotopologia

9 Vertailu

Vertailussa painotetaan kappaleessa 6 esitettyjä kohtia. Taulukoon 1 on merkitty arvosanat asteikolla 1–5 jokaiselle vertailtavalle kohdalle.

Hinta

Tuotteilla on hieman erilaiset hinnoittelut, Checkmk hinta perustuu valvottujen palveluiden määrään ja laskutus on kuukausiperusteinen. Nagios XI lisenssi on taas kertamaksullinen ja hinta riippuu hostien määrästä. Nagios XI enterprise lisenssi 500 hostilla maksaa noin 9200 euroa, kun taas Checkmk vastaavilla määriä valvottuja palveluja maksaisi vuodessa noin 2100 tai 3300 euroa. Eli pelkkä tuotelisenssi on Nagioksella hieman edullisempi.

Tuki

Checkmk maksullisiin versioihin kuuluu palveluntarjoajan tuki (Checkmk Pricing, n.d). Nagios XI:llä tämä on maksullinen lisäpalvelu, joka sisältää myös pääsyn ohjelmistopäivityksiin. Kun ostat lisenssin ensimmäisen kerran, kuuluu tuki ja ylläpitopalvelut tähän vuodeksi, jonka jälkeen ne pitää uusia vuosittain. 500 hostin enterprise lisenssille tukipalvelu maksaa noin 7000 euroa vuosittain. Tämä muuttaa hintakysymystä merkittävästi, käytännössä Nagioksen päivittäminen vuosittain maksaa vähintään 7000 euroa, vaikka tukipalveluille ei olisi käyttöä. (Support Plans, n.d.)

Tueksi voidaan laskea myös yhteisökeskustelut ja sovelluksen kehittäjien omat artikkelit tai blogikirjoitukset. Nagios on vanhempi sovellus ja sillä on enemmän käyttäjiä, joten ongelmiin löytää melko suurella todennäköisyydellä ratkaisun hakemalla tietoa ongelmasta. Checkmk:lla on taas laajemmat ja selkeämmät dokumentaatiot sekä paljon artikkeleita ja blogikirjoituksia siitä, miten sovellusta on mahdollista käyttää tai verkonvalvonnasta yleisellä tasolla.

Käyttökokemus

Molempia sovelluksia oli melko yksinkertaista käyttää asennuksesta lähtien. Eroavaisuuksia ympäristön pystytyksessä oli siinä, että Checkmk:lla hostien lisääminen tapahtuu aina samasta paikasta, kun taas Nagioksella joutuu valitsemaan aina eri asennuswizardin. Checkmk:lla joutui käyttämään komentoriviä useammin, MySQL ja FreeBSD valvonnan yhteydessä, mutta näihin löytyi kuitenkin

selkeät ohjeet dokumentaatioista. Nagioksella joutui tutkimaan konfiguraatiotiedostoja ongelmien yhteydessä, mutta tämänkin olisi voinut tehdä graafisen käyttöliittymän kautta.

Käyttöliittymä on Checkmk:lla miellyttävämpi ja selkeämpi. Asiat on selkeästi jaoteltu eri otsikoiden alle. Nagioksella esimerkiksi Core Config Managerin on laitettu edistyksellisen käytön välilehdelle, vaikka mielestäni sitä tarvitaan jo ihan peruskäytössä. Visuaalisesti Checkmk on selkeämpi. Nagioksessa graafeja valvotuista palveluista löytyy useasta eri paikasta, joka ei ole selkeyden kannalta suotavaa. Hostin kaikkia palveluita ei myöskään saa samanaikaisesti näkymään tällä tavalla.

Yhteensopivuus

Yhteensopivuudesta molemmista sovelluksista löytyy hyviä puolia. Checkmk:lla on vain yksi agentti, joka voidaan asentaa oikeastaan jokaiselle yleisimmälle käyttöjärjestelmälle. Nagioksella agenttisovelluksia on useampia, joista tässä työssä käytettiin kahta. NCPA on oletusagentti Nagios XI:llä, muita ei ole edes mahdollista ottaa käyttöön automatiikalla. Toinen agentti oli NRPE, joka vaatii hieman manuaalista konfigurointia.

Molemmilta sovelluksilta löytyy mittavasti virallisia liitännäisiä sekä yhteisön kehittämiä liitännäisiä. Käytännössä molempia sovelluksia on mahdollista laajentaa niin, että ne toimivat millä tahansa laitteella.

Valvontaominaisuudet

Valvontaominaisuuksiltaan sovellukset ovat hyvin samanlaiset. Suurimmilta osin valvonta perustuu siihen, että valvontapalvelin lähettää tietyin väliajoin kyselyjä kohteelle itse kohteen tai jonkin palvelun tilasta. Ero toteutuksessa sovellusten välillä näyttäisi olevan se, että Checkmk tekee kyselyn agentille, joka palauttaa tiedot jokaisesta passiivisesta palvelusta samalla kertaa. Passiivisella tarkoitetaan sitä, että valvontapalvelin ei saa suoraan tietoja näistä, vaan ulkoiselta lähteeltä, tässä tapauksessa agenttisovellus kerää tiedot. Nagioksella ainakin oletuksena valvontapalvelin kysyy agentilta jokaisesta palvelusta erikseen ja palauttaa tiedot yksi kerrallaan.

Molemmilla sovelluksilla pystyy valvomaan myös ilman agenttia eri tietoliikenneprotokollia hyödyntäen, kuten HTTP/S, ICMP, SSL/TLS tai valvomaan tiettyä TCP/UDP porttia.

Järjestelmään pääsy

Molempiin sovellukseen on mahdollista luoda käyttäjiä ja käyttäjäryhmiä sekä rajoittaa oikeuksia joko käyttäjä tai ryhmäkohtaisesti. Molemmilla sovelluksilla on mahdollisuus LDAP/AD integraatioon, eli käyttäjä voi esimerkiksi kirjautua järjestelmään yrityksen Windows toimialueen tunnuksilla. Checkmk:lla löytyy tuki myös SAML (Security Assertion Markup Language) kirjautumiselle, joka käytännössä tarkoittaa, että yhdellä autentikoinnilla on mahdollista saada pääsyt usealle sovellukselle yhtä aikaa. Eli molemmat sovellukset kykenevät multi-tenancyyn, samalla valvontasovellusinstanssilla on mahdollisuus tarjota useille käyttäjille palveluja. Checkmk:lla on mahdollisuus jakaa esimerkiksi asiakkaat täysin omille kokonaisuuksilleen, joissa data on aidosti erillään muista asiakkaista.

Ominaisuudet

Joitakin ominaisuuksia on jo vertailun yhteydessä käsitelty. Muita ominaisuuksia, joita molemmista löytyy, on esimeriksi datan visualisointi ja raportointimahdollisuudet. Molemmista sovelluksista saadaan irti yksittäisistä palveluista ja hosteista saatavuusdataa. Esimerkkinä voidaan määritellä, että jonkin palvelun täytyy olla OK tilassa 95 % ajasta per kuukausi tai hostilla täytyy olla 99 % käytettävyysaika. Molemmilla sovelluksilla saadaan jokaisesta valvotusta palvelusta visuaalista dataa graafin muodossa. Myös yleisiä raportteja yksittäisistä valvottavista kohteista saa molemmilla sovelluksilla, joissa näkyy saatavuuden ja palveluiden graafien lisäksi kaikki tapahtumat tietyltä ajanjaksolta. Checkmk:lla nämä ovat selkeämpiä ja helpommin luettavissa sekä kustomoitavissa.

Molemmilla sovelluksilla on mahdollista esittää topologioita. Nämä voidaan joko määritellä manuaalisesti tai automaattisesti. Automaattista määritystä ei voitu tämän työn yhteydessä testata, koska ympäristö ei sijainnut kokonaan samassa verkossa. Topologian avulla ylläpitäjät näkevät vian yhteydessä helposti, missä kohtaa verkkoa vika on ja mitkä ovat mahdolliset kerrannaisvaikutukset.

Molemmista sovelluksista löytyy myös automaattinen hälytystenkäsittelijä ominaisuus, jolla voidaan määritellä valvontapalvelinta ajamaan skripti tapahtumien yhteydessä. Esimerkiksi jos jokin palvelu lakkaa vastaamasta, voidaan se käynnistää uudelleen automaattisesti.

Merkittävät lisäominaisuudet

Muita merkittäviä lisäominaisuuksia, joita löytyy vain toisesta sovelluksesta ei ole kummassakaan merkittävästi enempää kuin toisessa. Checkmk:lla tälläiseksi voi laskea SW/HW inventory -ominaisuuden, jonka avulla saadaan selville käytännössä kaikki tieto valvotusta järjestelmästä.

Nagios XI:llä on mahdollisuus kirjautua valvotuille hosteille suoraan graafisen käyttöliittymän kautta SSH:n, RDP:n, Telnetin tai VNC:n avulla.

Taulukko 1. Verkonvalvontaohjelmien vertailu

	Checkmk	Nagios XI
Hinta	****	**
Tuki	****	***
Käyttökokemus	*****	***
Yhteensopivuus	****	****
Valvontaominaisuudet	****	***
Järjestelmään pääsy	****	***
Ominaisuudet	****	***
Merkittävät lisäominaisuudet	***	***

10 Pohdinta

Vertailun perusteella voidaan tulla lopputulokseen, että näistä kahdesta vaihtoehdosta Checkmk on parempi verkonvalvontasovellus. Suurimmat erot Checkmk:n eduksi löytyivät hinnasta ja käyttökokemuksesta. Checkmk on käyttöliittymän ja muokattavuuden kannalta selkeämpi ja yksinkertaisempi käyttää.

Kun verrataan Checkmk:ta yrityksen nykyiseen valvontajärjestelmään, on se kaikilla osa-alueilla reilusti parempi, pois lukien hinta, koska nykyinen järjestelmä ei kustanna käytännössä mitään. Checkmk:n mukana tulisi siis lisenssimaksut, jos halutaan käyttää kaupallista versiota. Toinen huomioitava asia on järjestelmän käyttöönotto ja opettelu. En usko, että käyttöönoton kanssa tulisi ylitsepääsemättömiä haasteita, käyttöönottoon kuitenkin kuluu jonkin verran aikaa, koska ensiksi täytyy esimerkiksi varmistaa, että kaikki vanhat toiminnallisuudet on mahdollista ottaa käyttöön jollain tapaa. Järjestelmiä pitäisi myös luultavasti ajaa rinnakkain, kunnes voidaan olla täysin varmoja, että migraatio voidaan lopullisesti tehdä. Järjestelmän käytön opettelu ei luultavasti tuota ongelmia.

Nagios XI:n etu olisi siinä, että nykyinen verkonvalvontajärjestelmä toimii Nagios Core -valvontamoottorilla. Osaamista löytyisi siis jo valmiiksi ja siirtyminen olisi helpompaa. Tässä vaihtoehdossa hinta olisi luultavasti ratkaiseva tekijä. Lisenssi- ja päivityskustannukset ovat huomattavasti korkeammat Nagios XI:llä.

Työn toteutuksen olisi voinut tehdä eri tavalla. Nykyisessä toteutuksessa puutteita oli testiympäristön koossa, sekä siinä, että ympäristö ei ollut kokonaan samassa verkossa. Jos valvottuja hosteja olisi ollut enemmän, olisi voinut luoda riippuvuuksia eri laitteiden välille ja tehdä parempia käytännön testejä aidosta vikatilanteesta. Myös muita automatisointi ominaisuuksia, kuten hostien löytäminen automaattisesti verkosta olisi ollut mielenkiintoista testata. Tämä olisi kuitenkin vaatinut huomattavasti enemmän työtä. Jos koko ympäristö olisi pystytetty omaan sisäverkkoon, esimerkiksi TNNetin virtuaalipalvelinalustaa ei olisi voinut hyödyntää.

Lähteet

Checkmk Pricing. N.d. Artikkeli Checkmk:n sivustoilla. Viitattu 25.4.2.2024. https://checkmk.com/pricing.

Fiore, G. 2022. Why SNMP monitoring for Linux is not recommended. Blogikirjoitus Checkmk:n verkkosivuilla. Viitattu 24.4.2024. https://checkmk.com/blog/why-snmp-monitoring-linux-not-recommended.

ITIL Foundation. ITIL 4 Edition. 2019. Lontoo: The Stationery Office. Viitattu 31.1.2024. https://janet.finna.fi, Ebook Central.

LaFlamme, R. N.d. Agent vs Agentless Monitoring: Which is Best? Blogikirjoitus Auvikin verkkosivustoilla. Viitattu 24.4.2024. https://www.auvik.com/franklyit/blog/agent-vs-agentless-monitoring/.

Monitoring agents. 2023. Artikkeli Checkmk:n sivustoilla. Viitattu 24.4.2024. https://docs.checkmk.com/latest/en/wato_monitoringagents.html.

Monitoring FreeBSD. 2022. Artikkeli Checkmk:n dokumentaatioissa. Viitattu 27.5.2024. https://docs.checkmk.com/latest/en/agent_freebsd.html.

Nagios Cross-Platform Agent. N.d. Nagios verkkosivut. Viitattu 19.5.2024. https://www.nagios.org/ncpa/.

Nagios XI. N.d. Artikkeli Nagioksen sivustoilla. Viitattu 19.5.2024.https://www.nagios.com/products/nagios-xi/.

Nagios XI // Licensing Policy. N.d. Pdf esite Nagioksen sivuille. Viitattu 19.5.2024. https://assets.nagios.com/handouts/nagiosxi/Nagios-XI-Licensing-Policy.pdf.

Notifications. N.d. Artikkeli Checkmk dokumentaatioissa. Viitattu 30.5.2024. https://docs.checkmk.com/latest/en/notifications.html.

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. PDF artikkeli kehittämistutkimuksesta Helsingin Yliopiston avoimessa julkaisuarkistossa. Viitattu 2.6.2024. https://helda.helsinki.fi/items/56af5e77-73d5-4beb-94d2-9bdd9b2ed232.

RFC 793:1981. Transmission Control Protocol. Viitattu 1.6.2024. https://www.ietf.org/rfc/rfc793.txt

RFC 1157:1990. Simple Network Management Protocol (SNMP). Viitattu 24.4.2024. https://datatracker.ietf.org/doc/rfc1157/.

Setting up Checkmk. 2023. Artikkeli Checkmk:n sivustoilla. Viitattu 25.4.2024. https://docs.checkmk.com/latest/en/intro_setup.html.

SNMP Monitoring Overview. N.d. Artikkeli Datadogin sivustoilla. Viitattu 3.4.2024. https://www.datadoghq.com/knowledge-center/network-monitoring/snmp-monitoring/.

Support Plans. N.d. Artikkeli Nagioksen sivustoilla. Viitattu 27.5.2024. https://www.nagios.com/support-plans/.

Tietoja meistä. N.d. Artikkeli TNNet Oy sivustoilla. Viitattu 26.5.2024. https://tnnet.fi/tietoja-meista/.

The Managed Services Edition. 2024. Artikkeli Checkmk:n sivustoilla. Viitattu 2.5.2024. https://docs.checkmk.com/latest/en/managed.html.

The Open Monitoring Distribution. N.d. Artikkeli Checkmk:n sivustoilla. Viitattu 28.4.2024. https://checkmk.com/guides/open-monitoring-distribution.

What is network monitoring? N.d. Artikkeli CheckMK:n sivustoilla. Viitattu 31.1.2024. https://checkmk.com/guides/network-monitoring.

What is server monitoring? N.d. Artikkeli CheckMK:n sivuistoilla. Viitattu 3.4.2024. https://checkmk.com/guides/what-is-server-monitoring

What is Transmission Control Protocol TCP/IP? N.d. Artikkeli Fortinetin verkkosivuilla. Viitattu 1.6.2024. https://www.fortinet.com/resources/cyberglossary/tcp-ip.

Xiang, F. 2021. What Is ICMP? Artikkeli Huawein verkkosivuilla. Julkaistu 24.11.2021. Viitattu 12.12.2024. https://info.support.huawei.com/info-finder/encyclopedia/en/ICMP.html.

Liitteet

Liite 1. PfSense xinetd konfiguraatiotiedosto

```
service check-mk-agent
{
   type         = UNLISTED
   port         = 6556
   socket_type    = stream
   protocol      = tcp
   wait         = no
   user         = root

   # If you use fully redundant monitoring and poll the client
   # from more then one monitoring servers in parallel you might
   # want to use the agent cache wrapper:
   #server        = /usr/bin/check_mk_caching_agent
   server        = /opt/bin/check_mk_agent.freebsd

   # To avoid intentional or unintentional overload due to too many parallel
   # queries from one source we set this parameter. It limits the number of
   # concurrent connections per source address.
   per_source     = 3

   # listen on IPv4 AND IPv6 when available on this host
   #flags         = IPv6

   # configure the IP address(es) of your Nagios server here:
   only_from      = <palvelimenip>

   # Don't be too verbose. Don't log every check. This might be
   # commented out for debugging. If this option is commented out
   # the default options will be used for this service.
   log_on_success =

   disable       = no
}
```