LAB University of Applied Sciences

Verkonvalvonnan ja häiriönhallinnan tehostaminen

LAB-ammattikorkeakoulu

Insinööri (AMK), Tieto- ja viestintätekniikka
2024
Riku Muhonen

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Muhonen Riku	Opinnäytetyö, AMK	2024
	Sivumäärä 25(27)	

Työn nimi

Verkonvalvonnan ja häiriönhallinnan tehostaminen

Tutkinto ja koulutusala

Tieto- ja viestintätekniikan Insinööri (AMK)

Toimeksiantajaorganisaatio (jos opinnäytetyöllä on toimeksiantaja)

Telia Cygate

Tiivistelmä

Opinnäytetyön tavoitteena on löytää kehityskohteita Telia Cygaten häiriönhallintaan sekä verkonvalvontaan.

Työssä suoritettiin vertailu kahden verkonvalvontaohjelmiston, OpenNMS Meridianin ja Zabbixin välillä. Vertailussa tarkasteltiin ohjelmistojen keskeisiä ominaisuuksia, käytettävyyttä, skaalautuvuutta ja kustannustehokkuutta.

Työ osoitti, että tehokas häiriönhallinta edellyttää luotettavia teknologioita. OpenNMS Meridianin vahvuutena on sen joustavuus suurten ja monimutkaisten verkkojen valvonnassa. Zabbix tarjoaa käyttäjäystävällisen käyttöliittymän ja laajan yhteisön tuen. Molemmat ohjelmistot mahdollistavat kattavan valvonnan ja häiriönhallinnan automaation, mutta niiden valinta riippuu organisaation tarpeista.

Asiasanat

Zabbix, OpenNMS Meridian,Verkonvalvonta

Abstract

Author(s)	Type of Publication	Published
Muhonen Riku	Thesis, UAS	2024
	Number of Pages	
	25(27)	

Title of Publication

Enhancing Network Monitoring and Incident Management

Degree, Field of Study

Bachelor of engineering in Information and Communication Technologies (UAS)

Organisation of the client (if the thesis work is commissioned by another party)

Telia Cygate

Abstract

The aim of this thesis is to identify areas for improvement in Telia Cygate's incident management and network monitoring.

The study involved a comparison of two network monitoring software solutions, OpenNMS Meridian and Zabbix, focusing on their key features, usability, scalability, and cost-effectiveness.

The results showed that effective incident management requires reliable technologies. OpenNMS Meridian excels in its flexibility for monitoring large and complex networks, while Zabbix provides a user-friendly interface and strong community support. Both software solutions enable comprehensive monitoring and automation of incident management, but the choice between them depends on the organization's specific needs.

Keywords

Zabbix,OpenNMS Meridian, Network monitoring

Sisällys

Lyhenteet

ACL	Access Control List, on sääntöluettelo, joka hallitsee pääsyä tietokoneympäristöön.
API	Application Programming Interface, on rajapinta, minkä avulla eri järjestelmät ja ohjelmistot voivat viestiä ja vaihtaa tietoja keskenään.
IP	Internet Protocol, on protokolla, jolla laitteet kommunikoivat keskenään.
ITIL	Information Technology Infrastructure Library on viitekehys, jota käytetään häriönhallinnassa.
MIB	Management Information Base, SNMP-valvonnassa käytettävä tietokanta, joka sisältää tietoja hallittavista verkkoresursseista.
NMS	Network Management System, on sovellus, jota käytetään verkkojen hallinnassa.
OID	Object Identifier ,on tunniste, jolla kuvataan hallittavia objecteja.
OSI	Open Systems Interconnection, on internetissä käytettävä toimintamalli.
SNMP	Simple Network Management Protocol, on verkonvalvonta protokolla, jolla valvottavat laitteet kommunikoivat keskenään

1 JOHDANTO

Nykypäivänä, kun liiketoiminta on yhä riippuvaisempaa digitaalisista järjestelmistä, verkonvalvonta ja häiriönhallinta ovat tärkeä osa yritysten toimintavarmuutta ja tehokkuutta. Tietoverkkojen monimutkaistuessa ja niiden merkityksen kasvaessa on olennaista, että käytössä olevat työkalut mahdollistavat nopean reagoinnin ja ongelmien ennakoivan ratkaisun.

Tämän opinnäytetyön tavoitteena on selvittää, miten verkonvalvontaa ja häiriönhallintaa voidaan tehostaa vertailemalla kahta erilaista verkonvalvontaohjelmistoa sekä antaa kehitysideoita, miten Telia Cygate voisi parantaa heidän häiriönhallinta prosessia. Vertailussa keskitytään ohjelmistojen ominaisuuksiin, suorituskykyyn ja käytettävyyteen. Lopputuloksena pyritään tarjoamaan kattava analyysi, jonka avulla yritys voi valita tarpeisiinsa parhaiten sopivan ratkaisun ja kehittää häiriönhallintaansa.

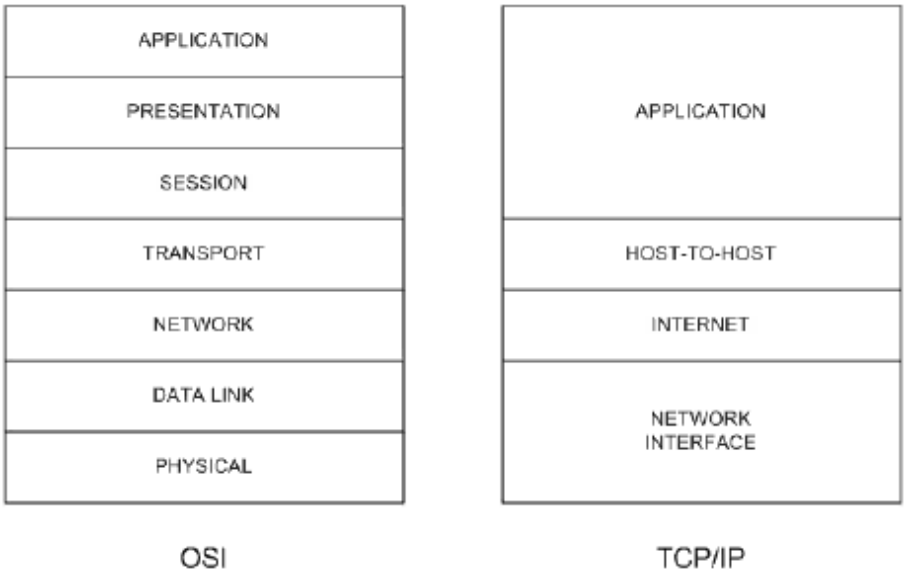
Tutkimus tarjoaa tietoa yrityksille, jotka etsivät tehokkaita työkaluja verkkonsa hallintaan ja parantamiseen. Lisäksi työ auttaa tunnistamaan kehityskohteita ja antaa suosituksia, jotka voivat edistää häiriöttömyyttä ja tehostaa verkonvalvontaa.

2 VERKONVALVONTA

2.1 Verkonvalvonta yleisesti

Verkonvalvonta on IT-prosessi, jota käytetään tietokoneverkkojen ja niiden komponenttien, kuten reitittimien, kytkimien, palvelimien ja palomuurien valvontaan. Sen avulla verkon ylläpitäjät voivat arvioida verkon suorituskykyä ja parantaa tehokkuutta reaaliajassa. Tehokas verkonvalvonta auttaa havaitsemaan ja ratkaisemaan ongelmat varhaisessa vaiheessa sekä ehkäisee katkoksia.(IBM 2024.)

Prosessiin kuuluu verkkoon kytkettyjen laitteiden suorituskyvyn ja mittareiden seuranta. Valvottavat laitteet, kuten reitittimet ja kytkimet, ovat tärkeässä roolissa verkon infrastruktuurissa ja niiden toiminta vaikuttaa suoraan koko verkon suorituskykyyn. Verkonvalvontaan käytetyt työkalut keräävät tietoja verkon suorituskyvystä, nopeuttavat vianmääritystä ja hallitsevat monimutkaisia verkkoympäristöjä useiden eri valmistajien laitteilla. Lisäksi valvonta tarjoaa tietoa verkon kunnosta ja yksityiskohtaista tietoa jokaisesta laitteesta. Verkkovalvonnan keskeinen näkökohta on verkkojen toiminnan ymmärtäminen. Verkot mahdollistavat tietojen vaihdon järjestelmien välillä käyttämällä OSI-mallin protokollia (kuvassa1). (IBM. 2024.)



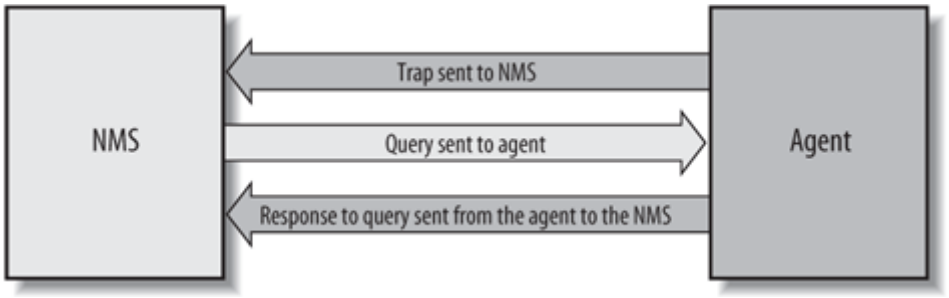
Kuva 1. OSI TCP/IP malli (Cisco 2005.)

Verkonvalvontaa toteutetaan usein verkon operaatiokeskuksesta, jossa tiimit valvovat verkkolaitteiden tilaa ja kuntoa. Operaatiokeskuksen tehtävä on varmistaa, että mahdolliset häiriöt eivät vaikuta loppukäyttäjiin. Se tarjoaa ennakoivan suojan verkkoon liittyviä ongelmia vastaan. (IBM 2024.)

2.2 Simple Network Management Protocol

SNMP on verkkoprotokolla, jota käytetään TCP/IP-verkoissa erilaisten verkkolaitteiden hallintaan ja valvontaan. SNMP esiteltiin ensimmäisen kerran vuonna 1988 ja se luotiin asettamaan standardi kaikille verkkolaitteille laitevalmistajasta riippumatta. Tämä tarjoaa yhtenäisen tavan kerätä tietoja. Ajan myötä se on saavuttanut laajan käyttöönoton ja siitä on tullut keskeinen työkalu verkonvalvonnassa. (Kentik2024.)

SNMP antaa työkalut tarkkailla laitteiden tilaa, säätää niiden asetuksia ja kerätä tietoa verkon suorituskyvystä. SNMP:n avulla voidaan esimerkiksi sammuttaa reitittimen portti, tarkistaa Ethernet-liitännän tila ja nopeus. Sillä voidaan myös valvoa kytkimen lämpötilaa ja antaa hälytyksiä, jos lämpötila nousee liian korkeaksi. Näin ollen se auttaa varmistamaan verkkoinfrastruktuurin toimivuuden ja estämään ongelmia ennen niiden eskaloitumista. (O’Reilly 2001.)



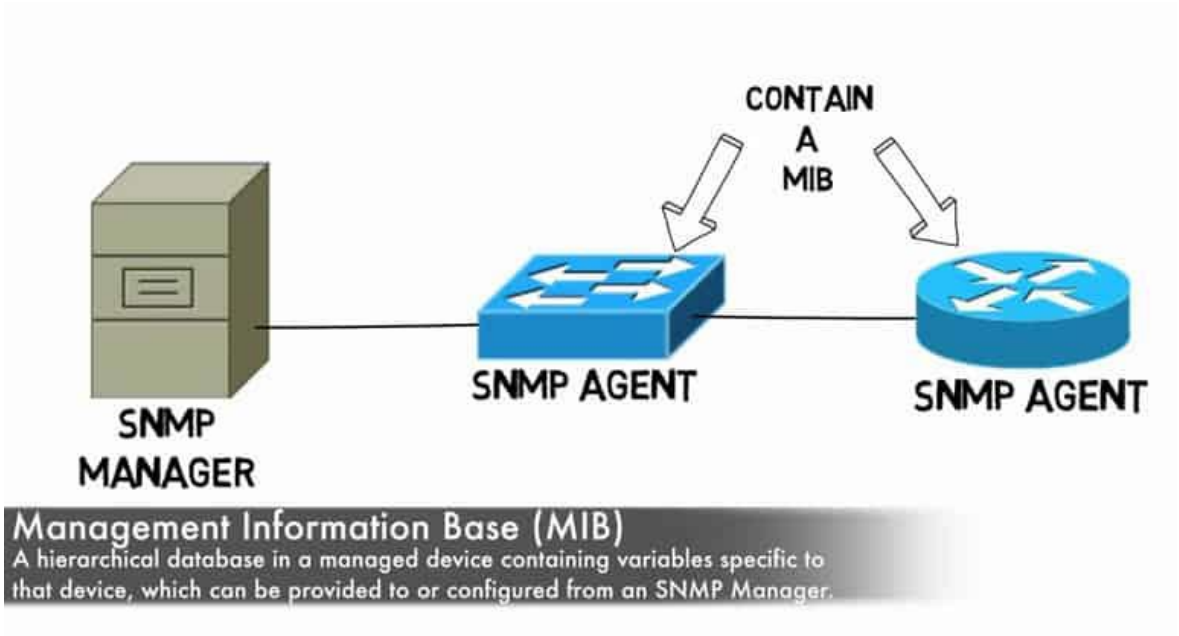
Kuva 2. SNMP-managerin ja Agentin pyynnöt (O'Reilly 2001)

SNMP koostuu SNMP-managerista sekä SNMP-agentista. SNMP-managerit tunnetaan myös nimellä NMS. NMS on sovellus, joka hallitsee verkonhallintatehtäviä. NMS on vastuussa kyselyjen tekemisestä laitteille tietojen hälytysten keräämiseksi, joita kutsutaan trap-pyynnöiksi. Kyselyssä kysytään agentilta kuten reitittimeltä, kytkimeltä tai palvelimelta, tiettyjä tietoja, jotka voivat auttaa määrittämään onko ongelmia ilmennyt. Kun NMS vastaanottaa tiedot agentilta, se ryhtyy toimiin, esimerkiksi varoittaa verkon ylläpitäjiä ongelmasta. (O'Reilly 2001.)

SNMP-agentit ovat taas verkkolaitteissa toimivia ohjelmistoja, jotka vastaavat NMS:n tietopyyntöihin ja ne lähettävät trap-viestejä ilmoittaakseen NMS:lle tietyistä tapahtumista (Kuvassa 2). Useimmissa IP-laitteissa on sisäänrakennetut SNMP-agentit, jotka valvovat laitteen eri komponentteja, kuten liitännän tilaa, ja toimittavat nämä tiedot NMS:lle. Kun agentti havaitsee ongelman, se lähettää trap-pyynnön NMS:lle, joka voi myös lähettää takaisin viestin ”all-clear”, kun ongelma on ratkaistu. (O'Reilly 2001.)

2.2.1 MIB

MIB on tietokanta, jota käytetään SNMP verkkolaitteiden hallintatietojen tallentamiseen ja järjestämiseen. Se sisältää tietokohteita, jotka edustavat erilaisia laiteasetuksia ja tilatietoja, ja jokaisella MIB-tiedoston objektilla on siihen liittyvä yksilöllinen objektitunniste OID. MIB toimii viitekehyksenä SNMP-hallintajärjestelmille, auttaen niitä tulkitsemaan ja näyttämään tietoja verkkolaitteista. (Solarwinds 2024.)



Kuva 3. SNMP-Manageri ja SNMP-Agentit. (Cyberhoot. 2022.)

2.2.2 SNMPv1

SNMPv1 on alkuperäinen versio SNMP-protokollasta, mutta se kärsii merkittävistä tietoturva- ja suorituskykyongelmista. SNMPv1 todennus perustuu salasanan kaltaiseen yksinkertaiseen merkkijonoon, joka lähetetään selkeänä tekstinä verkossa NMS ja SNMP-agenttien välillä. Tämä tekee hallittavista laitteista alttiita luvattomille käyttäjille, jotka voivat helposti muuttaa laitteiden asetuksia, erityisesti jos ACL ei ole käytössä. (Noction 2022.)

SNMPv1-protokollan suorituskyky on rajoittunut, koska se käsittelee vain yksittäisiä objekteja kerrallaan käyttäen Get-, Set- ja Trap-toimintoja. Tämän vuoksi suurten tietomäärien hakeminen vaatii useita erillisiä pyyntöjä, mikä tekee prosessista tehotonta erityisesti silloin, kun kyse on laajamittaisesta tiedonkeruusta. (Noction 2022.)

2.2.3 SNMPv2

SNMPv2 on paranneltu versio alkuperäisestä SNMPv1:stä, joka on suunniteltu korjaamaan useita rajoituksia ja parantamaan verkonhallintatehtävien suorituskykyä. Verrattuna SNMPv1 käyttäviin 32-bittisiin kokonaislukuihin SNMPv2 tuo 64-bittisen kokonaislukutyypin. Tämä muutos antaa SNMPv2:lle mahdollisuuden käsitellä dataa tehokkaammin, koska suurempi kapasiteetti voi vastaanottaa laajempaa dataa. (Noction 2022.)

SNMPv2 tuo myös GetBulkRequest-toiminnon, mikä tehostaa merkittävästi tiedonhakua. Sen sijaan, että NMS-manageri lähettäisi useita toistuvia GetNext-pyyntöjä suuren tietojoukon keräämiseksi, se lähettää yhden GetBulk-viestin agentille. Tämä toiminto palauttaa arvot kaikille pyydetyille muuttujille kerralla, mikä vähentää verkon ylimääräisiä pyyntöjä ja parantaa yleistä suorituskykyä. (Noction 2022.)

Toinen SNMPv2:n huomionarvoinen ominaisuus on InformRequest, joka mahdollistaa luotettavan tiedonsiirron. Tätä pyyntötyyppiä käytetään tyypillisesti ilmoitusten kuittauksiin, jolloin yksi SNMP-hallinta voi vahvistaa viestien vastaanottamisen toiselta. InformRequest-paketti lähetetään toistuvasti, kunnes SNMP manageri vastaanottaa kuittauksen. (Noction 2022.)

2.2.4 SNMPv3

SNMPv3 on vuonna 1998 julkaistu verkonhallintaprotokolla, joka vastaa edeltäjiensä tietoturvapuutteisiin. Tietoturvaa paranneltiin uusilla tyokaluilla: SNMP View, SNMP Groups ja SNMP Users. Näiden ominaisuuksien avulla varmistetaan, että verkkolaitteiden välinen viestintä on aina todennettu ja salattu, mikä merkittävästi vähentää luvattoman käytön riskiä. (Auvik 2024.)

SNMP View'n avulla voidaan tarkasti hallita, mitä tietoja verkonlaitteista käyttäjillä on oikeus nähdä. Esimerkiksi yhdelle käyttäjäryhmälle voidaan sallia pääsy ainoastaan laitteiden rajapintojen tilastoihin, kun taas toiselle ryhmälle voidaan antaa oikeudet tarkastella laitteiston kuntoa koskevia tietoja. Tämä auttaa vähentämään tiedon vuotoriskiä ja parantaa verkon tietoturvaa. (Auvik 2024.)

SNMP Groupsit määrittävät käyttäjien käyttöoikeustason, kuten luku- tai kirjoitusoikeudet, ja ne asettavat yhteyksiin tarvittavan tietoturvatason. Näin voidaan varmistaa, että vain tietyillä käyttäjäryhmillä on oikeus tärkeisiin tietoihin. (Auvik 2024.)

SNMP Usersit ovat ryhmiin lisättäviä käyttäjiä, joilla on omat käyttäjätunnukset, salasanat sekä määritetyt todennus- ja salausmenetelmät. Tämä käyttäjäpohjainen malli lisää tietoturvaa vaatimalla aina todennuksen, kun tietoja halutaan hakea. SNMPv3 tuo myös turvallisuuden parantamiseksi salausstandardeja, kuten SHA, MD5 ja DES, tietojen väärinkäytön estämiseksi. (Auvik 2024.)

3 VERKONVALVONTA OHJELMAT

3.1 Yleistä verkonvalvonta ohjelmista

Verkonvalvontaohjelmien tarkoitus on valvoa verkkoa. Verkonvalvontaohjelmat ovat järjestelmiä, jotka on suunniteltu jatkuvasti valvomaan tietoverkkoa ongelmien, kuten hitaan liikenteen tai komponenttien vikojen varalta. Nämä ohjelmat skannaavat verkkoa jatkuvasti ja ne on suunniteltu ilmoittamaan häiriöt automaattisesti verkonvalvojille.

Ennakoiva verkonvalvonta on tärkeää tietoverkon ylläpitämiseksi. Se havaitsee poikkeamat, jotka voivat johtaa seisokkiin, jos niitä ei valvottaisi. Parhaat verkonvalvontatohjelmat sisältävät ominaisuuksia, kuten visualisoinnin tai kojelaudat. Nämä tarjoavat nopean yleiskatsauksen verkon kunnosta ja näyttävät kaikki poikkeavat olosuhteet, jotka saattavat vaatia huomiota.

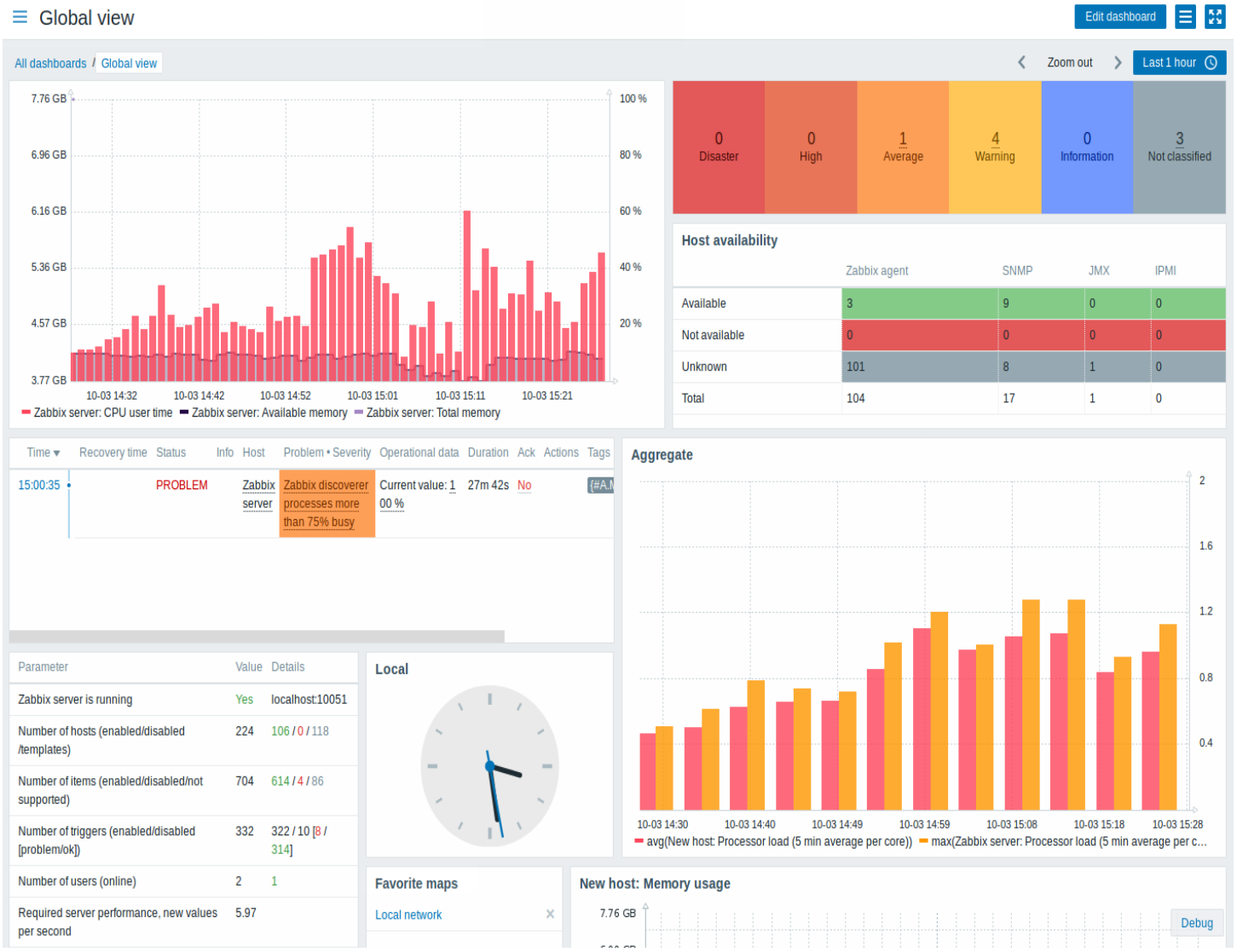
3.2 Zabbix

Zabbix on avoimen lähdekoodin työkalu yritystason valvontaan, jonka kehitti Aleksei Vladishev ja sitä ylläpitää Zabbix SIA. Sen ensimmäinen julkinen versio julkaistiin vuonna 2001. Uusin versio Zabbix 7.2 julkaistiin 22. marraskuuta 2024. Zabbix-yritys perustettiin Latviassa vuonna 2005 Alexei Vladishevin toimesta. (Zabbix 2024.)

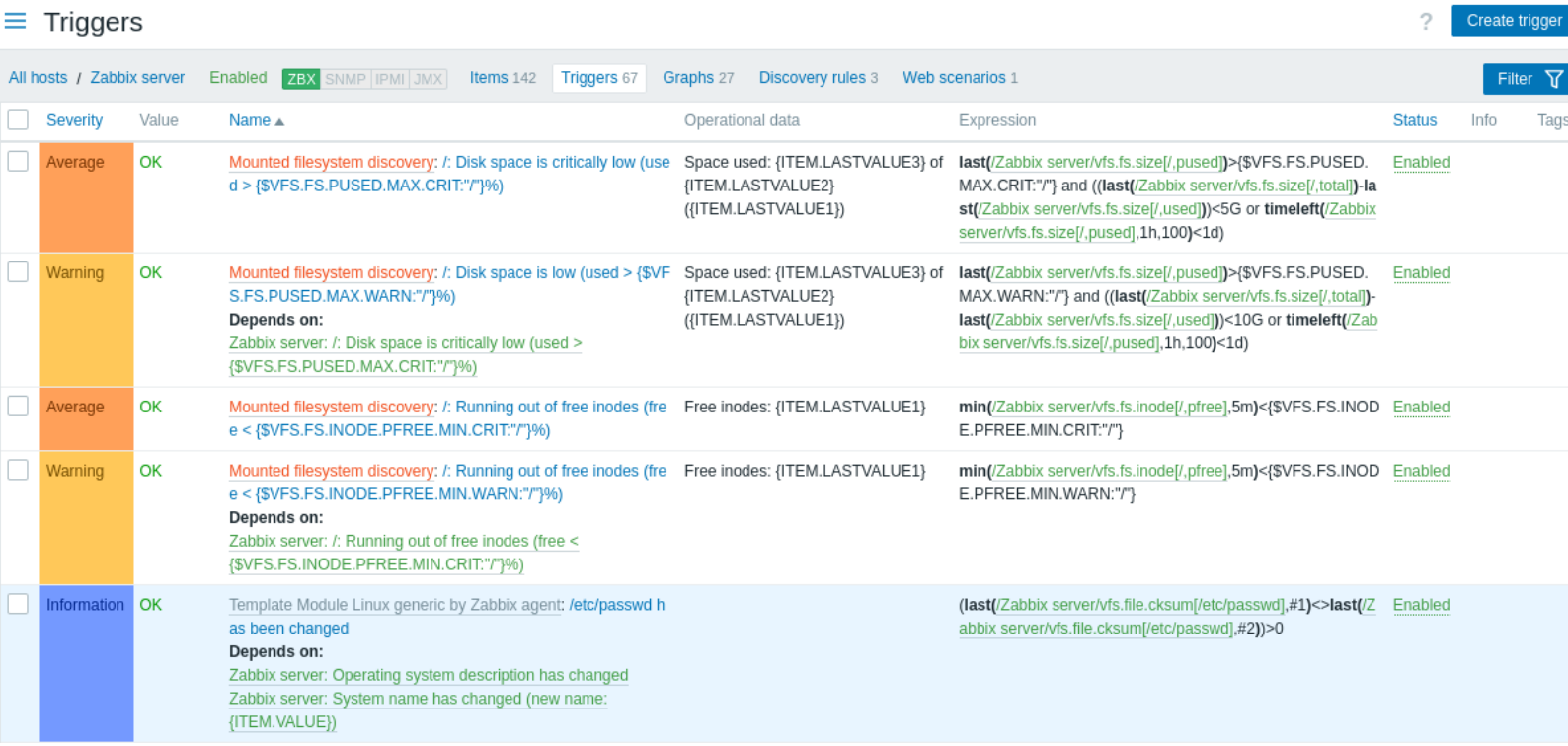
Zabbix on suunniteltu yritysympäristöihin ja se tarjoaa ratkaisuja IT-infrastruktuurin hallintaan ja valvontaan. Kuvassa 4 on Zabbixen kojelauta, mikä toimii valvontakeskuksena. Sitä voi räätälöidä käyttäjän eri tarpeisiin. Ongelmat havaitaan triggereiden avulla. Zabbixen triggereissä on yksityiskohtaiset tiedot ja historia vianmääritystä varten. Kojelaudassa näkyvät tietojen visualisointityökalut, kuten kaaviot ja kartat. Nämä tarjoavat interaktiivisia ja reaaliaikaisia näkemyksiä. (Zabbix 2024.)

Zabbixin yksi komponenteista on Zabbix-palvelin, joka toimii tiedonkeruun keskuksena. Zabbix Agentit keräävät tietoa valvotuista järjestelmistä. Zabbix hyödyntää erilaisia valvontatekniikoita, kuten SNMP ja IPMI. (Zabbix 2024.)

Laitteiden lisääminen valvontaan on yksinkertaista. Nopean ja käyttäjäystävällisen käyttöliittymän ansiosta alusta on käytettävissä mistä tahansa. Zabbixen API mahdollistaa myös automatisoinnin ja integroinnin. Käyttöoikeusjärjestelmä varmistaa turvallisuuden käyttäjien todennuksen ja katselurajoitusten avulla. (Zabbix 2024.)



Kuva 4. Zabbix Kojelauta.(Zabbix 2023)



Kuva 5. Zabbixen triggerit.(Zabbix 2024)

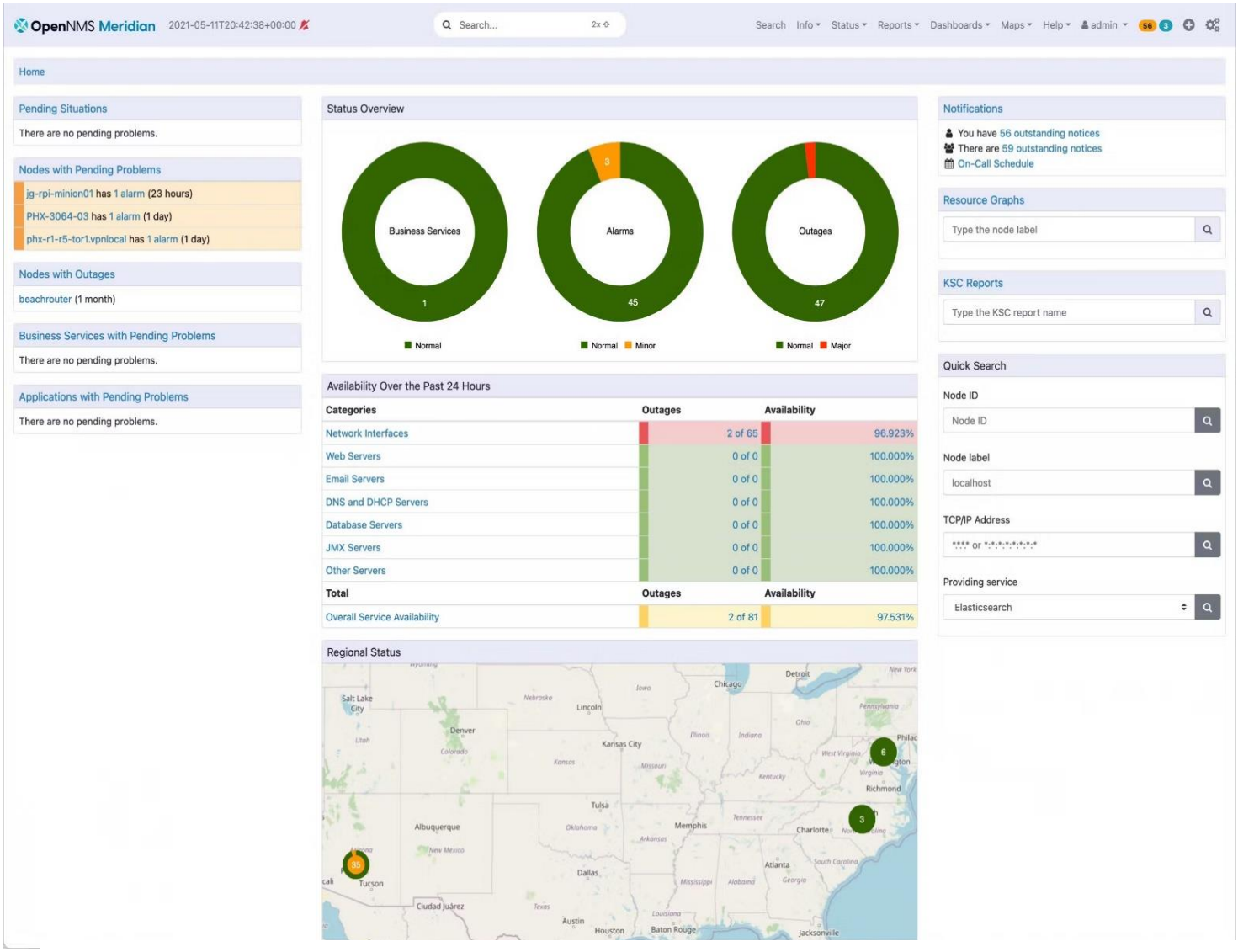
3.3 OpenNMS Meridian

OpenNMS on avoimen lähdekoodin alusta yritystason verkon valvontaan ja hallintaan. Sitä kehittää ja ylläpitää OpenNMS Group. He tarjoavat kaupallisia palveluita, koulutusta ja tukea. OpenNMS:n tavoitteena on olla täysin hajautettu ja skaalautuva verkonvalvonta-alusta. (OpenNMS 2021.)

OpenNMS on suunniteltu yrityksille verkkotopologioiden, palveluiden, sovellusten ja rajapintojen hallintaan ja valvontaan. Sen avulla käyttäjät voivat havaita ja ratkaista tehokkaasti sovellusten ja yrityspalvelujen latenssi- ja saatavuusongelmia. OpenNMS:n mukautettavien monitorien avulla käyttäjät voivat kerätä tietoja viiveestä ja saatavuudesta. Tämä auttaa ratkaisemaan ongelmat nopeasti. (OpenNMS 2021.)

Alusta tarjoaa käyttäjäystävällisen kojelaudan (kuvassa 6), joka näyttää verkko-ongelmia. Se tarjoaa työkaluja tietojen suodattamiseen, ilmoitusten käyttämiseen ja valvontatulosten analysointiin. Tämän kojelaudan avulla järjestelmänvalvojat ja verkonhallitsijat voivat tarkastella ja käsitellä verkko-ongelmia.

OpenNMS:n merkittävä vahvuus on sen häiriölähtöinen arkkitehtuuri, joka tunnistaa käyttökatkokset ja ongelmat nopeasti, luoden tapahtumia ja lähettäen ilmoituksia tai hälytyksiä tarvittaessa. Järjestelmä keskittyy tärkeisiin verkon osiin, mikä auttaa välttämään turhat hälytykset, pitää ilmoitukset selkeinä ja keskittyneinä olennaisiin ongelmiin. (OpenNMS 2021.)



Kuva 6. OpenNMS kojelauta (Softwareadvice.)

4 HÄIRIÖNHALLINTA

4.1 Yleistä häiriönhallinnasta

Häirionhallinta on prosessi, jolla pyritään vähentämään odottamattomien häiriöiden vaikutuksia palauttamalla nopeasti normaali palvelutoiminta. Tavoitteena on minimoida seisokit ja rajoittaa tapausten negatiivisia vaikutuksia käyttäjiin, asiakkaisiin ja koko yrityksen liiketoimintaan. Ratkaisemalla ongelmia nopeasti häirönhallinta auttaa ylläpitämään palvelun laatua ja saatavuutta, mikä varmistaa minimaalisen häiriön päivittäisessä toiminnassa. (IBM)

Verkonhallinnan yhteydessä häirö voi olla eri muodoissa. Se voi olla odottamaton verkkokatkos, joka vaikuttaa yhteyksiin tai kaistanleveyden vaihtelu, joka johtaa vaihtelevaan palvelun laatuun. Häiriö voi olla myös mahdollinen tietoturvauhka, joka voi vaarantaa palvelun luotettavuuden. Tapaukset vaativat tyypistä riippumatta tyypillisesti välitöntä huomiota, jotta ne eivät kasvaisi vakavammiksi ongelmiksi. Jos ongelmat, eivät ratkea tarpeeksi nopeasti ne, voivat aiheuttaa pitkittyneitä seisokkeja tai tietojen menetyksiä. (IBM)

.

4.2 Häiriöiden luokittelu

Häiriöt luokitellaan eri luokkiin vikatilanteesta riippuen. Kun tapahtumat on kirjattu järjestelmään, seuraava vaihe on luokitella ja priorisoida ne. Tämä prosessi on välttämätön vianmääritykseen tarvittavan ajan arvioimiseksi. Se on myös tärkeää eskaloinnin tarpeellisuuden päättämiseksi ja oikean tiimin määrittämiseksi kunkin ongelman ratkaisuun.

Järjestämällä tapaukset luokkiin, kuten verkko-, pilvi-, palvelin- tai virtuaalikerroksiin, häiriönhalinta tiimit voivat rakentaa hyödyllisen tietopohjan aiemmista tapauksista. Tämä data helpottaa vastaavien ongelmien ratkaisemista tulevaisuudessa ja estää niiden toistumisen.

Tapahtumat priorisoidaan myös vakavuuden perusteella. Luokittelu auttaa tiimiä keskittymään kiireellisiin ongelmiin samalla, kun se automatisoi tai ajoittaa alemman prioriteetin tehtävät hoidettaviksi tehokkaammin. (IBM.)

Prioteetti	**Kuvaus**	**Vaikutus**	**Esimerkit**
Prioriteetti 4	- Yleisiä, ei niin vakavia häiriöitä.	- Minimaalinen vaikutus kohteen toiminnallisuuteen.	- Yksittäisen tulostimen toiminnallisuus.
Prioriteetti 3	- Monimutkaisia ongelmia, jotka voivat häiritä suorituskykyä.	- Vaikuttaa kohteen suorituskykyyn, mutta ei estä toimintaa kokonaan.	- Hidas verkkoyhteys. - Yksittäisen palvelimen korkea kuormitus.
Prioriteetti 2	- Keskisuuria häiriöitä, joilla voi olla vakava vaikutus toimintaan.	- Harvinaisia, mutta kriittisiä. - Voivat vaikuttaa merkittävästi osaan verkosta.	- Palvelimen kaatuminen - Verkkokatkos tärkeässä komponentissa
Prioriteetti 1	- Vakavia häiriöitä, joilla on merkittävä vaikutus toimintaan.	- Koko verkon toiminnallisuuden vaarantuminen. - Vaatii välitöntä reagointia.	- Keskuspalvelimen vika. - Core-reitittimen tai core-kytkimen toimimattomuus.

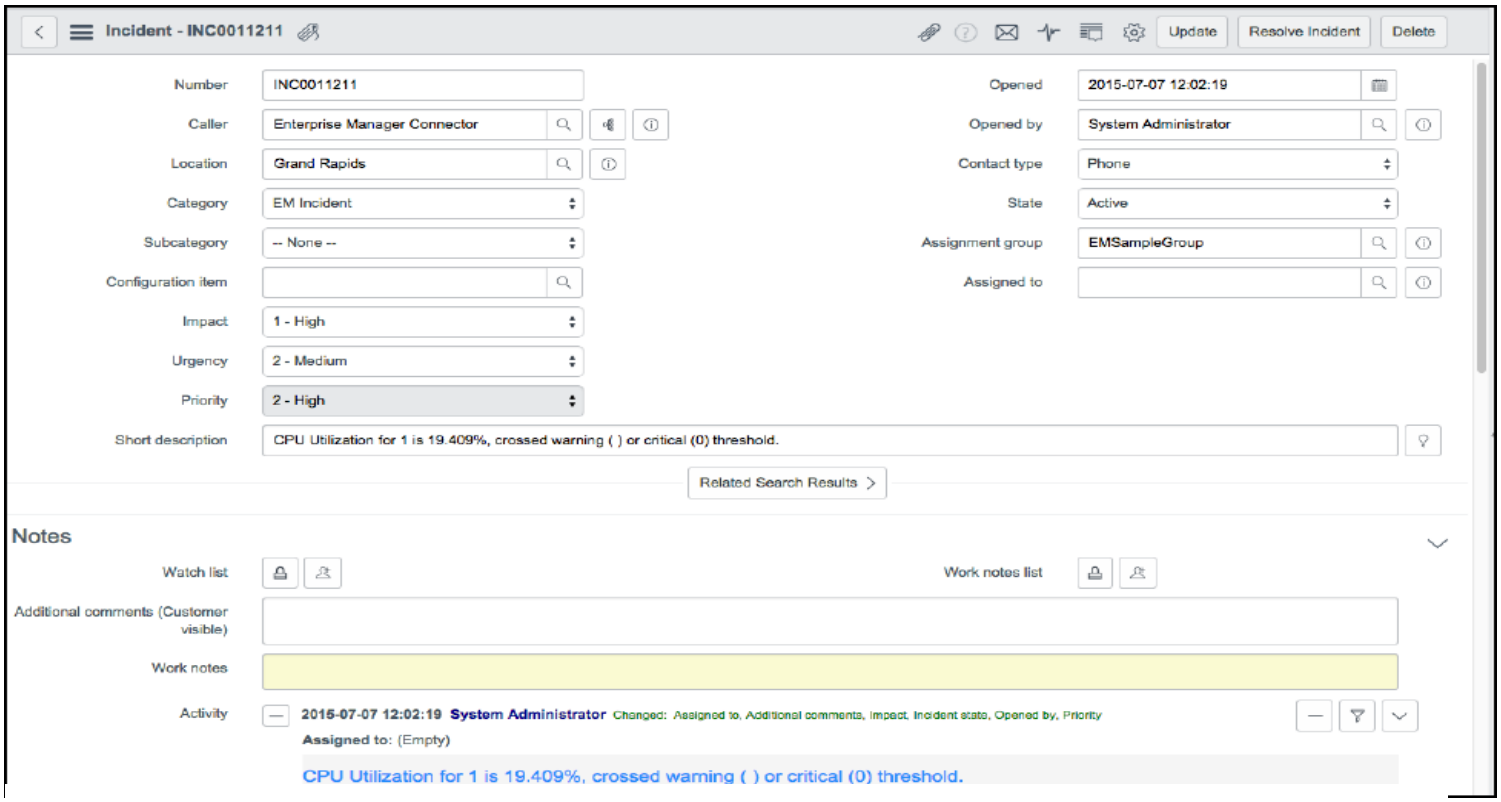
Taulukko 1. Häiriöiden prioteetit

4.3 Häiriöiden tiketöinti

Häiriötiketit ovat häiriöistä generoituneita tikettejä. Häiriöt ovat yleensä suunnittelemattomia ja vaikuttavat normaaliin palvelun toimintaan. Häiriötiketit ovat osana häiriönhallintaprosessia, joka on tärkeä osa IT-palvelunhallintaa. Häiriötiketit ovat osana ITIL-viitekehyksen käytäntöjä. Häiriötioketin luomisen yhteydessä tallennetaan tärkeät tiedot, kuten ongelman kuvaus, siihen liittyvät palvelut tai järjestelmät, kiireellisyys, tärkeys sekä tehdyt toimenpiteet. Tavoitteena on palauttaa normaali toiminta mahdollisimman nopeasti, minimoiden seisokit ja organisaation toimintaan kohdistuvat vaikutukset. (ServiceNow 2024.)

Häiriön tunnistamisen jälkeen ongelma raportoidaan ja dokumentoidaan häiriötikettinä. Tämän jälkeen tiketti luokitellaan ongelman vakavuuden mukaan. Tämä helpottaa sen ohjaamista oikeille tiimeille tai resursseille. Kriittisimmät häiriöt eskaloidaan välitöntä huomiota varten. Ilmoitukset lähetetään asiakkaille tiketin sen hetkisestä tilasta. Tiketti voidaan eskaloida, jos sen ratkaiseminen vaatii lisää asiantuntemusta tai resursseja. Ratkaisun toteutuksen jälkeen tiketti suljetaan ja kaikki merkittävät tiedot, kuten ratkaisutoimet ja ehkäisevät toimenpiteet, kirjataan myöhempää analysointia varten. (ServiceNow 2024.)

Häiriötiketit tuovat merkittäviä etuja, kuten tehokkuuden parantamisen standardoimalla ongelmien käsittelyä ja ratkaisua. Tiketit parantavat palvelun laatua auttamalla priorisoimaan ongelmat tehokkaasti ja varmistamalla kriittisten häiriöiden ripeän käsittelyn. Häiriötiketit lisäävät myös läpinäkyvyyttä ja mahdollistavat työntekijöille ja sidosryhmille ongelmien tilan seuraamisen alusta loppuun. Tämä vahvistaa luottamusta ja parantaa viestintää. Ne tarjoavat myös arvokasta tietoa toistuvien ongelmien ja trendien tunnistamiseen, mahdollistaen ennakoivien toimenpiteiden suunnittelun ja häiriöiden ehkäisemisen. (ServiceNow 2024.)



Kuva 7. Esimerkki häiriö tiketistä.(Oracle)

5 VERKONVALVONNAN TEHOSTAMINEN

5.1 Tehostamisen tarpeet ja tavoitteet

Työn tavoitteena on suorittaa kattava vertailu kahden tietoverkon valvontaohjelmiston, OpenNMS Meridianin ja Zabbixin välillä ja valita niistä organisaation tarpeisiin parhaiten soveltuva vaihtoehto. Tämä auttaa tunnistamaan ohjelmiston, joka tarjoaa optimaalisen yhdistelmän ominaisuuksia, kustannustehokkuutta ja käytettävyyttä sekä samalla täyttää tietoturvan ja toimintavarmuuden vaatimukset. Verkonvalvonnan tehostamisessa pyritään löytämään oikea ohjelmisto, joka voisi toimia Telia Cygaten verkonvalvonnan varaohjelmistona.

Tavoitteena on myös varmistaa, että valittu ohjelmistoratkaisu tukee organisaation kasvua ja skaalautuvuutta. Tietoverkkojen laajentuessa valvonnan ja häiriönhallinnan tarpeet muuttuvat ja monimutkaistuvat.

5.2 Zabbixen ja OpenNMS meridianin vertailu

Zabbix ja OpenNMS Meridian ovat molemmat loistavia valvontatyökaluja. Ne palvelevat kuitenkin eri tarkoituksia ja vastaavat erilaisiin käyttäjien tarpeisiin.

Zabbix on monipuolinen verkonvalvonta alusta, joka on suunniteltu palvelimien, verkkojen ja sovellusten seurantaan. Se tunnetaan helppokäyttöisyydestään, vahvoista visualisointiominaisuuksistaan ja laajoista hälytysvaihtoehdoistaan. Zabbix sopii hyvin pienille ja keskisuurille yrityksille, jotka etsivät mukautettavaa ja joustavaa seurantaratkaisua.

OpenNMS Meridian puolestaan on suunniteltu erityisesti laajamittaiseen verkon suorituskykyyn ja vianhallintaan. Se on erinomainen ympäristöissä, joissa on monimutkaisia, hajautettuja verkkoinfrastruktuureja ja se tarjoaa syvällisiä näkemyksiä palvelunvarmistuksesta, suorituskyvystä ja liikenteen hallinnasta.

Zabbix tarjoaa kaikki yhdessä lähestymistavan IT- ja yritysvalvontaan, kun taas OpenNMS Meridian keskittyy enemmän verkonhallintaan ja edistyneisiin ominaisuuksiin. OpenNMS meridian on ihanteellinen suuria verkkoja hallinnoiville yrityksille. Zabbix toisaalta tarjoaa laajemman valvontaratkaisun, joka vetoaa laajempaan käyttäjäjoukkoon, kuten IT-osastot ja pienemmät tiimit.

Ominaisuudet	**OpenNMS Meridian**	**Zabbix**
Skaalautuvuus	- Erittäin skaalautuva. - Suunniiteltu suurille verkoille.	- Sopii pienille sekä suurille yrityksille.
Helppokäyttöisyys	- Monimutkainen asennus - Suunniteltu suurille yrityksille.	- Käyttäjäystävällinen käyttöliittymä - Sopii erityisesti pienille ja keskikokoisille ympäristöille.
Hinta	- OpenNMS core 12000$ vuodessa. - OpenNMS Essential 49000$ vuodessa . - OpenNMS premier+ asiakaskohtainen.	- Ilmainen.
Tuetut protokollat	- SNMP, WMI, HTTP ja JMX.	- SNMP, HTTP, IPMI ja SSH.

Käyttöliittymä	- Monipuolinen, mutta sekava.	- Selkeä ja käyttäjäystävällinen.
Käyttäjätuki	- OpenNMS core versiossa ei ole käyttäjätukea. - Muissa suunnitelmissa on käyttäjätuki.	- Viiden eri tason käyttäjätuki. - Lisämaksusta.

Taulukko 2. OpenNMS Meridian ja Zabbix vertailu.

6 HÄIRIÖNHALLINNAN KEHITYSEHDOTUKSET

Yksi kehityskohteista on dokumentaation kehittäminen. On tärkeää, että dokumentointi verkonvalvonnasta ja häiriönhallinnasta on hyvin ylläpidetty ja helposti saatavilla. Dokumentaatio tukee kaikkia häiriönhallinnan vaiheita aina vian selvittämisestä ongelman ratkaisuun. Kehitystoimet sisältävät dokumentaation yhtenäistämistä, ohjeiden päivittämistä ja verkkokuvien päivitystä. Tärkeitä toimenpiteitä ovat verkon rakenteiden ja laitteiden konfiguraatioiden säännöllinen tarkistus ja päivittäminen, jotta kaikki tärkeät tiedot ovat aina saatavilla. Parannettu dokumentaatio vähentää tietokatkoja, edistää sujuvaa yhteistyötä tiimien välillä ja nopeuttaa häiriöiden hallintaa. Tämä johtaa ICT-palveluiden parempaan luotettavuuteen ja suorituskykyyn.

Toinen kehityskohde on automaattiset korjaustoimenpiteet. Tietyissä järjestelmissä voidaan määrittää, että ohjelmisto suorittaa tiettyjä korjaavia toimia ilman ihmisen puuttumista. Esimerkiksi palvelimen uudelleenkäynnistys tai palveluprosessin uudelleenkäynnistäminen voidaan toteuttaa automaattisesti. Näin on mahdollista estää häiriön leviämisen ja palauttaa palvelun toiminta nopeasti.

Toistuvien tehtävien automatisointi on myös tehokas tapa vähentää IT-tiimin työkuormaa. Rutiininomaiset tehtävät, kuten lokitiedostojen analysointi tai järjestelmän päivitysten tarkistus voidaan hoitaa esimerkiksi skripteillä. Tämä vapauttaa asiantuntijoiden aikaa monimutkaisempien ongelmien käsittelyyn.

.

7 YHTEENVETO

Tässä opinnäytetyössä tutkittiin, miten verkonvalvontaa ja häiriönhallintaa voidaan tehostaa vertailemalla kahta verkonvalvontaohjelmistoa, OpenNMS Meridiania ja Zabbixia. Tavoitteena oli selvittää, millä tavoin organisaatiot voivat kehittää häiriönhallintaansa ja parantaa verkonvalvontaansa. Vertailussa keskityttiin ohjelmistojen tärkeimpiin ominaisuuksiin, suorituskykyyn, käytettävyyteen ja skaalautuvuuteen.

Tulokset osoittivat, että OpenNMS Meridian sopii erityisen hyvin suurten ja monimutkaisten verkkoympäristöjen hallintaan. Ohjelmisto tarjoaa edistyneitä ominaisuuksia, kuten topologiakartoituksen ja BGP-valvonnan, jotka auttavat pitämään suuret verkot hallinnassa. Zabbix taas on monipuolinen ja käyttäjäystävällinen ratkaisu, joka sopii erityisesti IT-osastoille ja pienemmille tiimeille. Se tarjoaa kattavan valvontaratkaisun, joka täyttää laajan käyttäjäjoukon tarpeet.

Ohjelmiston valinta riippuu aina organisaation erityistarpeista, kuten verkon koosta, monimutkaisuudesta ja valvonnan tarpeista. Myös palvelun hinta vaikuttaa oikean ohjelmiston löytämiseen.

Tulevaisuudessa häiriönhallinnan merkitys korostuu entisestään. Yritysten toimintaympäristöt monimutkaistuvat ja digitaaliset palvelut yleistyvät. Nykyisessä liiketoimintamaailmassa jo pienetkin käyttökatkokset aiheuttavat merkittäviä taloudellisia tappioita ja heikentävät asiakkaiden palvelukokemusta. Näihin asioihin panostaminen yrityksissä on tärkeää, jotta ne pystyvät säilyttämään paremmin kilpailukykynsä.

Lähteet

Mauro, D. Schmidt K. 2001 Chapter 1. Introduction to SNMP and Network Management. Viitattu 15.10.2024 Saatavissa https://www.oreilly.com/library/view/essential-snmp-2nd/0596008406/ch01.html

IBM. 2024 What is network monitoring?
Viitattu 15.10.2024 Saatavissa https://www.ibm.com/topics/network-monitoring

Noction 2022. SNMP evolution and version differences. SNMP security models/levels details. Viitattu 18.10.2024 saatavissa https://www.noction.com/blog/snmp-versions-evolution-security

Solarwinds What is MIB 2024. Viitattu 19.10.2024 Saatavissa https://www.solarwinds.com/resources/it-glossary/mib

Steve Petryschuk protocols & communication SNMPv2 vs. SNMPv3: An SNMP Versions Comparison Table. 2024 Viitattu 21.10.2024 Saatavissa https://www.auvik.com/franklyit/blog/difference-between-snmp-v2-v3/

SNMP Monitoring: An Introduction and Practical Tutorial. Kentik 2024 Viitattu 15.10.2024 Saatavissa https://www.kentik.com/kentipedia/snmp-monitoring/

Zabbix 6.0 dokumentaatio. Viitattu 30.10.2024 Saatavissa https://www.zabbix.com/documentation/6.0/en/manual/web_interface/frontend_sections/monitoring/dashboard

Cisco 2005. TCP/IP Overview. Viitattu 25.10.2024 Saatavissa https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html

IBM. What is incident management? Viitattu 30.10.2024

Saatavissa https://www.ibm.com/topics/incident-management

OpenNMS 2021.OpenNMS Meridian Datasheet. Viitattu 25.11.2024

Saatavissa https://www.opennms.com/wp-content/uploads/2021/05/Meridian-Data-Sheet.pdf

Servicenow 2024. What is incident management? Viitattu 26.11.2024

Saatavissa https://www.servicenow.com/products/itsm/what-is-incident-management.html

Zabbix 2024. What is Zabbix. Viitattu 28.11.2024 Saatavissa https://www.zabbix.com/documentation/current/en/manual/introduction/about

Zabbix 2024. Triggers. Viitattu 28.11.2024 Saatavissa

https://www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/data_collection/hosts/triggers

Softwareadvice. OpenNMS Viitattu 29.11.2024 Saatavissa https://www.softwareadvice.ie/software/240633/opennms

Cyberhoot 2022. Management Information Base. Viitattu 29.11.2024 Saatavissa https://cyberhoot.com/cybrary/management-information-base-mib/

OpenNMS. OpenNMS Meridian. Viitattu 20.11.2024 Saatavissa https://www.opennms.com/wp-content/uploads/2021/05/Meridian-Data-Sheet.pdf

Oracle. Creating ServiceNow Tickets. Viitattu 27.11.2024 Saatavissa https://docs.oracle.com/cd/E24628_01/em.121/e64520/create_tickets.htm#EMSNC137