



SAVONIA

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

EIS -INFRASTRUKTUURIN MONITOROINTI

TEKIJÄ/T: Henri Järveläinen

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Henri Järveläinen	
Työn nimi EIS -infrastruktuurin monitorointi	
Päiväys 6.6.2019	Sivumäärä/Liitteet 22/0
Ohjaaja(t) Pasi Liimatainen, Keijo Kuosmanen	
Toimeksiantaja/Yhteistyökumppani(t) Proxion Oy	
<p>Tiivistelmä</p> <p>Tämän opinnäytetyön aiheena oli tutustua eri monitorointiohjelmistoihin, vertailla niitä ja valita Proxionin antamiin vaatimuksiin sopivin. Sopiva ohjelmisto tulisi tämän jälkeen asentaa ja konfiguroida osaksi Proxionin EIS -infrastruktuuria ja demonstroida sen toimivuutta Proxionin ympäristössä.</p> <p>Alustavasti monitoroitavien kohteiden määrä ja monitoroinnin tarve on aika minimaalinen, mutta uutena ja kasvavana yrityksenä Proxionin tulevaisuuden suunnitelmissa on laajentaa EIS -infrastruktuuriaan ja näin ollen monitoroinnin tarve ja tarpeellisuus kasvaa monitoroitavien kohteiden lisääntyessä.</p> <p>Lopputuloksena monitorointiohjelmistoksi valikoitui Zabbix. Zabbix asennettiin ja integroitiin osaksi Proxionin IT -infrastruktuuria. Toimivuus demonstroitiin muutamalla tärkeimmällä monitorointikohteella ja jatkossa kohteita lisätään. Monitorointiprojekti jatkuu opinnäytetyön jälkeenkin.</p>	
Avainsanat EIS -infrastruktuuri, IT -infrastruktuuri, monitorointi	

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Henri Järveläinen			
Title of Thesis Monitoring of EIS infrastructure			
Date	6.6.2019	Pages/Appendices	22/0
Supervisor(s) Pasi Liimatainen, Keijo Kuosmanen			
Client Organisation /Partners Proxion Oy			
<p>Abstract</p> <p>The subject of this thesis was to research and compare different IT infrastructure monitoring solutions and find a suitable programme for Proxion's needs. After finding a suitable program, it had to be installed and integrated in to the EIS infrastructure of Proxion. After this, basic functionality of the program in Proxion's environment had to be demonstrated.</p> <p>At the moment the need and scope for monitoring is minimal, but as a young and growing organisation Proxion aims to enlargen their infrastructure and thus increase the need for proper monitoring.</p> <p>As a result of this thesis, the monitoring software Zabbix was chosen and implemented into Proxion's IT -infrastructure. Basic functionality was demonstrated. The monitoring project will continue further after this thesis.</p>			
Keywords EIS infrastructure, IT infrastructure, monitoring			

ESIPUHE

Haluaisin aluksi kiittää Proxionia opinnäytetyön aiheen laatimisesta ja antamisesta, sekä tuesta ja joustavuudesta projektin teon aikana.

Kiitokset kuuluvat myös opinnäytetyöni ohjaavalle opettajalle, Pasi Liimataiselle, joka on tarjonnut tukea ja ohjausta tarvittaessa.

Lopuksi iso kiitos perheelle ja ystäville, jotka ovat tukeneet ja kannustaneet koko opinnäytetyöprosessin aikana minua ja motivoineet ja joskus jopa potkineetkin minua puristamaan loppuun asti.

TERMIT JA LYHENTEET

EIS = Energy Integration System eli erilaisista energiantuotantolaitteista ja muista oheislaitteista koostuva infrastruktuuri.

HTTPS = Hypertext Transfer Protocol Secure eli suojattuun verkkoyhteyteen käytettävä protokolla.

SSL = Secure Sockets Layer eli varmenne suojatun verkkoyhteyden luotettavuudesta.

MYSQL = My Structured Query Language eli tiedonhallinnassa käytettävä kyselykieli.

TCP = Transmission Control Protocol eli datankuljetusprotokolla.

LDAPS = Lightweight Directory Access Protocol Secure eli suojattuun AD -liikenteeseen käytettävä protokolla.

SNMP = Simple Network Management Protocol eli laitteen tilatietojen lähettämiseen käytettävä protokolla.

SMTP = Simple Mail Transfer Protocol eli sähköpostin välitykseen käytettävä protokolla.

SSH = Secure Shell eli komentorivipohjainen etäyhteys.

UFW = Uncomplicated Firewall eli Linuxin oma palomuuuri.

VPN = Virtual Private Network eli tapa yhdistää ja käyttää verkkoa johon ei saa suoraan yhteyttä.

SISÄLTÖ

1	JOHDANTO	8
2	TYÖ	9
2.1	Tarkoitus.....	9
2.2	Vaatimukset	9
2.2.1	Ilmainen ja avoin lähdekoodi.....	9
2.2.2	Kolmannen osapuolen pluginit.....	9
2.2.3	SQL.....	10
2.2.4	SNMP	10
2.2.5	OS Lokit.....	10
2.2.6	Open VPN	10
2.2.7	Käyttäjälöki	10
2.2.8	Käyttäjäkohtaiset asetukset ja näkymät.....	10
2.2.9	SMS ja Email notifikaatiot	10
2.3	Suunnittelu.....	11
2.4	Dokumentointi	11
3	MONITOROINTIOHJELMISTON VALINTA	12
3.1	Ohjelmistovaihtoehdot ja niiden vertailu.....	12
3.2	Lopullinen valinta	13
4	ZABBIX -PALVELIN	14
4.1	Yleiskatsaus Zabbixiin	14
4.1.1	Zabbix server	14
4.1.2	Zabbix agent.....	15
4.2	Asennus virtuaalipalvelimelle	15
4.2.1	Tiedonhallinta.....	16
4.2.2	Tietoliikenne ja tietoturva	16
4.2.3	Autentikointi.....	17
4.2.4	Version päivittäminen.....	17
5	MONITOROINTI	18
5.1	Monitoroitavat kohteet ja virhetilanteet.....	18
5.2	Käyttäjänhallinta	19
5.3	Sähköpostinotifikaatiot.....	20

6 YHTEENVETO.....	21
LÄHTEET	22

1 JOHDANTO

Proxion on raideliikenteen ja raideinfrastruktuurin turvallisuuden, käytettävyyden ja sujuvuuden kehittämiseen keskittynyt suomalainen yritys. Se on perustettu vuonna 2005 ja sillä on toimipisteitä ympäri suomen. Pääkonttori sijaitsee Helsingissä. IT -osasto, jossa tein hommia, on vain muutaman vuoden vanha.

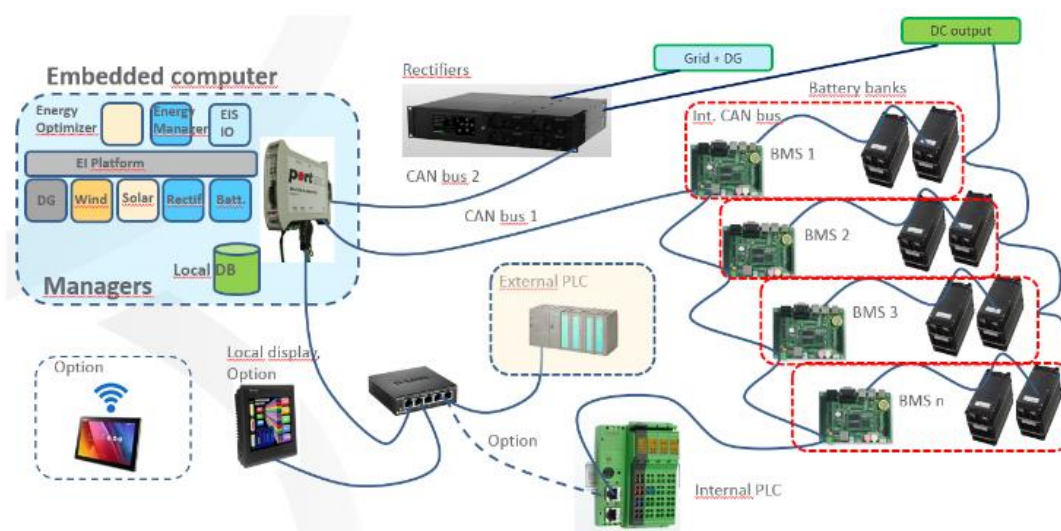
Proxionin EIS eli Energy Integration System -infrastruktuuri koostuu erilaisista laitteista, kuten palvelimista, kytkimistä, reitittimistä, sekä päätelaitteista. Monitoroinnin tarve on tässä vaiheessa vielä varsin minimaalinen, mutta tulevaisuudessa toivottavasti pystyttäisiin laajentamaan jopa tuhansiin laitteisiin.

Opinnäytetyöni aihe oli siis tutkia ja tutustua eri monitorointiohjelmistoihin, valita Proxionin vaatimuksiin sopiva ja asentaa ja konfiguroida se toimimaan Proxionin ympäristöön ja demonstroida sen toimintaa.

2 TYÖ

2.1 Tarkoitus

Työn tarkoitus oli asentaa ja konfiguroida vaatimusten mukainen monitorointiohjelmisto Proxionin EIS -infrastruktuuriin, jonka avulla pystytään valvomaan infrastruktuurin eri osia ja niiden välillä kulkevaa dataliikennettä. Infrastruktuurin eri laitteet kommunikoivat toimintaansa omien rajapintojensa kautta. Näitä rajapintoja hyödyntäen monitorointiohjelmisto näyttää ja varastoi laitteista haluttua dataa, ja ilmoittaa oikeille vastuuhenkilöille mahdollisista vikatilanteista ja häiriöistä, sekä lähettää vikatietoja eteenpäin esim. tiketteinä Proxionin omiin järjestelmiin.



KUVA 1. EIS -infrastruktuurin laitteisto.

2.2 Vaatimukset

Tavoitteena oli siis löytää, asentaa ja konfiguroida Proxionin tarpeisiin sopiva monitorointiohjelmisto. Ohjelmiston tekniset vaatimukset olivat etenkin allaolevat.

2.2.1 Ilmainen ja avoin lähdekoodi

Lähtökohtana oli, että ohjelma olisi ilmainen ja avoimen lähdekoodin omaava. Maksullinen ohjelma ei kuitenkaan ollut täysin poissuljettua, jos tarpeeksi hyvää ilmaista ohjelmaa ko. tarpeeseen ei löydy.

2.2.2 Kolmannen osapuolen pluginit

Ohjelmaan pitää pystyä implementoimaan kolmannen osapuolen plugineita, tai kirjoittamaan omia tulevaisuuden tarpeiden mukaan.

2.2.3 SQL

SQL -kantoja ja -palvelimia tulisi pystyä monitoroimaan, sillä on tärkeää tietää milloin kantoihin on tehty muutoksia, mitä on tehty ja kuka on tehnyt.

2.2.4 SNMP

Monitorointia täytyy pystyä suorittamaan SNMP -protokollan, eli laitteen tilatietojen välittämiseen tarkoitetun protokollan avulla.

2.2.5 OS Lokit

Ohjelmiston täytyy pystyä monitoroimaan lokitiedostoja, joiden avulla pysytään kartalla siitä mitä on tapahtunut, milloin on tapahtunut, ja mistä se on johtunut.

2.2.6 Open VPN

VPN -verkkoyhteyksien monitoroinnin on oltava tuettua, jotta pystyttäisiin havaitsemaan infrastruktuurissa olevien verkkojen tila ja virhetilanteissa ongelman etsiminen olisi helpompaa ja nopeampaa.

2.2.7 Käyttäjälöki

Ohjelmassa pitää olla käyttäjälöki, josta näkee kuka on tehnyt, mitä on tehnyt ja milloin on tehnyt. Tällöin ongelmanratkaisu on nopeampaa kun osataan kohdentaa se tietylle käyttäjälle.

2.2.8 Käyttäjäkohtaiset asetukset ja näkymät

Eri käyttäjille tulee pystyä määrittämään eri näkymiä ja monitorintikohteita vastuualueiden mukaan. Tämä selkeyttää yksittäisten henkilöiden työtä välttämällä kaikki itseään koskemattomat virhetilanteet ja notifiikaatiot.

2.2.9 SMS ja Email notifiikaatiot

SMS – ja Email -notifiikaatioiden lähettäminen virhetilanteissa tulee olla mahdollista. Tällöin tarvittavat henkilöt saavat nopeasti tiedon vikatilanteista.

2.3 Suunnittelu

Opinnäytetyön suunnittelu aloitettiin aloituspalaverilla, jossa käytiin työnkuva läpi pääpiirteittäin, sovittiin kaikki byrokraattiset asiat kuntoon ja mietittiin myös aikataulusioita. Aloituspalaverin jälkeen pidettiin pienemmällä porukalla toinen palaveri, jossa käytiin tarkemmin läpi työn tavoitteet ja aikataulutus. Suunnitteluvaiheessa nousi ilmi projektin tutkimuksellinen luonne, ja miten helposti se voi valua väitöskirjamaiseksi. Kyseessä on kuitenkin nimenomaan insinöörityö, joten pyrkimyksenä on pitää lopputulos mahdollisimman insinöörimäisenä ja käytännönläheisenä.

2.4 Dokumentointi

Kuten joka ikisessä tekemässäni IT -projektissa, tässäkin työssä dokumentointi on erittäin tärkeää, ja sitä painotettiin paljon myös työnantajan toimesta. Tämän raportin lisäksi dokumentoin kaikki työn vaiheet Proxionin ATLASIAN -pohjaiseen wikisivustoon. Hyvän dokumentoinnin avulla kaikki pysyy hyvin kartalla mitä Zabbix -palvelimelle on oikeasti tehty, virhetilanteissa tämä on todella arvokasta ajanhallinnan ja täsmällisyyden kannalta.

3 MONITOROINTIOHJELMISTON VALINTA

3.1 Ohjelmistovaihtoehdot ja niiden vertailu

Työn ensimmäinen vaihe oli hakea tietoa eri monitorointiohjelmista, ja vertailla niiden soveltuvuutta Proxionin vaatimuksiin. Alla lueteltuna kuusi löytämäni ja tutkimaani kandidaattia.

- Nagios
- Icinga
- Zabbix
- Prometheus
- Pandora FMS
- Open NMS

Kaikki löytämäni vaihtoehdot soveltuivat enemmän tai vähemmän Proxionin tarpeisiin ja vaatimuksiin. Vaatimusmäärittelyjen lisäksi vertailin ohjelmistojen käytettävyyttä, sekä tuen ja ohjeiden saatavuutta ja yleisyyttä.

Alla taulukko, jossa vertailen kaikkia ohjelmistoja ja niiden sopivuutta Proxionin vaatimuksiin (Nagios on jätetty pois ennen tätä vaihetta, sillä Nagioksen ilmaisversio Nagios Core on liian pelkistetty tähän tarkoitukseen).

Monitorointiohjelmistovertilu

	ZABBIX	ICINGA	PROMETHEUS	PANDORA FMS	OPEN NMS
Kolmannen osapuolen pluginit	x	x	x	x	
SMS ja Email ilmoitukset	x	x	x	x	x
SQL tuki	x	x	x	x	x
SNMP tuki	x	x	x	x	x
OS Logit	x	x	x	x	x
Open VPN	x	x	x	x	
RMS	x	x			
TSDB	x	x	x		x
Käyttäjä logit	x	x	x	x	x
Käyttäjakohtaiset asetukset ja näkymät	x	x	x	x	x

KUVA 2. Monitorointiohjelmistojen vertailu annettuun vaatimuksiin.

3.2 Lopullinen valinta

Tarkastelin eri ohjelmistovaihtoehtoja kunkin ohjelmiston nettisivuja ja manuaaleja lueskellen, joiden perusteella siis tein edellisessä kappaleessa olleen taulukon. Taulukon perusteella valitsin kaksi vaihtoehtoa jatkovertailuun. Nämä olivat **Icinga** ja **Zabbix**.

Tarkastelin Icingaa ja Zabbixia saamieni vaatimusten perusteella, sekä myös yleisen käytettävyyden ja monipuolisuuden kantilta. Yksi tärkeä tekijä oli myös tunnettuus ja tiedon ja ohjeiden ja tuen saatavuus.

Alkuperäinen suunnitelma oli testiksi asentaa sekä Zabbix että Icinga omalle virtuaalikoneelleni ja sitä kautta testailla ja päättää kummalla lähden jatkamaan työtä eteenpäin. Molemmilla ohjelmilla löytyi webissä testattava demo, joita vertailin ja tein jo joitakin havaintoja Zabbixin paremmasta käytettävyydestä ja monipuolisemmasta käyttöliittymästä. Asensin Zabbixin virtuaalikoneelleni ja se sujui kaikin puolin mutkattomasti. Katselin myös hieman Icingan asentelua, mutta en missään vaiheessa kerinnyt omalle virtuaalikoneelle asti sitä asentaa. Zabbixin käyttöliittymä vetosi monipuolisuudellaan ja käytettävyydellään, ja koko Zabbixin brändi oli netissä lukemani ja näkemäni perusteella paljon laajemmin tuettu ja tunnettu. Zabbixissa oli myös kaikki vaaditut ominaisuudet, joten lopullinen päätös oli aika selkeä.

4 ZABBIX -PALVELIN

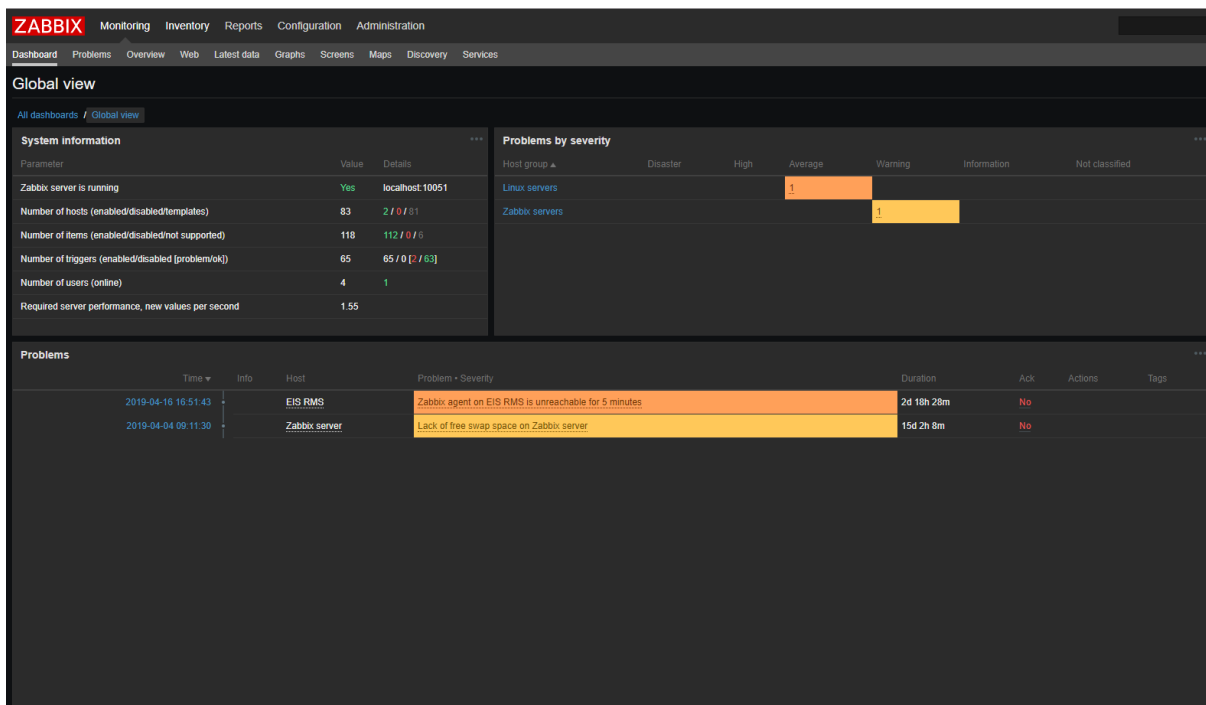
4.1 Yleiskatsaus Zabbixiin

Zabbix on ilmainen, avoimen lähdekoodin IT -infrastruktuurien monitorointiohjelmisto. Zabbix on erittäin monipuolinen ja sillä voi monitoroida lähes mitä vaan IT -infrastruktuuriin kuuluvia komponentteja, kuten palvelimia, päätelaitteita, pilvipalveluita, tietoverkkoja, ohjelmistoja, palveluja, sekä tietokantoja.

Zabbixiin kuuluu kaksi pääkomponenttia: **Zabbix server** ja **Zabbix agent**. (Zabbix.)

4.1.1 Zabbix server

Zabbix server on itse monitorointiohjelma. Se on saatavilla ainoastaan Linuxille, joten monitorointipalvelimen täytyy aina olla Linux. Zabbix serverillä on intuitiivinen web-käyttöliittymä, jolla on helppo valvoa ja monitoroida kaikkia infrastruktuurin eri komponentteja. Web-käyttöliittymällä pystyy myös piirtämään monitorointidatan avulla kaikenlaisia graagisia kaavioita, taulukoita ja diagrammeja.



KUVA 3. Zabbix serverin web -käyttöliittymän etusivu

4.1.2 Zabbix agent

Zabbix agent on monitoroitavien kohteiden tapa kommunikoida monitorointipalvelimelle. Agentti asennetaan monitoroitavaan kohteeseen, josta monitorointitarpeen mukaan se joko itse automaattisesti lähettää tietoa monitorointipalvelimelle (aktiivinen monitorointi), tai odottaa monitorointipalvelimelta pyyntöä tietojen lähettämisestä (passiivinen monitorointi). Agentista on myös Windows ja Mac versiot, joten IT -infrastruktuurin monitorointi onnistuu kohteiden käyttöjärjestelmästä riippumatta.

Itselläni ei ollut oikeuksia itse monitoroinnin kohteille, joten agenttien asentaminen jäi muiden työntekijöiden vastuulle.

Zabbixilla pystyy myös monitoroimaan laitteita, joille ei pysty tai ei ole järkevää asentaa agenttia. Tämän voi toteuttaa esim. SNMP: n avulla. (Zabbix manual.)

4.2 Asennus virtuaalipalvelimelle

Zabbix asennettiin virtuaalipalvelimelle kolmannen osapuolen virtuaalikoneympäristöön.

Käyttöjärjestelmänä on Linux.

Palvelimen pystytys oli kolmannen osapuolen vastuulla ja se kesti valitettavan kauan (työt seisoivat lähes kuukauden), joten tästä muodostui pieni aikataulullinen ongelma. Lopulta palvelin saatiin pystyyn ja työt pääsivät jatkumaan.

Virtuaalipalvelinta käytin SSH -yhteyden avulla.

Zabbix serverin virtuaalipalvelimelle asennus toteutettiin Linux -komentojen avulla. Zabbix pyörii Apache -palvelinympäristössä. Apachea ei tarvitse kuitenkaan asentaa erikseen, vaan se tulee Zabbixin asennuksen yhteydessä palvelimelle.

4.2.1 Tiedonhallinta

Zabbix käyttää apache -palvelinta ja sen kanssa MySQL -tietokantaa. Proxionin muissa järjestelmissä on tietokantana käytössä PostgreSQL, jonka takia alkuperäinen suunnitelma oli käyttää sitä myös Zabbixin kanssa. Zabbix kyllä tukee PostgreSQL -tietokantaa, mutta sen integroiminen osoittautui kuitenkin liian monimutkaiseksi ja aikaavieväksi opinnäytetyön aikatauluun ja tavoitteisiin nähden, joten se jätettiin pois. MySQL on ylivoimaisesti yleisin Zabbixin kanssa käytetty tietokanta, ja se on myös itselleni paljon tutumpi kuin PostgreSQL, joten en halunnut ruveta tuhlaamaan opinnäytetyöaikaa turhaan uuden tekniikan opettelemiseen, varsinkin kun firma antoi vihreää valoa MySQL -tietokannalle.

4.2.2 Tietoliikenne ja tietoturva

Zabbixia varten tarvittiin palomuurista auki erilaisia portteja:

- SSH -portti 22
- HTTPS -portti 443
- Monitorointiliikenteeseen käytettävä portti 10051
- AD -autentikointiin käytettävä LDAP -portti 636

Zabbixia haluttiin päästä käyttämään ja hallinnoimaan myös Proxionin verkon ulkopuolelta internetistä, joten https -ja ssh -portit piti avata koko internetille.

Virtuaalipalvelin on erillisessä kolmannen osapuolen palveluntarjoajan ylläpidossa, joten heillä on omat palomuurit, jotka piti pyytää avaamaan yllämainittujen sääntöjen osalta. Tämä muodostui lieväksi ongelmaksi, sillä ko. palveluntarjoajalla tuppasi kestäämään välillä turhankin pitkään tukipyyntöjen ratkaisemisessa. Kaikki kuitenkin saatiin pelittämään lopulta.

Lisäksi palvelimella on oma paikallinen palomuuuri (UFW), jonka itse konfiguroin.

Paikallisen palomuurin portit avasin ufw allow -komennolla ja palomuurin käynnistin ufw enable -komennolla.

Palvelimelle asennettiin myös SSL -sertifikaatti, koska sinne syötetään salasanoja ja muita konfidentiaalisia tietoja, jotka on hyvä pitää suojassa.

4.2.3 Autentikointi

Konfiguroin Zabbixiin LDAP -autentikoinnin, eli siihen pystyy kirjautumaan Active Directory -tunnuksilla. LDAP -autentikoinnin pystyi helposti tekemään suoraan Zabbixin käyttöliittymästä käsin. LDAP -autentikointia varten vaadittiin seuraavat tiedot: Proxionin AD -palvelimen nimi ja portti, polku AD -palvelimen käyttäjiin, LDAP tilin etsimiseen käytettävä attribuutti (tässä tapauksessa sAMAccountname), LDAP -käyttäjien etsimiseen käytettävä tili ja sen salasana, sekä LDAP -autentikoinnin testaamiseen käytettävä tili (tässä tapauksessa omani). Allaolevassa kuvassa näkyy LDAP -autentikoinnin asetussivu. Proxionin AD -palvelimen osoitteen edessä on lyhenne LDAPS, joka tarkoittaa suojattua LDAP -yhteyttä. Tämä otettiin käyttöön suojaamaan AD -salasanoja ja muita tietoja, joiden salassapito olisi suotavaa.

KUVA 4. LDAP -autentikoinnin asetukset

4.2.4 Version päivittäminen

Zabbixista julkaistaan säännöllisesti uusia versioita, ja uusimmassa versiossa oleminen olisi suotavaa kokonaisuuden toimivuuden kannalta. Tämän takia täytyy pysyä kartalla uusimmasta versiosta, ja tarpeen tullen päivittää se uusimpaan. Päivittäminen on helppoa, tehdään vanhasta versiosta varmuuskopio, jonka jälkeen ladataan ja asennetaan uusi versio tilalle. Päivittämisen yhteydessä MySQL -kannan konfiguraatiot resetoituu ja ne pitää muistaa käydä vaihtamassa oikeiksi.

5 MONITOROINTI

5.1 Monitoroitavat kohteet ja virhetilanteet

Zabbixilla pystyy monitoroimaan kaikenlaisia asioita. Tämän opinnäytetyön tekohetkellä Proxionilla ei ole kuitenkaan tarvetta kovin laajalle monitoroinnille. Työn aihe on vain valita sopiva ohjelmisto ja demonstroida sen toimintaa, joten tähän työhön sisällytettiin vain kriittisimmät monitoroinnin kohteet EIS -infrastruktuurissa. Tärkeintä on saada tieto monitoroitavan kohteen hengissäolosta ja verkossa saatavuudesta, sekä lähettää sähköpostilla notifi kaatio kaikille asiaankuuluville henkilöille, mikäli vikatilanteita syntyy.

Zabbixissa monitoroitavilta kohteilta saatavat tilatiedot ovat luokiteltu sisältönsä ja kriittisyytensä mukaan kuuteen eri kategoriaan:

Not classified, Information, Warning, Average, High ja Disaster.

Näiden kategorioiden avulla voidaan määritellä, kuinka vakavista tilanteista halutaan saada asiaankuuluvalla henkilölle mahdollisimman nopeasti notifi kaatio, ja mistä puolestaan riittää olla vain tieto näkyvillä Zabbixissa. Tässä tapauksessa konfiguroin notifi kaation lähtemään aina, kun tilatieto on vähintään Warning -kategoriassa.

Virhetilanteen syntyessä kaikille asiaankuuluville henkilöille tulee Zabbixin etusivulle ilmoitus ko. virheestä. Sen lisäksi on mahdollista määrittää eri virhetilanteille **actioneita** eli tapahtumia, jotka tapahtuvat virhetilanteen sattuessa. Actioneita voivat olla esim. sähköpostin tai tekstiviestin eli notifi kaation lähetys asianomaisille henkilöille.

Opinnäytetyövaiheessa monitoroitavia kohteita on vain muutama, jatkossa määrä tulee kasvamaan.

5.2 Käyttäjänhallinta

Konfiguroin siis Zabbixin käyttämään LDAP -autentikointia. Käyttäjät täytyy kuitenkin luoda käsin Zabbixiin ja jos Zabbixiin asetettu käyttäjänimi löytyy myös AD: sta, pystyy ko. AD -tunnuksella kirjautumaan Zabbixiin. Zabbixissa on kolme eri käyttäjätyyppiä.

Ylin mahdollinen käyttäjätaso on **Super Admin**. Super Adminilla on oikeus käyttäjänhallintaan, monitoroitavien kohteiden hallintaan, palvelimen asetusten hallintaan, sekä luonnollisesti kaiken mahdollisen monitorointidatan katseluun ja hallinnoimiseen.

Toiseksi ylin taso on **Admin**. Adminilla on oikeus katsella monitorointidataa ja hallinnoida monitorointikohteita, joihin kyseisellä käyttäjällä on oikeus. Oletusarvoisesti Adminilla ei ole oikeuksia mihinkään kohteeseen, ne pitää Super Adminin toimesta lisätä.

Alin taso on peruskäyttäjä eli **User**. User pystyy ainoastaan katselemaan monitorointidataa, eli se on käytännössä Admin ilman hallinnoimisoikeuksia. Userille täytyy siis myös antaa oikeudet kohteisiin, joita hänen tarvitsee katsella.

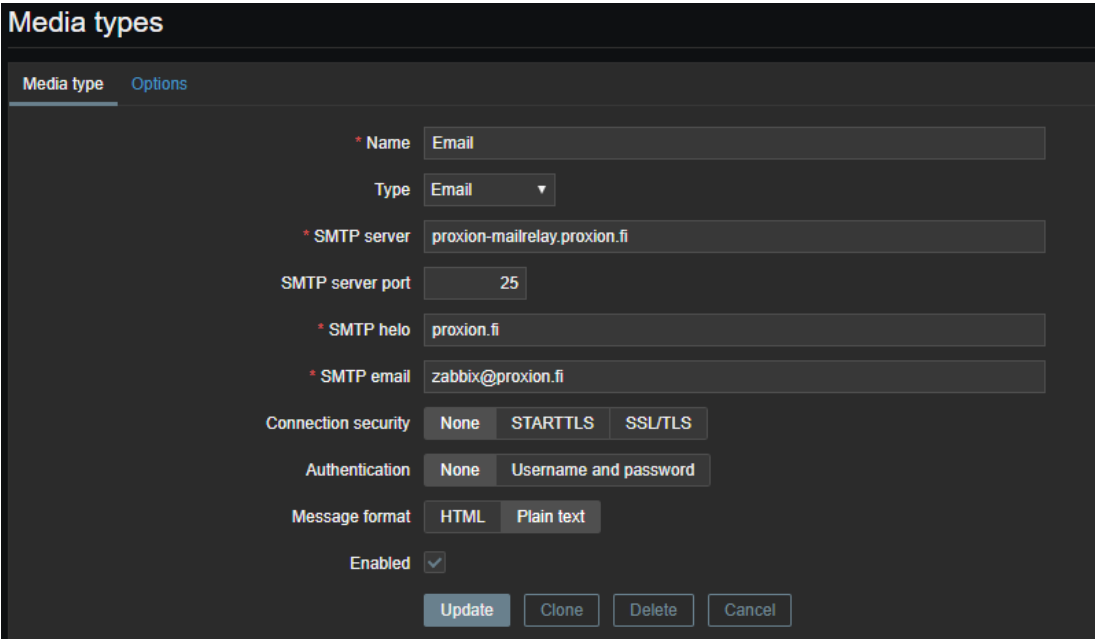
Proxionin tapauksessa Zabbix -tunnuksia tarvitsee tällä hetkellä vain ohjelmistopuolen työntekijät, käyttäjätasoina joko Super Admin tai User, välimallille eli Adminille ei toistaiseksi ole ollut tarvetta.

Zabbixissa on myös olemassa käyttäjäryhmiä eli **User groups**. Näiden avulla pystytään ryhmittelemään tietyille käyttäjäryhmälle oikeus tiettyihin monitorointikohteisiin, ettei tarvitse jokaiselle erikseen lisätä oikeuksia. Opinnäytetyön tekovaiheessa Zabbixin käyttäjiä on sen verran vähän ja monitorointi sen verran suppeaa, että tarvetta käyttäjäryhmille ei ole vielä ollut. Zabbixissa on oletuskäyttäjäryhmiä, esim. kaikki Adminit ja Super Adminit kuuluvat Zabbix Administrators -käyttäjäryhmään. (Zabbix, Manual.)

5.3 Sähköpostinotifikaatiot

Demonstroidakseni sähköpostinotifikaatioiden toimivuutta konfiguroin notifikaation tulemaan kaikkien Super Adminien sähköpostiin aina, kun jokin monitoroinnissa olevista kohteista on jonkinasteisessa virhetilassa. Tulevaisuudessa käyttäjämäärän ja monitorointikohteiden lisääntyessä konfiguroin notifikaatiot niin, että tietyt käyttäjät saavat vain heille kohdistettujen kohteiden virhetilanteiden notifikaatiot.

Konfiguroin Zabbixin lähettämään sähköpostia Proxionin oman postipalvelimen kautta. Kuten yllämainitsin, konfiguroin siis notifikaation lähtemään aina, kun kohteen tilatieto on vähintään Warning -kategoriassa.



The screenshot shows the 'Media types' configuration page in Zabbix. The 'Options' tab is selected. The configuration is for an 'Email' media type. The fields are as follows:

Field	Value
Name	Email
Type	Email
SMTP server	proxion-mailrelay.proxion.fi
SMTP server port	25
SMTP helo	proxion.fi
SMTP email	zabbix@proxion.fi
Connection security	None (selected), STARTTLS, SSL/TLS
Authentication	None (selected), Username and password
Message format	HTML (selected), Plain text
Enabled	<input checked="" type="checkbox"/>

At the bottom, there are four buttons: 'Update', 'Clone', 'Delete', and 'Cancel'.

KUVA 5. Sähköpostinotifikaatioiden SMTP -asetukset

6 YHTEENVETO

Opinnäytetyön tavoitteena oli vertailla eri monitorointiohjelmistoja, valita Proxionin vaatimuksiin sopivin, asentaa ja integroida se osaksi Proxionin IT -infrastruktuuria ja demonstroida sen toimintaa perustasolla.

Omasta ja Proxionin mielestä tavoitteisiin päästiin. Monitorointiohjelmistokandidaatteja oli monta, ja varsin monipuolisen vertailun jälkeen päädyttiin kaikin puolin sopivaan vaihtoehtoon, Zabbixiin. Zabbix on nyt asennettu omalle virtuaalipalvelimelleen ja se on toimiva osa Proxionin yhä kasvavaa IT -infrastruktuuria.

Aikataulullisesti projekti pysyi suhkot hyvin hallinnassa. Kapuloita rattaisiin laitto kolmannen osapuolen palveluntarjoaja, jonka vastuulla oli pystyttää virtuaalikone Zabbixia varten, sekä availla palomuuristaan portteja tarvittuihin suuntiin. Itsekin olisin voinut aika ajoin hieman tehokkaaminkin työskennellä ja koittaa minimoida ulkopuolisten viivästysten aiheuttamat haitat, tosin kolme viikkoa virtuaalipalvelimen odottelua ei ainakaan ylitöihin motivoi. Tämän työn motto, ja valitettavasti välillä myös teemakin, oli äitini opettama lausahdus: ”Minkä taakseen jättää, sen edestään löytää”.

Olosuhteisiin ja itsestäni riippumattomiin aikataulullisiin tekijöihin nähden opinnäytetyö on onnistunut hyvin. Itse aihe on itselleni ei niin mukavuusalueella ja alussa olikin hankala saada juonesta kiinni, mutta ajan myötä työ kävi koko ajan vaan mielenkiintoisemmaksi ja loppu onkin historiaa.

LÄHTEET

ICINGA. [www-sivu] [Viitattu 2019-01-25] Saatavilla:

<https://icinga.com/>

NAGIOS. [www-sivu] [Viitattu 2019-01-25] Saatavilla:

<https://www.nagios.org/>

OpenNMS. [www-sivu] [Viitattu 2019-01-25] Saatavilla:

<https://www.opennms.com/>

PANDORA FMS. [www-sivu] [Viitattu 2019-01-25] Saatavilla:

<http://pandorafms.org/>

PROMETHEUS. [www-sivu] [Viitattu 2019-01-25] Saatavilla:

<https://prometheus.io/>

ZABBIX. [www-sivu] [Viitattu 2019-01-25] Saatavilla:

<https://www.zabbix.com/>

ZABBIX. Manual. [www-sivu] [Viitattu 2019-05-02] Saatavilla:

<https://www.zabbix.com/documentation/4.2/manual>