VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Valtteri Kamppila

IT-INFRASTRUKTUURIN VALVONNAN KEHITTÄMINEN VALVONTATYÖKALUJEN AVULLA

Tekniikka
2019

VAASAN AMMATTIKORKEAKOULU
Tietotekniikka

TIIVISTELMÄ

Tekijä	Valtteri Kamppila
Opinnäytetyön nimi	IT-infrastruktuurin valvonnan kehittäminen valvontatyökalujen avulla
Vuosi	2019
Kieli	suomi
Sivumäärä	54
Ohjaaja	Ghodrat Moghadampour

Työn tarkoituksena oli kartoittaa nykyisen IT-infrastruktuurin verkkolaitteet ja palvelimet. Kerätyllä tiedolla on tarkoitus miettiä kuinka verkko- ja palvelinympäristöä olisi hyvä tarkkailla ja mitä nykyisessä ympäristössä tulisi päivittää.

Keskeistä, etenkin verkkoympäristön kartoituksessa, on verkon vikasietoisuus ja verkon topologiat. Myös VLAN konfiguraatiot verkkoympäristössä määrittävät tietoturvan tason, kuten myös palomuuri- ja verkkolaitteiden salaukset. Verkonvalvonnan kannalta tarkkailtavan datan laatu määrittää miten valvontatyökalua pystytään hyödyntämään. Työ toteutettiin kolmessa vaiheessa. Alussa suoritettiin infrastruktuurin kartoitus ja tämän jälkeen arvioitiin mahdolliset työkalut. Lopussa päädyttiin Icinga2-ohjelmaan, joka toteutettiin Linux-palvelimelle. Icinga2 on websovellus, joka hyödyntää Apache-webpalvelinta, tietokantaa ja REST APIa.

Verkkoympäristön ikä oli suurin syy, miksi nykyiset verkkolaitteet tulee päivittää. Myöskin verkkolaitteiden määrää voidaan karsia hankkimalla kytkimiä, joissa on enemmän portteja kuin nykyisissä kytkimissä. Valvontatyökalu osoittautui hyödylliseksi ja toimivaksi, mutta verkkoliikenteen laadun tarkkailu vaatii vielä muiden työkalujen tutkimista ja mahdollista käyttöönottoa.

Avainsanat	verkonvalvonta, IT-infrastruktuuri, verkkolaitteet, LAN ja tietoturva

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietotekniikka

ABSTRACT

Author	Valtteri Kamppila
Title	Developing Monitoring of IT Infrastructure with Monitoring Tools
Year	2019
Language	Finnish
Pages	54
Name of Supervisor	Ghodrat Moghadampour

The aim for the job is to map out the devices and servers in the current IT infrastructure. The need to update the infrastructure and the best method to monitor was determined by the data that was accumulated in this study.

The network topology and network fault tolerance are the key of the network part of the study. The password and VLAN configurations along with the firewall determine the safety of the local area network. The quality of the data determines how the monitoring tool can be used in the future. The work was done in three steps. The first step was to survey the infrastructure then evaluate and choose the possible tools. In the end the chosen program was Icinga2 and it was implemented on a Linux server. Icinga2 is a web application that uses the Apache webserver, database and REST API.

The age of the network devices is one major reason to update the devices. The number of devices can also be reduced when the future devices will have more interfaces than the current ones. The monitoring server proved to be useful but further studies will show if there is a need for other monitoring tools to ensure the required will be monitored.

Keywords monitoring, IT-infrastructure, network devices, LAN and security

SISÄLLYS

KUVIO- JA TAULUKKOLUETTELO

LYHENTEET

AD DC	Active Directory Domain Controller, Toimialueen kontrolleri
DNS	Domain Name Service, Nimipalvelin
WLAN	Wireless Local Area Network, Langaton lähiverkko
LAN	Local Area Network, Lähiverkko
VLAN	Virtual Local Area Network, Virtuaalilähiverkko
WAN	Wide Area Network, Laajaverkko
AP	Access Point, WLAN-tukiasema
FQDN	Fully-Qualified Domain Name, Palvelimen tai tietokoneen täydellinen nimi
DHCP	Dynamic Host Control Protocol, IP-osoitteiden dynaaminen jako
WSUS	Windows Server Update Services, Paikallinen palvelin, joka jakaa ja hyväksyy Windows-päivitykset
WDS	Windows Deployment Services, Ohjelmistojen jakaminen sisäverkossa
SNMP	Simple Network Management Protocol, Verkonhallintaprotokolla
SMTP	Simple Mail Transfer Protocol, TCP-protokolla sähköpostien välittämiseen
GVRP	GARP VLAN Registration Protocol, VLAN-hallintaprotokolla
SSH	Secure Shell, Tietoliikenteen salaus
REST API	Representational State Transfer Application Programming Interface, Ohjelmointirajapinta

GDPR General Data Protection Regulation, EU:n yleinen tietosuoja-asetus

RHEL Red Hat Enterprise Linux, Linux-jakelu

SOC Security Operations Center, kyberuhkia tarkkaileva palvelin/osasto

SIEM Security Incident and Event Management, kyberuhkien ja tapahtumien tarkkailuun

1 JOHDANTO

Tietoliikennetekniikan merkitys yrityksissä nykypäivänä on kriittinen. Muutama vuosikymmen taaksepäin, kun tietotekniikka ja internet alkoivat vasta yleistyä, yritykset tyytyivät lähinnä sähköpostien lähettämiseen. Palvelimet muistuttivat työasemia ja niitä oli harvassa. Tänä päivänä yrityksillä on joko omat pienet palvelinhuoneet tai salit, jos niitä ei ole, ovat ne ulkoistettu ulkopuolisille tekijöille. Palvelimia on useita, koska useat järjestelmät niitä vaativat. Toiminnanohjausjärjestelmät, kuten ERP tai tuotekehityksen järjestelmät, kuten PDM ja talouden ohjelmistot (osto- ja laskureskontra) hakevat lisenssinsä palvelimilta. Windows- tai Linux-palvelimet (AD DC, DNS) mahdollistavat edellä mainittujen ohjelmistojen käytön.

Yritysten järjestelmät ovat tiukasti kiinni toisissaan. Tavaran tuonti ja vienti merkitään ERP, mikäli ERP-järjestelmä on alhaalla tai verkkoliikenne palvelimelle on poikki, hidastaa se yrityksen toimintaa. Mikäli suunnitteluohjelma ei saa lisenssiä palvelimelta tai tietokoneella, on jokin ajurikonflikti, ja työntekijä ei saa suunniteltua tuotetta tai tuotteita.

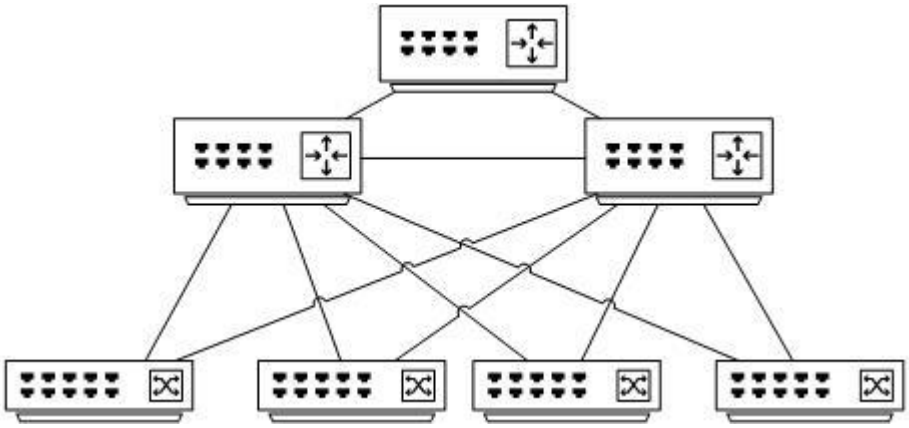
IT-infrastruktuurin valvonta on elintärkeää yrityksen tuottavuuden kannalta. Tämän opinnäytetyön tarkoituksena on saada niin palvelimet kuin tietoliikenneverkot valvonnan alle niin, että mahdolliset virhetilanteet voitaisiin ennakoida ja täten estää ennen kuin se vaikuttaa järjestelmiin ja liiketoimintaan. Erilaisia tietoliikenneverkkoja valvovia palvelimia on saatavana valmiina ja näihin palvelimiin on mahdollisuutena saada myös moduuli, jolla saadaan kerättyä palvelimilta virhelokeja.

Tämän työn aikana tulisi saada uusittua T-Drill Oy:n dokumentaatiot nykyisestä sisäverkosta sekä palvelimista, verkon kytkimet ja niiden tietoliikenteen mahdolliset häiriöt valvonnan alaisiksi sekä palvelimet, jotka ovat VMwaren ESXi alustan päällä olevia virtuaalipalvelimia.

2 VERKKOARKKITEHTUUREJA

Erilaisia verkkoarkkitehtuureja ja topologioita on useita. Verkkoa suunnitellessa tulee huomioida millaiseen käyttöön verkko tulee. Esimerkiksi verkon vikasietoisuus (Fault tolerance, Network redundancy) määritetään jo verkon suunnitteluvaiheessa ja on erittäin tärkeä ominaisuus, mikäli verkossa ilmenee palveluita, jotka eivät saa missään tapauksessa pudota pois verkosta (Downtime, Network outage). Kriittiset palvelut, kuten verkkokaupat ja muut reaaliaikaisesti ihmisten tietoja käsittelevät palvelut, tulee sijaita vikasietoisessa verkossa.

Alla olevassa kuviossa on esimerkki vikasietoisuudesta. Verkossa on kolme reititintä ja neljä kytkintä, joista jokainen on liitetty toisiinsa. Mikäli yksi reititin putoaa pois verkosta, pysyy verkko silti ylhäällä. Näin minimoidaan verkkokatkon riski ja pidetään kriittiset palvelut pystyssä laiterikon sattuessa. /1/



Kuvio 1. Vikasietoisuus lähiverkossa

2.1 Fyysiset verkkotopologiat

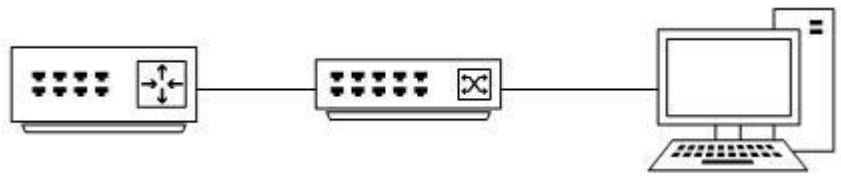
Fyysiset verkkotopologiat määrittyvät laitteiden sijoittelun mukaan. Topologiassa laite voi olla joko solmukohta (Node), päätelaite/päätepiste (Endpoint) tai linkki (Connections/links). Erilaisia topologioita on useita ja ne eritellään seuraavissa kappaleissa. Yleisesti verkot ovat näiden topologioiden yhdistelmiä. Solmukohtana tai päätepisteenä voi toimia esimerkiksi reititin, kytkin tai tietokone.

Teoreettisesti verkko olisi helppo rakentaa solmukohdasta solmukohtaan luoden näin pisteestä pisteeseen (point-to-point) verkon, mutta se on erittäin epäkäytännöllinen. Suuressa verkossa tämä vaatisi liian suuren määrän jatkuvia yhteyksiä. IP-verkoissa toimiva pakettikytkentä (packet switcing) auttaa tässä, näin saadaan viestit kulkemaan myös point-to-point verkoissa hajottamalla viestin pienempiin osiin. /3, s.10/

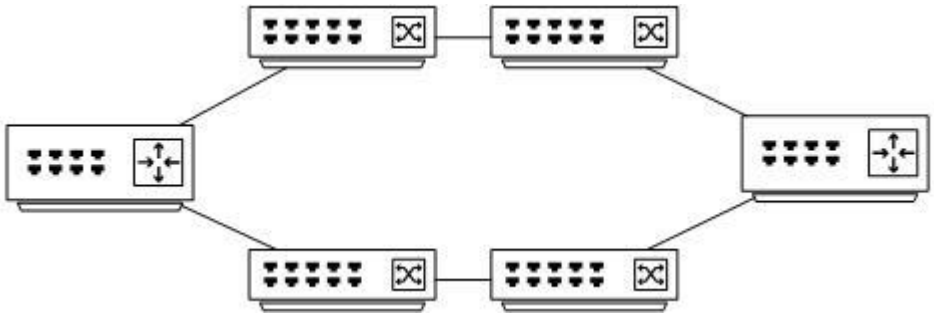
2.1.1 Väylätopologia (Bus)

Väylä (**Kuvio 2.**) on yleinen topologia, jossa on yhdistettynä kaksi tai useampi laite tai verkko. Väylässä viesti kulkee ketjun läpi, kunnes se saavuttaa halutun määränpäänsä. Väyläverkko, joka yhdistää useita aliverkkoja tai lähiverkkoja (Backbone network) voi olla erittäin tehokas tapa siirtää dataa, mutta se ei ole joustava järjestelmä.

Mikäli järjestelmään halutaan joustavuutta, saadaan sitä, jos lineaarinen väylä (linear bus system) muutetaan jakelumuotoiseksi (distributed bus system, **Kuvio 3.**) Tällöin saadaan uusia oksia (branch), jotka yhdistävät verkkoon uusia solmukohtia. /2, 3, s. 10/



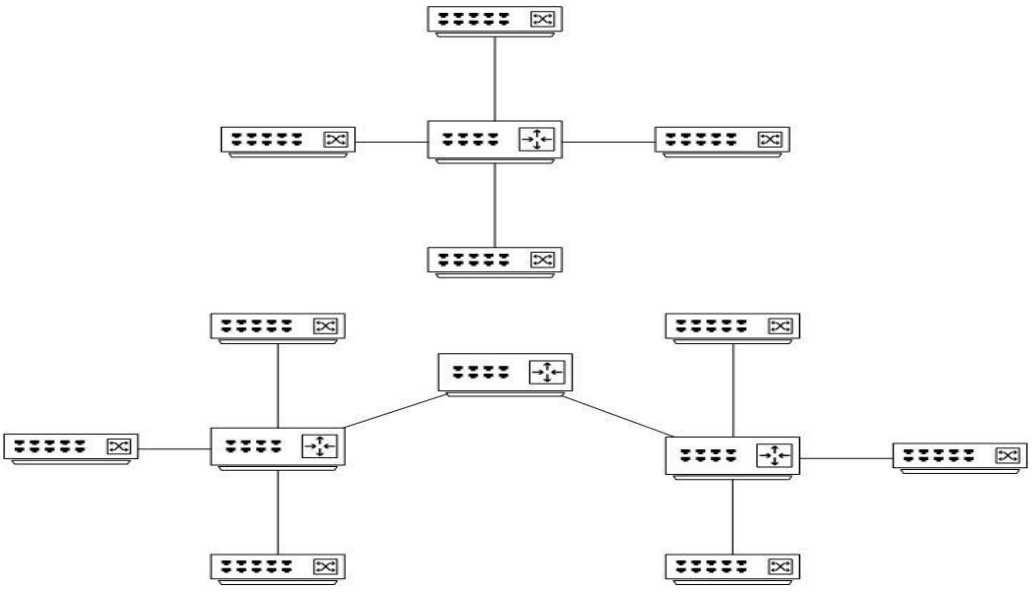
Kuvio 2. Esimerkki väylätopologiasta



Kuvio 3. Esimerkki jakeluväylätopologiasta

2.1.2 Tähtitopologia (Star)

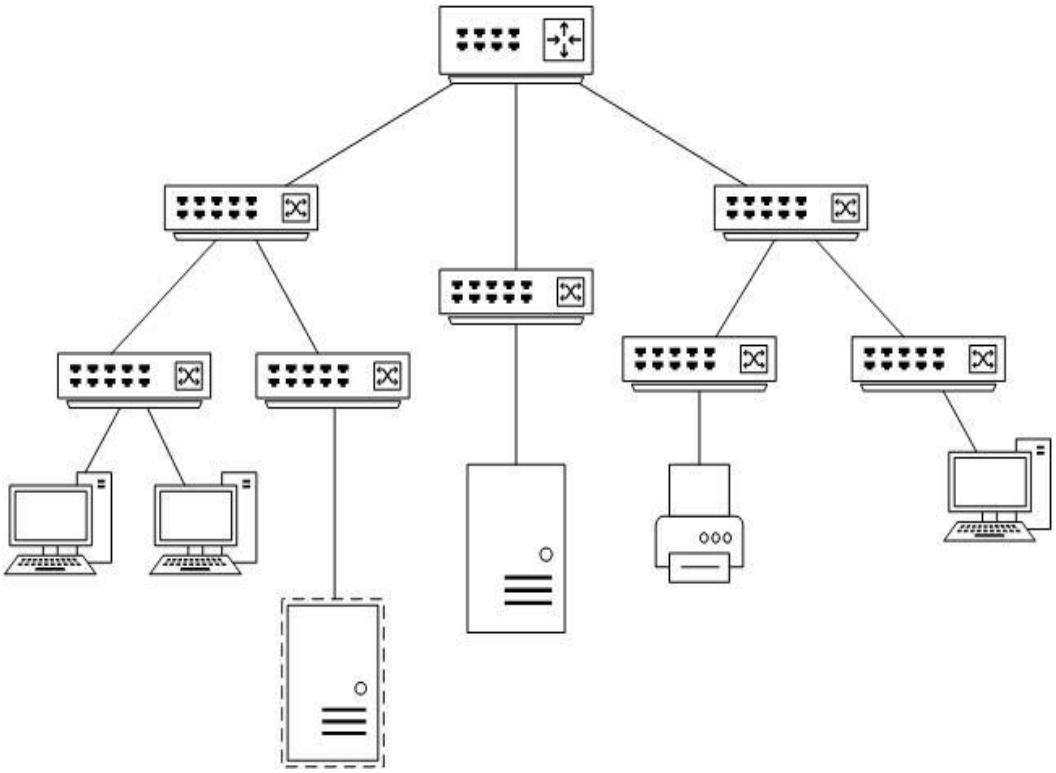
Tähtitopologia (**Kuvio 4.**) on erittäin yleinen topologia. Tähtitopologiassa pisteestä pisteeseen (point-to-point) yhteydet kiertävät keskellä olevan keskitetyn solmukohdan kautta. Topologiassa on mahdollista yhdistää useita tähtimalleja luoden joko jatketun tähtitopologian (Extended star topology) tai jakelupisteen kolmen tai useamman välille (Distributed star topology). /2, 3, s. 11/



Kuvio 4. Esimerkki tähdestä- ja laajennetusta tähdestä

2.1.3 Puutopologia (Tree)

Puutopologiassa (**Kuvio 5.**) on vahva hierarkia, jossa jokainen taso laskeutuu alaspäin seuraavalle laitteelle. Puutopologian erottaa tähtitopologiasta se, että siinä on kolme kerrosta eikä kaksi. Solmukohtien määrä, jotka on liitetty pääsolmukohtaan, kutsutaan fanout tai branching factoriksi, mikäli solmukohtaan on kytketty kaksi tai enemmän laitteita. Mikäli solmukohtaan on liitetty vain yksi laite, on kyseessä lineaarinen topologia eikä puutopologia. /2, 3, s. 15/



Kuvio 5. Esimerkki puutopologiasta

2.1.4 Mesh- ja hybriditopologiat

Mesh -topologiassa kaikki laitteet on kytketty toisiinsa suoralla yhteydellä. Topologiaa käytetään yleisimmin WLAN –verkoissa. WAN -verkoissa, kuten internetissä, käytetään myös Mesh -topologiaa.

Hybriditopologioita ovat edellä mainittujen ja muiden topologioiden yhdistelmiä. Kuten jo aiemmin kappaleen alustuksessa viitattiin verkot ovat yleisesti aina erilaisten topologioiden yhdistelmiä. Hybriditopologia luo joustavuutta verkon suunnitteluun. /2, 3, s. 16/

Taulukko 1. IEEE 802- standardit lähiverkossa

Standardi	Kuvaus
IEEE 802.1	LAN (Local area network) ja MAN (Metropolitan area network) standardi, joka käsittää OSI -mallista fyysisen ja verkkokerroksen.
IEEE 802.3	Ethernet- standardi, tukee IEEE 802.1 -standardia, määrittää myös esimerkiksi CSMA (Carrier-sende multiple access with collison detection).
IEEE 802.11	WLAN- standardi osana LAN- standardia, joka määrittää WLAN verkkojen MAC- ja fyysisen kerroksen, sekä taajuusalueet.

3 NYKYINEN IT-INFRASTRUKTUURI

Aiheena työ on erittäin laaja, tämän takia ympäristö luodaan aluksi vain testiympäristönä. Tavoitteena on saada aluksi vain kriittisimmät toiminnot valvonnan piiriin.

3.1 Kokonaiskuva

Laitteiden määrä on suhteellisen suuri yrityksen kokoon nähden. Infrastruktuuri koostuu kuudesta kytkimestä, joista neljä on sijoitettu palvelinhuoneeseen, yksi on sijoitettu rakennuksen tehdastilojen yhteyteen ja yksi kytkin sijaitse toisessa päässä yrityksen tiloja. Oma kytkin löytyy myös koneistamolta, joka sijaitsee toisella paikkakunnalla. Rakennuksessa on koko rakennuksen kattava WLAN- yhteys, niin sisäverkkoon kuin vierailijoille tarkoitettuun Visitor -verkkoon.

Huomioitavia suuria palvelimia yrityksessä on tuotehallinnan palvelin, johon on integroitu myös kahden suunnitteluohjelman lisenssimanagerit, ERP-järjestelmän palvelin, talouden hallintajärjestelmien palvelimia on kolme sekä tietysti Windows DC:tä kaksi kappaletta. DC:llä on myös DNS- sekä DHCP- palvelimet. Yrityksellä on myös WSUS-, WDS- ja tiedostopalvelin. Tällä hetkellä testikäytössä on myös QNAP NAS -palvelin ja Linux- palvelin, joka hyödyntää Docker- virtualisointia pyörittääkseen XIBO Info-TV järjestelmää.

Nykyisen infrastruktuurin huomioon ottaen, on valvonnalle tarvetta. Yrityksen IT-osasto koostuu kolmesta työntekijästä, joten valvonnan keskittäminen ja sen esille tuominen helpottaa arkea ja auttaa mahdollisten ongelmien ennalta ehkäisyä ja nopeuttaa ongelmien ratkaisua, täten edesauttaen työn tehokkuutta muilla osastoilla.

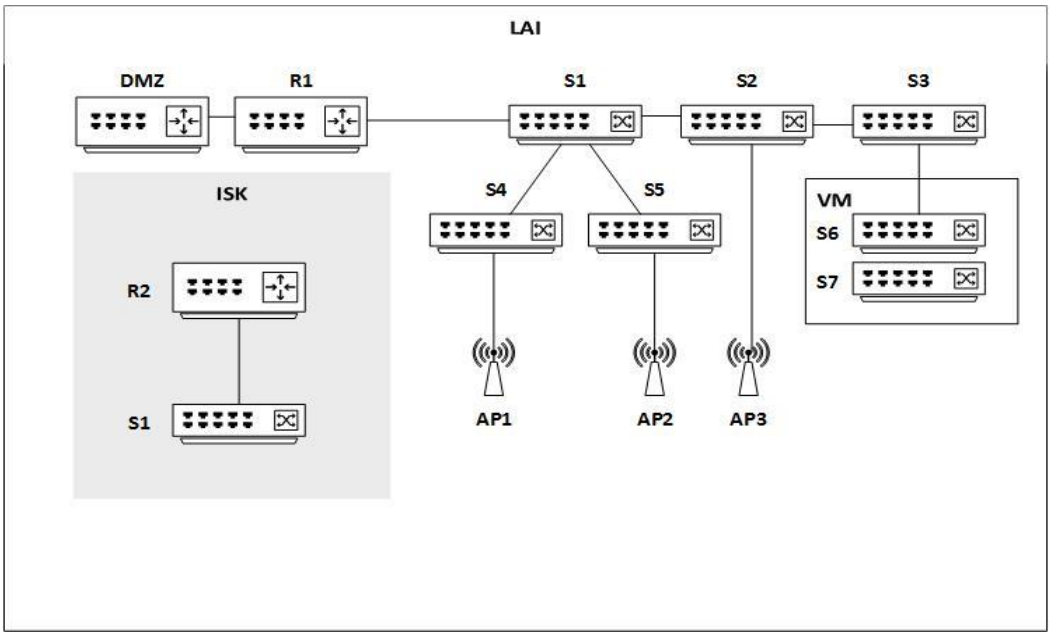
Testiympäristö, jota tässä työssä käytetään, tulee koostumaan yrityksen reitittimistä, kytkimistä ja palvelininfrastruktuurista, joista yhteen palvelimeen asennetaan keskitetty lokipalvelin.

3.2 Lähiverkko

Yrityksen lähiverkkoon kuuluu kaksi lähiverkkokokonaisuutta, toinen on Laihialla sijaitseva päätoimipiste sekä Isossakyrössä sijaitseva koneistamo. Kytkimiä yrityksen verkossa on tällä hetkellä kahdeksan ja reitittimiä kolme. Yksi reitittimistä erottaa lähiverkon ja DMZ:n (demilitarized zone). Yrityksellä on suuri määrä virtualisoituja palvelimia, joten levyjärjestelmät ja palvelimet sijaitsevat kahden kytkimen takana (**Kuvio 6.**)

VLANin kautta verkosta löytyy erilliset verkot vierailijoille (Visitor). Tämä vierailijaverkko on WLAN- yhteys, ja kyseiset VLANit on liitetty SOPHOS WLAN -tukiasemiin.

SOPHOS AP:t on asennettu Laihian verkkoon, mutta Isostakyröstä ne vielä puuttuvat. Työn aikana ne tullaan asentamaan myös Isoonkyröön.

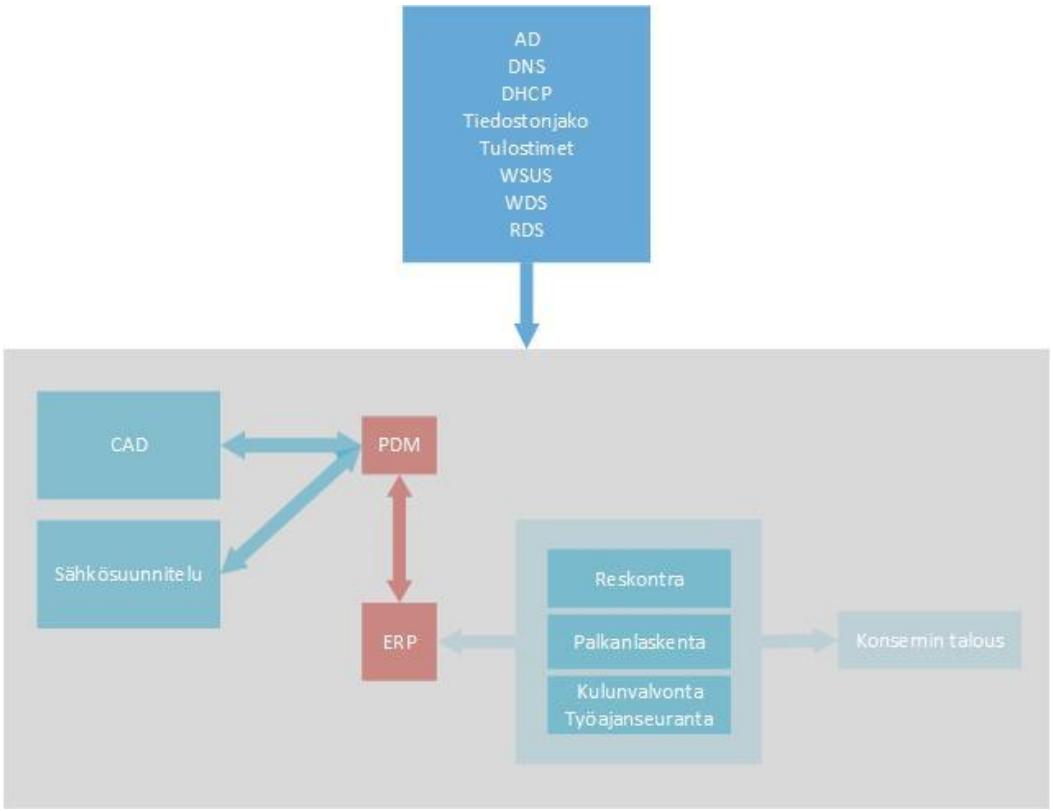


Kuvio 6. Nykyisen verkon kuvaus

3.3 Palvelimet ja palvelut

Yrityksen palvelimet ovat kaikki virtuaalisia. Palvelimet pyörivät VMware ESXi-alustojen päällä. Virtuaalipalvelimien hallinta suoritetaan selaimen kautta, josta palvelimia ja työasemia voi luoda levyjärjestelmälle.

Vaikkakin T-Drill Oy on keskikokoinen yritys, on palvelinten määrä suhteellisen suuri. Virtuaalipalvelimia on kaksikymmentä, esim. kaksi AD DC:tä, kaksi tuotehallintajärjestelmän palvelinta, toinen on testipalvelin ja toinen tuotantokäytössä oleva, ERP -palvelin, sähkösuunnitteluohjelman palvelin, joka toimii myös ohjelmalisenssimanagerina, kulunvalvonnan palvelin, WSUS -palvelin, Info-TV-järjestelmän palvelin, Isonkyrön poravarastoa tarkkaileva palvelin ja tiedostojakopalvelin.



Kuvio 7. Palvelinten ja palvelujen kuvaus

3.4 Riskianalyysi

Jokaisessa IT-ympäristössä tulisi olla kartoitettuna riskianalyysi mahdollisten ongelmatilanteiden varalta. Nykyisessä ympäristössä on määritelty riskit, joita palvelut tai infrastruktuuri voi kohdata, esimerkiksi levyjärjestelmän rikkoutuminen, verkon äkillinen kaatuminen tai jonkin kriittisen palvelun korruptoituminen tai muu vastaava vika.

Esimerkkinä jonkin kriittisen datan korruptoituminen tai katoaminen voi johtaa siihen, että tilanne saadaan ns. normalisoitua noin kahden päivän kuluessa tapahtumasta. Jokaiselle tapahtumalle on annettu jokin päiväarvio, jonka perusteella voidaan analysoida, kuinka paljon ongelma saattaa aiheuttaa kustannuksia yritykselle. Arvio ei itsessään ole kovin yksinkertainen, koska jokainen tapaus on aina jollakin tapaa ainutlaatuinen.

Pahimmassa tapauksessa kriittisimmät palvelut, kuten PDM ja ERP voivat kaatua. Tämä aiheuttaa kustannuksia arviolta 100 €/tunti per käyttäjä. Järjestelmien mahdollisen kaatumisen aikana työntekijät pystyvät vain osittain jatkamaan työskentelyään, joten kriittisten palveluiden vaikutus yrityksen liiketoiminnalle on erittäin suuri. Muista palveluista kriittisimmiksi voi luokitella AD, DNS ja DHCP, joiden vaikutus kuluissa on arviolta 50 €/tunti per käyttäjä.

Erilaiset haittaohjelmat ja tietojenkalastelu ovat nousseet myös suuriksi uhkiksi nykyaikana. Esimerkiksi erilaiset kiristysohjelmat (ransomware) ovat uhka yritystoiminnalle. Mikäli yrityksen dataa saadaan kryptattua, täytyy olla mahdollista palauttaa tiedot varmuuskopioiden avulla. Tämän takia käytössä on niin paikallinen (on-site) kuin myös toisessa paikassa (off-site) olevat varmuuskopiot mahdollisen tietojen katoamisen varalta.

4 TYÖN ALOITTAMINEN

Työn alkuvaiheessa on tarkoitus testata ja ottaa käyttöön uusi HPE OfficeConnect 1920S -kytkin. Tätä kytkintä tullaan käyttämään perustettavan lokipalvelintestauksessa.

Työn seuraavassa vaiheessa luodaan Linux -palvelin, jonka päällä pyörii Icinga2. Icinga2 on johdettu (fork) versio Nagios -järjestelmästä. Muita vaihtoehtoja olisi ollut esimerkiksi Zabbix, Nagios, Observium ja Cacti, mutta lopulta päädyimme Icingaan. Icinga2 on monitorointityökalu, jonka avulla voidaan tarkkailla esimerkiksi HTTP-, SMTP-, SNMP- ja SSH-yhteyksiä, tulostimia, reitittimiä tai kytkimiä. Palvelimen testivaiheessa monitoroinnin alle kuuluvat uusi HPE OfficeConnect- kytkin, sekä vanha varmuuskopiointipalvelin.

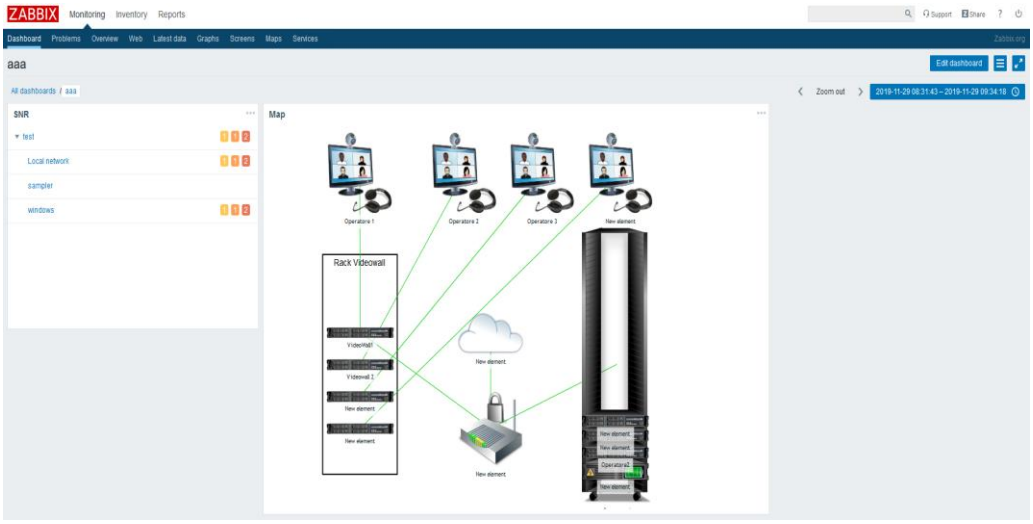
4.1 Zabbix

Zabbix on avoimen lähdekoodin järjestelmä samoin kuin Icinga. Zabbixin on kehittänyt Alexei Vladishev ja se on tällä hetkellä tuettu Zabbix SIA:n toimesta. Zabbix tarjoaa myös kaupallisesti tuettua versiota. Zabbix on lisensoitu GPL (GNU Public Lisence) alle. Zabbix on tarkoitettu verkon ja palvelinten monitorointiin ja sen notifikaatiojärjestelmä antaa käyttäjän luoda sähköpostiin hälytyksiä erilaisista tapahtumista ja varoituksista. Zabbix-versio, jota harkittiin, oli versio 4.2 LTS. LTS eli Long Term Support on tuettu pidemmän aikaa kuin muut versiot. Zabbix-asennusdokumentaatiossa on painotettu myös RHEL/Cent OS-asennusta, kuten muissakin monitorointiohjelmissa. Tämä myös painotti palvelimen käyttöjärjestelmän valinnaksi Cent OS. /4/

Zabbixin toimintaperiaate on sama kuin Icinga2. Palvelin koostuu kolmesta komponentista, Zabbix-palvelusta, web-palvelimesta ja tietokannasta. Zabbix agentti taas asennetaan paikallisesti, joko palvelimelle tai PC:lle. Agentti kerää dataa ja lähettää ne Zabbix -palvelimelle.

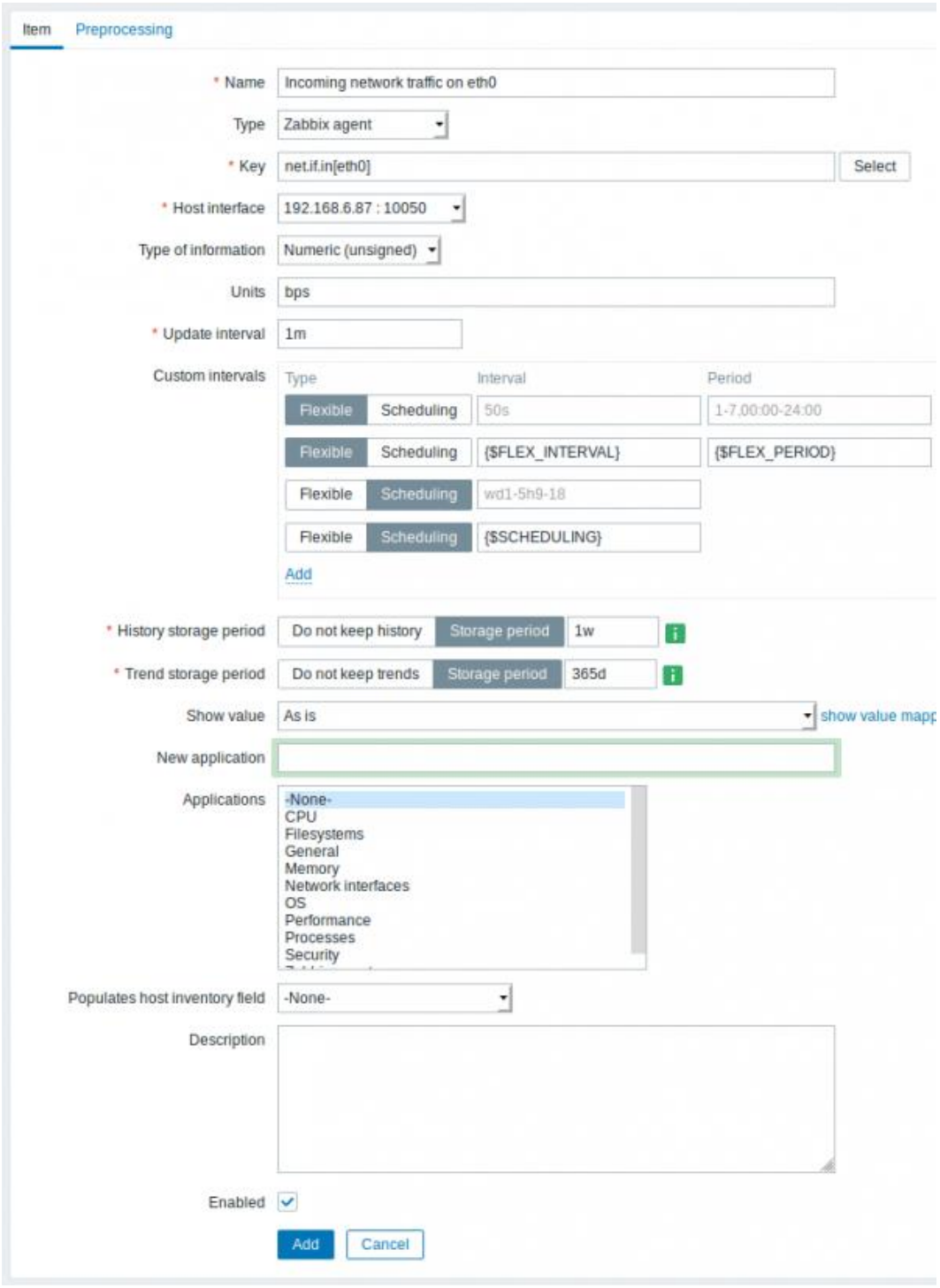
Zabbix-verkkokäyttöliittymä oli hyvin selkeä. Aloitussivu (Dashboard) tarjosi niin graafeja kuin kuvia sekä muuta dataa. Käyttöliittymästä sai avattua myös näky-

män kytkettyihin laitteisiin, mutta uuden palvelimen/työaseman lisäystä ei demossa saanut kokeiltua. Raportit sai jaoteltua päivien ja kuukausien mukaan ja yleisesti datan suodattaminen oli helppoa ja hyvin jäsenneltyä.

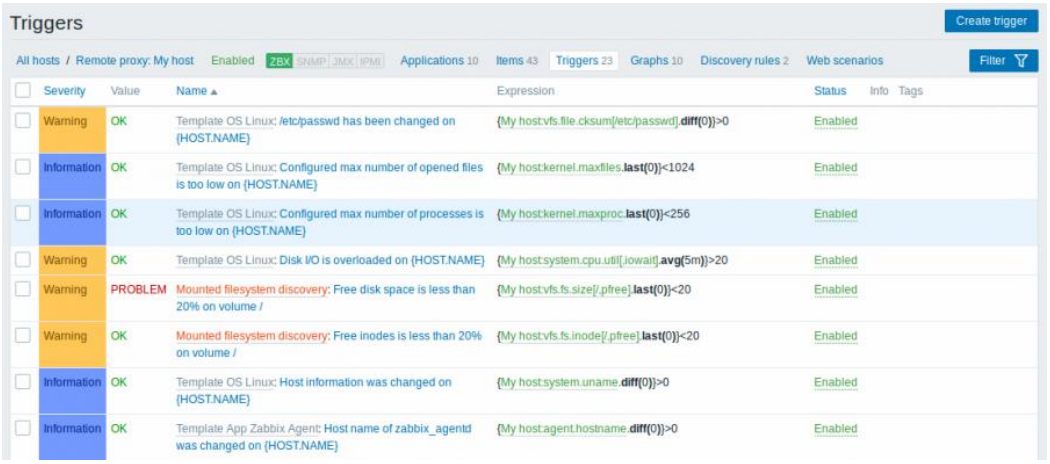


Kuvio 8. Zabbix-demo Dashboard

Dokumentaatiosta löytyy suorat ohjeistukset uusien laitteiden ja monitoroitavien kohteiden lisäämiselle. Websovelluksen käyttöliittymän kautta on helppo lisätä uusia laitteita ja monitoroitavia kohteita (Items). Erilaisia kohteita lisätessä, kannattavaa on huomioida dokumentaatiossa annetut muuttuja nimet sekä määritetyt tietokantarajoitteet (**Kuvio 9.**)

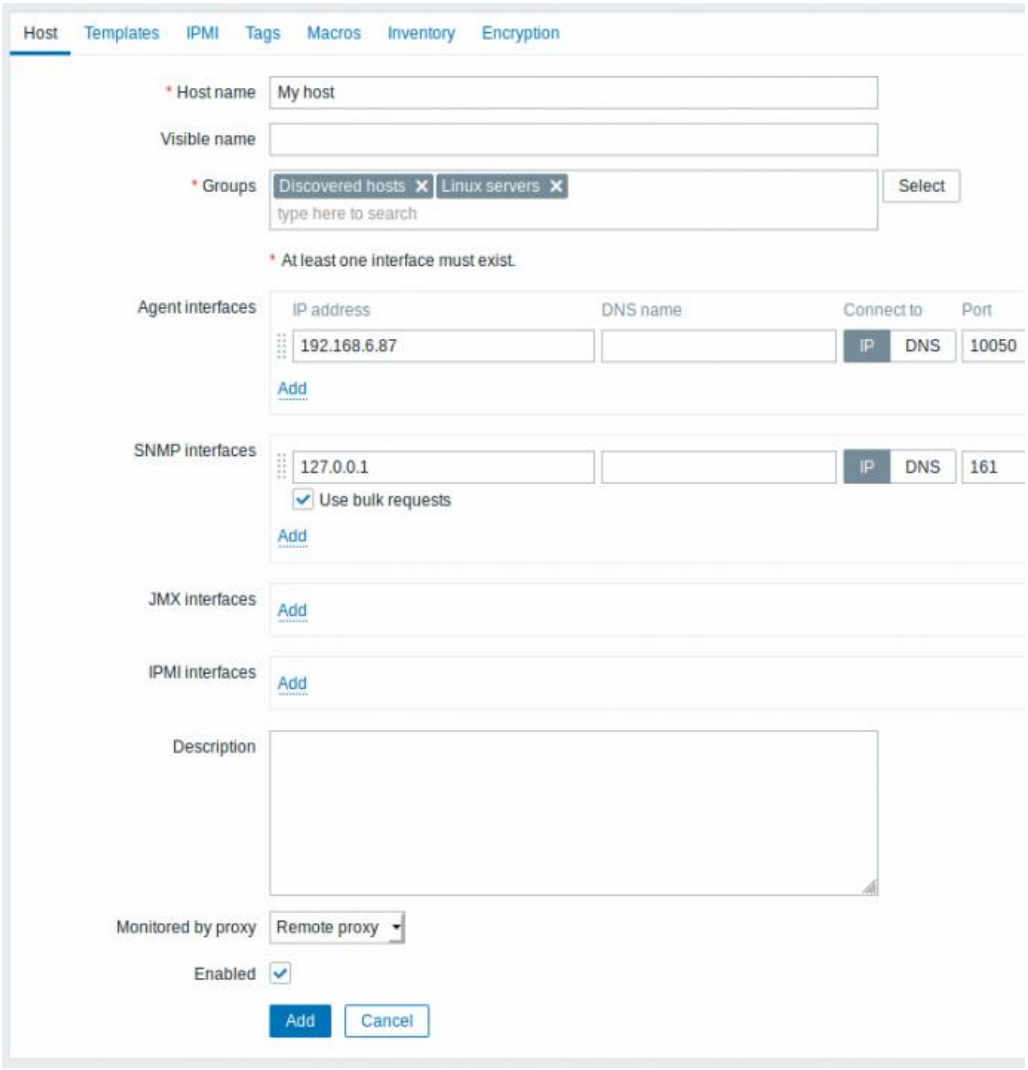


Kuvio 9. Esimerkkikuva monitoroitavien kohteiden lisäämisestä



Kuvio 10. Esimerkkikuva varoituksista Zabbix-dokumentaatiosta

Kuviossa 10 oleva esimerkki varoituksista ja huomautuksista oli valintaprosessin aikana huomioitu ja sitä vertailtiin muiden järjestelmien vastaaviin raportointitauluihin. Vertailussa huomattiin, että vaikka SNMP Trapit ja halutut monitoroitavat kohteet voidaan itse määrittää, on raportointitaulu selkeämpi Icingassa.



Kuvio 11. Esimerkkikuva laitteen määrittämisestä Zabbix-dokumentaatiosta

Visuaalisesti ja käyttöliittymän kannalta Zabbix vaikuttaa hyvältä. Ohjelman dokumentaatio oli melko suoraviivainen ja dokumentaatiossa selitettiin toiminnot, niin pakolliset kuin valinnaiset. Zabbix tulee asentaa suoraan lähdekoodista, kun taas Icingalla on oma hakemisto (repository). Suurimpana huolenaiheena oli mahdollinen ylläpidollinen kuorma. Zabbix, vaikkakin tunnettu kuten Nagios ja Icinga, oli huomattavasti vähemmän keskusteltu monitorointiohjelma verkossa. Tämä myös pudotti sen Icingan taakse vertailussa, koska oli helpompi hakea ratkaisuja Nagios pohjaiseen järjestelmään verkosta. Zabbix soveltuu sekä suurille että pienille ympäristöille.

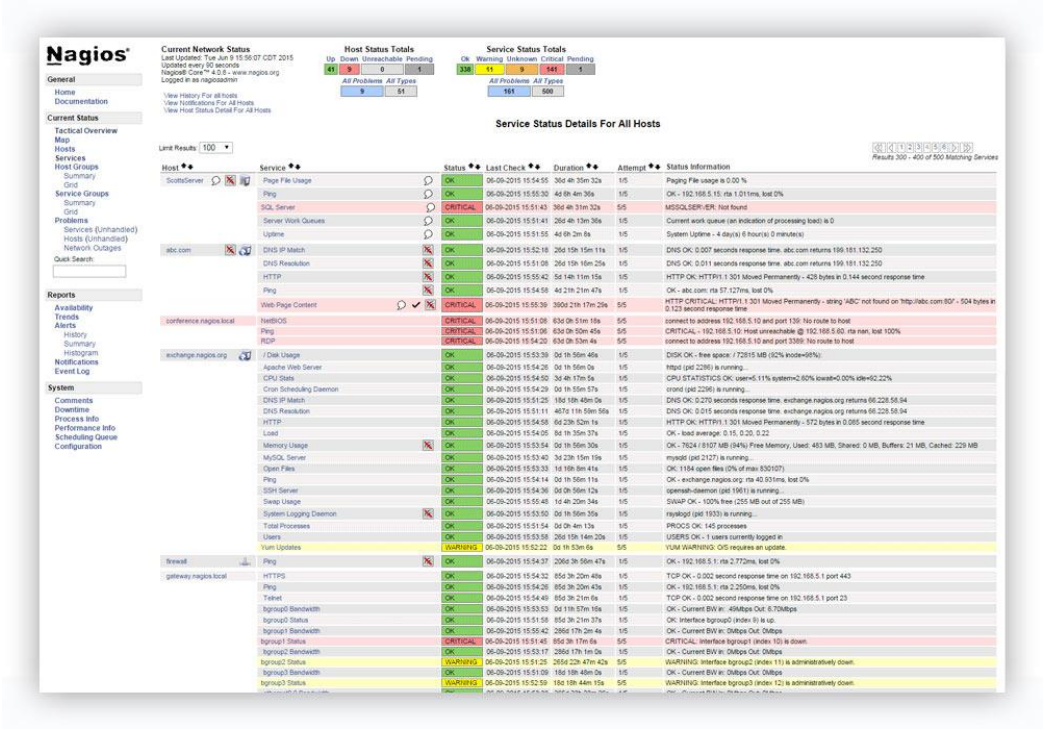
4.2 Nagios

Nagios oli kartoituksen alussa jo tuttu järjestelmä ja se esiintyi useissa vertailuissa. Nagios itsessään tarjoaa palveluna kolmea eri vaihtoehtoa; Nagios XI, joka tarjoaa kokonaisvaltaisen IT-infrastruktuurin valvonnan, Nagios Log Server, jonne voidaan kerätä lokidata keskitetysti ja Nagios Fusion, joka toimii taas suurempien klustereiden hallintaan. Avoimen lähdekoodin malli on nimeltään Nagios Core.

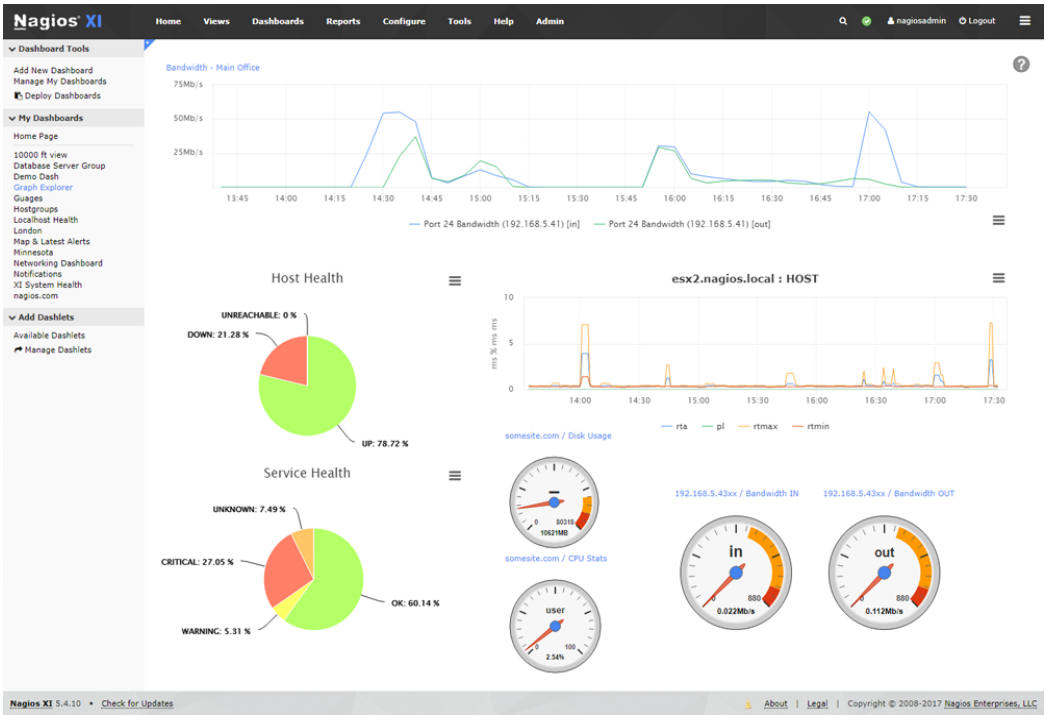
Nagios Core, kuten Icinga ja Zabbix, vaativat Unix -pohjaisen palvelimen toimiakseen. Nagios on C-pohjainen ohjelma,mikäli sen haluaa rakentaa suoraan lähdekoodista, vaaditaan gcc kääntäjäksi. Asennusprosessi on samankaltainen kuin Icingassa ja Zabbixissa. Kaikissa kolmessa on kolme peruspilaria: palvelin, web -palvelin ja tietokanta. /5/

Nagioksesta löytyy, kuten muistakin, onlinedemo sen palveluille. Nagios Core on käyttöliittymältään hyvin yksinkertainen ja samankaltainen kun esimerkiksi Zabbix. Kahdesta valikkopaneelista pystytään hakemaan tietoa eri valikoiden kautta. Nagioksen huonoksi puoleksi osoittautui dokumentaation suppeus. Dokumentaatio on kovin vaikealukuista ja esimerkiksi Zabbix ja Icinga ovat hoitaneet dokumentoinnin paremmin kuin Nagios.

Nagios, kaikkine lisäosineen on kuitenkin hyvin vahva paketti ja sopii erilaisiin monitorointitehtäviin hyvin. Sen etuna on myös se, että se on käyttäjän täysin muokattavissa. Dokumentaation esillepano ja yleisesti esilletuonti oli ainoa suuri miinus, jonka sille voi antaa.



Kuvio 12. Esimerkkikuva Nagios Core-käyttöliittymästä



Kuvio 13. Esimerkkikuva Nagios XI-maksullisesta versiosta

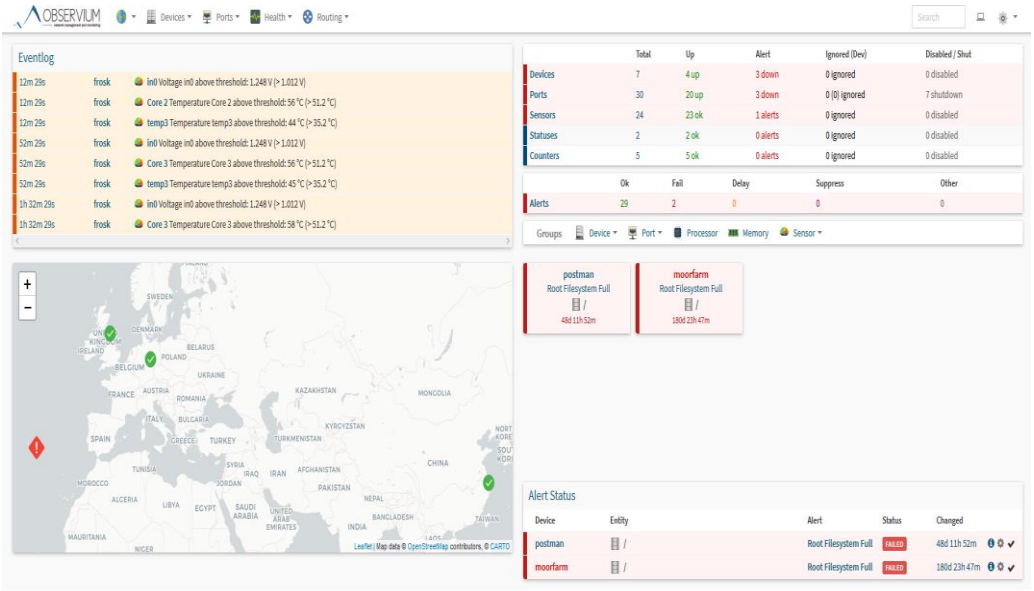
4.3 Observium

Observium on verkkomonitorointiohjelma, joka pystyy automaattisesti auto-discovery ominaisuuden avulla monitoroimaan useita laitteita. Observiumin sivuston mukaan se tukee esimerkiksi seuraavia järjestelmiä: Cisco, Windows, Linux, HP, Juniper, Dell ja FreeBSD. Observiumia löytyy kolmena versiona; Community, Professional ja Enterprise. Community on ilmainen versio karsituilla ominaisuuksilla. /6/

Observium pudotettiin vertailusta hyvin aikaisessa vaiheessa, koska sen Community-versio oli erittäin karsittu. Community-versiolla olisi voinut monitoroida verkkolaitteita, mutta esimerkiksi web frontendin REST API on vain maksullisessa versiossa ja erilaiset tilatiedot ja varoitukset kuuluivat maksulliseen versioon.

Observium keskittyy lähinnä verkon ja verkkolaitteiden tarkkailuun, missä taas esimerkiksi Zabbix voi monitoroida myös palveluita ja sovelluksia. Käyttöliittymältään Observium on erittäin siisti. Dokumentaatio on helposti löydettävissä ja ohjeet ovat suoraviivaisia. Observiumilla, kuten Icingalla, on omat hakemistot (repository), joten sitä ei tarvitse asentaa suoraan lähdekoodista.

Observiumin suurimmaksi ongelmaksi koitui sen karsitut ominaisuudet. Communityversiosta puuttuu lähes kaikki ominaisuudet ja se ei soveltunut työn vaatimaan käyttötarkoitukseen.



Kuvio 14. Observium demo

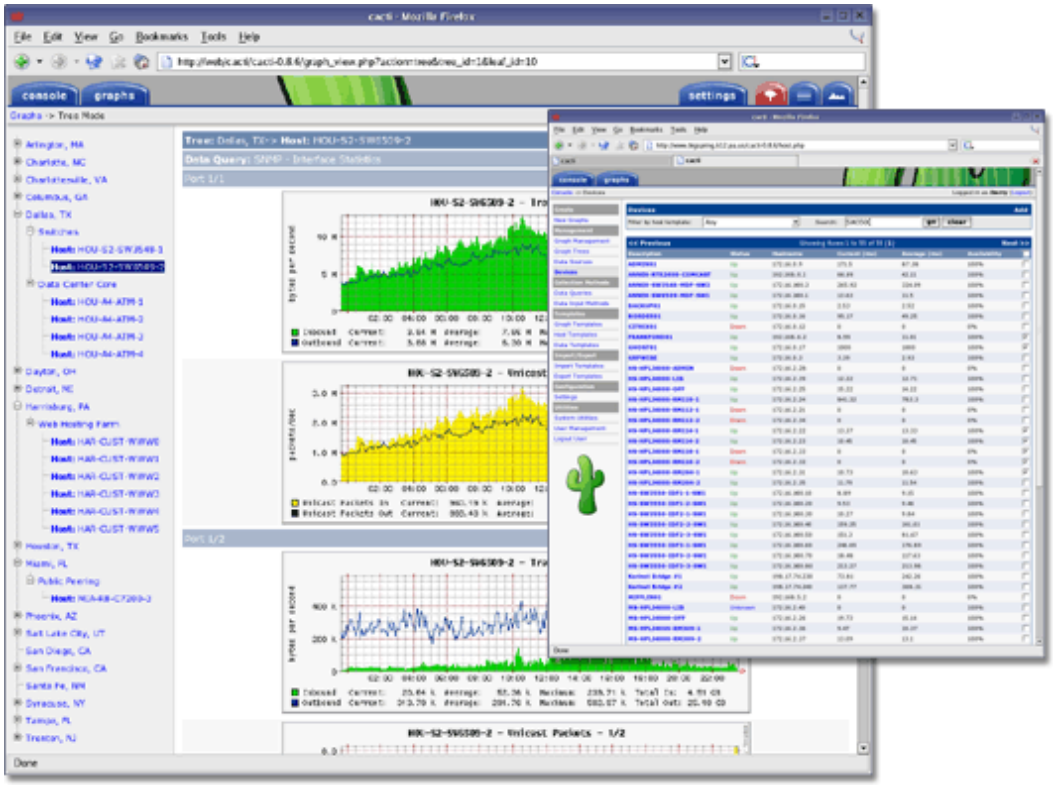
	Community *Ideal for home labs* **Free**	Professional *Ideal for SME and ISPs* **€230.00** / yr	Enterprise *Ideal for large Enterprises* **€1,200.00** / yr
Realtime software updates and fixes	✖	✔	✔
Twice-yearly releases	✔	✖	✖
Number of monitored devices, ports and sensors	Unlimited	Unlimited	Unlimited
Full autodiscovery of supported devices and metrics	✔	✔	✔
Network mapping through discovery protocols	✔	✔	✔
Rule-based automatic grouping	✖	✔	✔
Threshold, State and Syslog Alerting	✖	✔	✔
Traffic accounting system	✖	✔	✔
IP SLA, Pseudowire and Class-based QOS metrics	✖	✔	✔
RESTful API	✖	✔	✔
Support and Services options available	✖	✔	✔
Ability to scale an instance across multiple servers	✖	✖	✔
Priority consideration of feature requests	✖	✖	✔
Included Enterprise-grade support	✖	✖	✔ 10 Hours
	Download	Purchase	Purchase

Kuvio 15. Observium versiovertailu

4.4 Cacti ja RRDTool

Cacti oli yksi vaihtoehdoista, mutta se putosi kartoituksesta ensimmäisenä. Cacti on avoimen lähdekoodin monitorointityökalu. Cacti itsessään on vain graafinen sovellutus, joka on rakennettu RRDToolin päälle. Cacti hakee dataa UNIX/Linux-järjestelmän cron-job -työkalun avulla ja varastoi sen MySQL -tietokantaan. Tämän datan avulla RRDTool luo graafin, jota voidaan tarkastella. /7/

Cacti ei visuaalisen ilmeensä, dokumentaationsa ja yleisen tuntuman ja tunnettavuuden takia tullut prosessissa valituksi.



Kuvio 16. Esimerkkikuva Cactista

4.5 Kolmannen osapuolen SOC- ja SIEM-ratkaisut

Ulkopuoliset tarjoajat, kuten Elisa, tarjoavat ulkoistettua SOC (Security Operations Center) valvontaa. /8/ Tällöin monitoroinnin voi ulkoistaa kolmannelle osapuolelle. Suurempaa kartoitusta ei kolmannen osapuolen tarjonnasta tehty, muutamia palveluita on tarjottu ja niiden keskimääräinen hinta on alkaen 2000 € kuukaudessa.

Huomioiden, että jo kartoitetut avoimen lähdekoodin versiot eivät maksa mitään ja ne asennetaan RHEL/Cent OS-alustalle, joka on myös ilmainen, on oman monitoroinnin pystyttäminen taloudellisestikin kannattavaa. Vaikkakin SOC-palvelu tarkkailee kyberuhkia laajemmin kuin oma monitorointipalvelin, esimerkiksi sähköposti- ja käyttäjätunnus murtoja.

SOCin hankinnassa on tietenkin tärkeää verrata kustannustehokkuutta ja infrastruktuurin kokoa hankittavaan tuotteeseen. Huomioitavaa, että yrityksessä on noin 20 – 30 palvelinta ja noin 100 työasemaa (joista osa varakoneita/yhteiskäyttökoneita), ei SOC-ratkaisu välttämättä ole kannattava.

4.6 Kytkimen alustaminen

HPE OfficeConnect 1920S -kytkin on 24-porttinen kytkin, joka on suunniteltu käytettäväksi selaimen kautta, joko http- tai HTTPS-yhteydellä. Kytkimen kautta voi luoda sertifikaatin HTTPS:lle. Telnet- ja SSH-yhteyttä kyseiselle kytkimelle ei voi asettaa. /9, 10/

Kun kytkin on tehdasasetuksilla, kytkimeen tulee ottaa kiinni aluksi fyysisesti RJ-45:lla ja vaihtaa IP -alue yrityksen verkon IP -alueeksi. Jotta tuleva lokipalvelin saisi oikeat päivämäärä- sekä aikatiedot, tulee kytkimelle ilmaista SNTP- palvelimen osoite ja portti (portti 123). SNTP-palvelimena toimii AD DC -palvelin.

Admin -tunnukselle tulee luoda salasana. Kytkimen hallintasivulla on ”Password Manager” -asetusvalikko, jonka kautta voidaan määrittää salasanan pituuden mi-

nimimäärä sekä salasanan vanhenemispäivä ja määrä, jonka jälkeen tunnus menee lukkoon väärien kirjautumisyritysten johdosta.

Taulukko 2. HPE OfficeConnect 1920S IP -alue

	IP Address	**Subnet Mask**	**Gateway**
Default	192.168.1.1	255.255.255.0	
VLAN	194.188.125.7	255.255.255.0	194.188.125.3

4.7 LAN ja VLAN

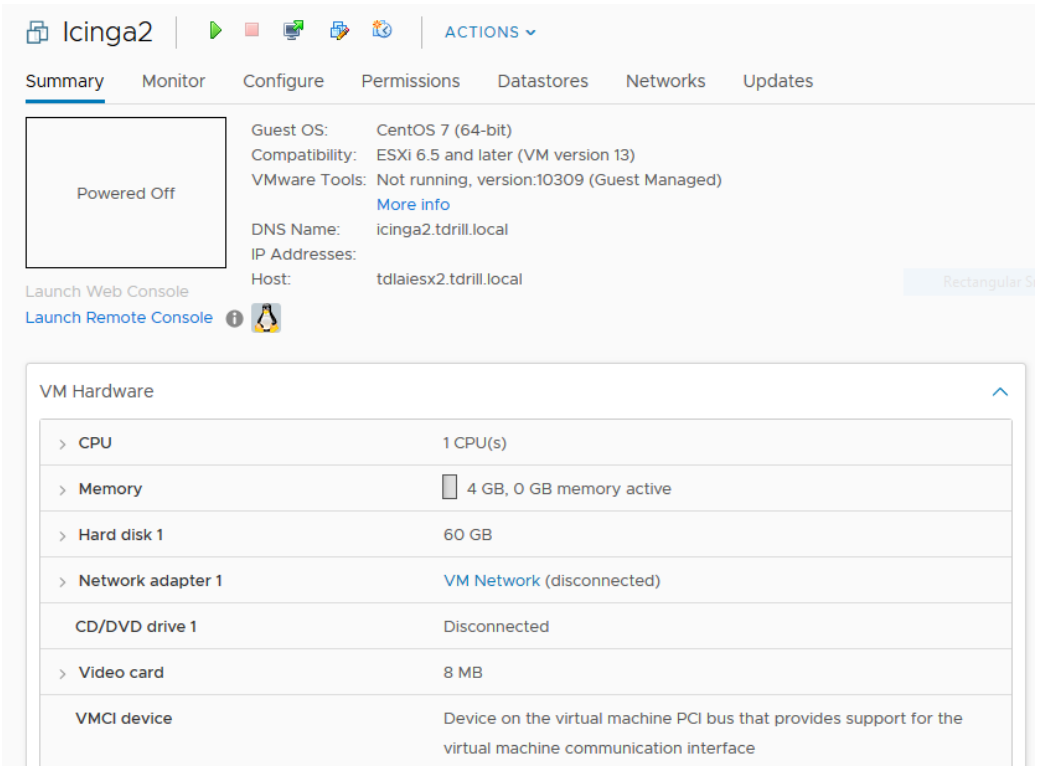
Nykyinen verkko koostuu seitsemästä kytkimestä ja reitittimestä (**Kuvio 6.**), ja nykyinen aliverkon maski on 255.255.255.0 (/24), joten kaikki yrityksen laitteet ovat samassa aliverkossa. Kytkintä konfiguroidessa tulee ottaa huomioon yrityksen VLANit, joita on kolme. Yksi näistä VLANista on tarkoitettu vierailijaverkolle ja toinen on palvelimille ja viimeinen VLAN on oletus VLAN (VLAN 1).

Nykyinen VLAN-ympäristö, joka on konfiguroitu HP:n ProCurve-kytkimillä, hyödyntää GVRP -tekniikkaa (GARP VLAN Registration Protocol), joka on määritetty standardissa IEEE 802.1p. /11, 12/ Tämän avulla porttien VLANit voidaan konfiguroida joko Untagged-, Tagged- tai Auto-tilaan. Untagged-tilassa kaikki liikenne sallitaan kyseisen portin läpi, eikä portilla ole erillistä merkattua VLANia. Tagged-tilassa portille on määritelty jokin VLAN, esimerkiksi WLAN AP:t on merkitty sekä vierasverkolle että yrityksen sisäverkolle, jolloin voidaan hyödyntää Wi-Fi-yhteyttä niin vierasverkossa kuin sisäverkossa. Viimeinen tila on Auto, johon GVRP liittyy. Tällöin GVRP-toiminto huomioi liikenteen laadun ja dynaamisesti mukauttaa portin määritettyjen VLAN-asetuksien mukaan. GVRP:n avulla helpotetaan VLAN-konfiguraatioita ja pienennetään konfiguraatiovirheiden riskiä.

Koska testiympäristö ei tule tarkkailemaan vierailijaverkkoa, kytkimelle asetetaan vain oleellinen palvelinten VLAN, koska verkkoliikenne tulee kulkemaan tämän kytkimen kautta monitorointipalvelimelle.

4.8 Linux -palvelimen asentaminen

Linux -palvelimeksi valikoitui CentOS 7. CentOS on Red Hat Enterprise-jakelun ilmainen avoimen lähdekoodin versio. CentOS on vakaa käyttöjärjestelmä, jossa paketit ja päivitykset jaetaan virallisista lähteistä (repository) vasta testausten jälkeen./13/



Kuvio 17. vSphere-selainikkuna

Virtuaalipalvelimelle varataan 60 Gt tilaa ja 4 Gt RAM -muistia. Virtuaalikone luodaan VMware vSphere-selainkäyttöliittymän kautta. Käyttöjärjestelmän asentaminen tapahtuu graafisen käyttöliittymän kautta. Palvelimelle määritetään staattinen IP -osoite sekä DNS -palvelin. Yrityksen DNS -palvelin on DC1 palvelimella Windows-ympäristössä, tämän takia täytyy käsin määrittää DNS -palvelimelta Linux -palvelimen nimi ja IP -osoite, jotta tulevaisuudessa palvelimeen voidaan PowerShellin tai PUTTYn kautta ottaa SSH -yhteys nimen (hostname) avulla. Linux:n tietoturva on jo ilman kolmannen osapuolen virustorjuntaohjelmia hyvä,

mutta varmistaaksemme, että palvelimelle ei pääse ulkopuoliset käsiksi, on hyvä asettaa SSH-konfiguraatio tiedostoon root -käyttäjälle kirjautumiskielto:

```
$ sudo nano /etc/ssh/sshd_config
> PermitRootLogin no
```

Kuvio 18. SSH-konfiguraatio

Toinen keino välttää ulkopuolisten mahdollinen kirjautuminen palvelimelle on luoda SSH -avaimet. SSH-avaimet voi luoda ssh-keygen komennolla.

```
$ ssh-keygen -b 4096 -t rsa
$ ssh-copy-id -I ~/.ssh/id_rsa.pub {user}@{hostname}
```

Kuvio 19. SSH-avainten luonti ja kopiointi

Tämä luo kaksi avainta, yksityisen (private) ja julkisen (public). Julkinen avain sijoitetaan palvelimelle kansioon (**Kuvio 19.**) ja yksityinen avain jää tietokoneelle, jolta SSH-yhteyttä käytetään. Avainten käyttöönoton jälkeen voidaan poistaa halutessa salasanalla kirjautuminen sshd_config- tiedostosta.

```
$ rpm -q centos-release
centos-release-7-6.1810.2.el7.centos.x86_64
```

Kuvio 20. CentOS 7

CentOS käyttää yum – ja rpm -paketinhallintaa. Eroavaisuutena näillä kahdella paketinhallinnalla on se, että yum osaa asentaa myös tarvittavat muut paketit, joita asennettava ohjelma tarvitsee. RPM taas huomauttaa käyttäjää, että asennettava paketti vaatii muita paketteja, mutta ei osaa näitä automaattisesti hakea ja asentaa. Eroavaisuutena on rpm:llä ja yum:lla on myös se, että rpm:n avulla voidaan asentaa useita versioita samasta paketista, missä taas yumissa ei tätä mahdollisuutta ole vaan se pyrkii päivittämään kyseisen paketin uuteen versioon tai vaihtoehtoi-

sesti antaa käyttäjälle varoituksen siitä, että paketti on jo asennettu tietokoneelle tai palvelimelle. Ominaisuutena yumissa on myös komennot yum update ja yum upgrade, jossa yum update päivittää kaikki päivitettävissä olevat paketit ja taas yum upgrade päivittää ja poistaa kaikki vanhentuneet paketit. Käyttöjärjestelmän asennuksen jälkeen tulee asentaa päivitykset sekä asentaa net-tools-paketti, joka mahdollistaa esim. ifconfig komennon käyttämisen. /14, 15/

On myös suositeltavaa asentaa yum-utils-paketti, joka mahdollistaa muita pakетinhallinnan komentoja (**Taulukko 3.**)

Taulukko 3. Yum-utils-komentoja

find-repos-of-install	Tarkistaa mihin repository:n paketti kuuluu
yumdownloader	Lataa paketin halutusta repository:sta
show-installed	Listaa kaikki RPM:llä asennetut paketit
reposync	Synkronoi repository:n tai useita paikalliseen hakemistoon

4.8.1 Lokipalvelinvaihtoehdot

Lokipalvelinta suunnitellessa pöydällä oli muutama vaihtoehto. Ensimmäinen vaihtoehto oli Nagios, johtuen sen yleisestä tunnettavuudesta. Toisena vaihtoehtona oli Zabbix, joko tuli vastaan tutkiessa muita avoimenlähdekoodin lokipalvelimia sekä jo aiemmin pudotetut Observium ja Cacti.

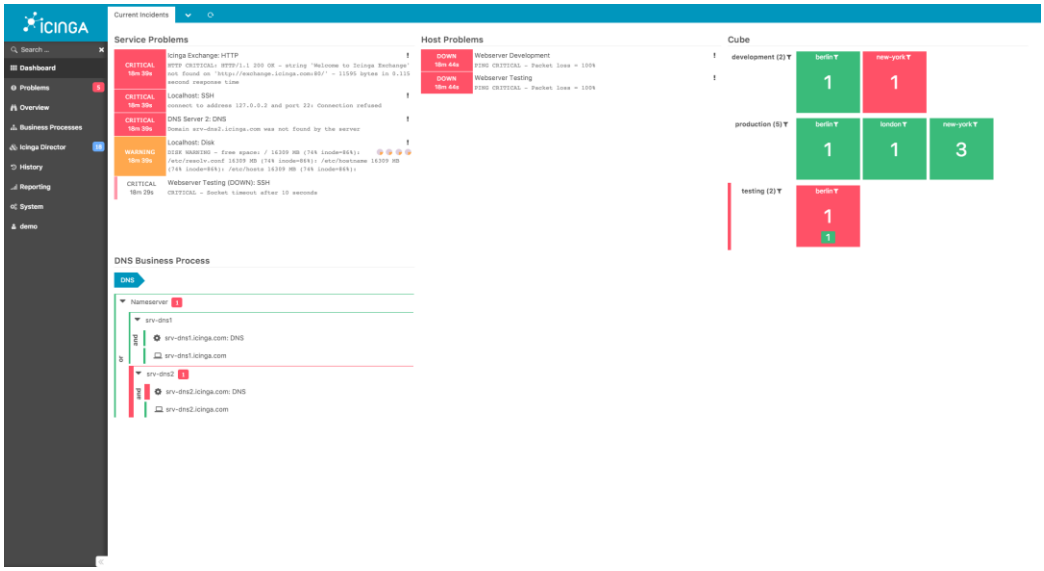
Viimeisenä vaihtoehtona oli Graylog, mutta se pudotettiin ensimmäisenä valinnoista. Graylog kerää lokitietoja halutuilta palvelimilta ja verkkolaitteilta, mutta koska sovelluksesta ja sen käyttämästä MangoDB:stä ja Elasticsearchista ei ollut mitään käyttökokemusta, se päätettiin siirtää mahdolliseksi projektiksi tulevaisuutta varten, jos tarve vaatii.

Icinga2 valikoitui sen käyttöliittymän perusteella ja siksi, koska se on Nagios-pohjainen järjestelmä. Icinga2-dokumentaatio oli myös paljon selkeämpi. Icinga2

tarjoaa myös suuren määrän erilaisia lisäosia, joita on mahdollista lisätä, mikäli järjestelmä täyttää halutut vaatimukset.

4.8.2 Icinga2

Icinga2 on avoimen lähdekoodin monitorointiohjelma, joka mahdollistaa verkon seurannan, sekä ilmoitukset mahdollisesti verkon katkoksista. Ohjelmalla voi luoda myös verkon käytön ja toimivuuden kattavia raportteja. Icinga2 on lisensoitu GNU General Public License Version 2 alle. Asennettava versio on 2.10.3. /16/



Kuvio 21. Icinga2-demon aloitussivu

Natiivina Icinga2 pystyy hakemaan Linux -palvelimien lokitietotoja ja tämän kautta esittämään esimerkiksi levytilan, heittovaihtomuistin (swap) tilan ja eri prosessien ja palveluiden tilan.

Windows-palvelimien ja tietokoneiden seuranta on myös mahdollista, mutta Windows -laitteessa tulee olla asennettuna joko NSClient tai Icingan oma monitorointipaketti, joka mahdollistaa Windows-lokien muuttamisen UNIX/Linux ystävällisemmäksi dataksi.

4.8.3 Icinga2 asentaminen

Icinga2 palvelimen asentamiseen löytyy suoraviivainen ”Getting Started”-sivu, joka ohjaa käyttäjän alkuun Icinga2 alustamisessa. Icinga2-hakemistoa (repository) on listattuina sivun alussa ja usealle Linux-jakelulle on ohjeistus, kuinka paketit asennetaan ja millä nimillä ne löytyvät hakemistoista. Kaikki asennuksessa suoritettavat komennot vaativat root -käyttäjäoikeudet. /16/

Icinga2:lla on oma hakemisto CentOS7:lle. Hakemistot kuuluvat EPEL-paketteihin (Extra Packages for Enterprise Linux). Jotta Icinga2 saadaan asennettua, tulee RPM -hakemisto asentaa yum -paketinhallinnan kautta, sekä asentaa EPEL -kirjasto. Hakemiston ja EPEL -paketin asentamisen jälkeen asennetaan Icinga2.

Icinga2 tarjoaa useita lisäosia (plugins) ja ne saadaan asennettua Icingaan omasta jakelupaketista. Icinga2 käyttää samoja lisäosia kuin Nagios, joten lisäosapaketti kulkee Nagios-nimellä (**Kuvio 22.**)

```
$ yum install https://packages.icinga.com/epel/icinga-rpm-
release-7-latest.noarch.rpm
$ yum install epel-release
$ yum install icinga2
$ yum install nagios-plugins-all
$ systemctl enable icinga2
$ systemctl start icinga2
```

Kuvio 22. Icinga2 hakemiston (repository) asennus ja käyttöönotto

Taulukko 4. Systemctl -komennot

Komento	Kuvaus
Start	Käynnistää Icinga2 palveluprosessin
Stop	Pysäyttää Icinga2 palveluprosessin
Restart	Käynnistää Icinga2 palveluprosessin uudelleen
Reload	Sama prosessi kuin Restart -komento, mutta ei odota, että palveluprosessi käynnistyy uudelleen
Status	Tarkistaa palveluprosessin tilan
Enable	Käynnistää palveluprosessin automaattisesti järjestelmän uudelleenkäynnistyksen jälkeen

Icinga2 vaatii SELinux (Security-Enhanced Linux) laajennuksen, jonka avulla voidaan laajennetuin oikeuksin hallita järjestelmää (MAC, mandatory access control). Icinga2 Red Hat-varianteissa on oma SELinux ”policy”, joka määrittää ominaisuuksien käyttöönoton sekä komentojen käyttämisen.

Valinnaisina ominaisuuksina järjestelmään voi asentaa tuen, joko Vim tai nano -tekstieditorille. Testijärjestelmään asennetaan tuki nanolle, jolloin saadaan Icingan konfiguraatiotiedostoille syntax highlightin päälle.

```
$ yum install icinga2-selinux
$ yum install nano-icinga2
$ cp /etc/nanorc ~/.nanorc
$ nano ~/.nanorc
## Icinga2
Include “/usr/share/nano/icinga2.nanorc”
```

Kuvio 23. SELinux ja nano syntax highlight

4.8.4 MySQL ja Icinga Web 2

Icinga2-käyttöliittymä on selaimen kautta käytettävissä, ja tämän takia palvelimelle tulee asentaa web -palvelin. Jotta lokidata saadaan hakemistottyä, myös tietokanta tulee asentaa palvelimelle.

MySQL Secure Installation suorittaa MariaDB-asennuksen tietoturva-asiat. Tietokannan root -käyttäjälle annetaan salasana, järjestelmästä poistetaan anonymous -käyttäjä, järjestelmästä poistetaan test -tietokanta sekä estetään root -käyttän etäkirjautuminen.

Icinga2 käyttää DB IDO (Database Icinga Data Ouput)-järjestelmää, joka huolehtii datan viemisestä tietokantaan. Järjestelmälle tulee luoda tietokanta. Icinga2 asennus luo käyttäjän icinga, jolla ei ole kirjatumista, mutta käyttäjä hallinnoi datan viemistä tietokantaan. IDO-moduulin konfiguraatiotiedostosta tulee poistaa kommentit käyttäjätiedoista. MySQL kautta luodaan tietokanta (**Kuvio 24.**) ja tuodaan IDO schema tietokantaan. IDO MySQL -moduuli tulee ottaa käyttöön ja käynnistää Icinga2 järjestelmäpalvelun uudelleen.

```
$ yum install mariadb-server mariadb
$ systemctl enable mariadb
$ systemctl start mariadb
$ mysql_secure_installation
$ yum install icinga2-ido-mysql
$ mysql -u root -p
CREATE DATABASE icinga;
GRANT SELECT, INSERT, UPDATE, DELETE, DROP, CREATE VIEW, IN-
DEX, EXECUTE ON icinga.* TO ‘icinga’@’localhost’ BY ‘ic-
inga’;
$ mysql -u root -p icinga < /usr/share/icinga2-ido-
mysql/schema/mysql.sql
$ nano /etc/icinga2/features-available/ido-mysql.conf
$ icinga2 feature enable ido-mysql
$ systemctl restart icinga2
```

Kuvio 24. MySQL asennus

Icinga Web 2 asennusta suositellaan asennettavaksi Apache2 -webpalvelimen päälle, mutta erillinen dokumentointi löytyy myös nginx-asennukselle. Webpalvelimen rinnalle suositellaan myös PHP-FPM lisäosaa.

Palomuuriin avataan portti 80 http -liikenteelle. Olisi suositeltavaa käyttää porttia 443 ja https -liikennettä, mutta testiympäristössä käytämme porttia 80.

Icinga2 vaatii myös REST APIn toimintojen käyttöön. API komennolla asennetaan API ominaisuus järjestelmälle ja konfiguraatiotiedostossa annetaan oikeudet käyttäjälle suorittaa toimintoja (**Kuvio 25.**)

```
$ yum install httpd
$ systemctl enable httpd
$ systemctl start httpd
$ firewall-cmd --add-service=http
$ firewall-cmd --permanent --add-service=http
$ icinga2 api setup
$ nano /etc/icinga2/conf.d/api-users.conf
 object ApiUser “icingaweb2” {
  password = “xxxxxxxxxxxxx”
  permissions = [ "status/query", "actions/*", "ob-
jects/modify/*", "objects/query/*" ]
}
$ yum install php php-php-gettext php-intl php-mbstring php-
common php-xml php-mysql php-ldap
$ yum install centos-release-scl
$ nano /etc/opt/rh/rh-php71/php.ini
 [Date]
 Date.timezone = “Europe/Helsinki”

$ yum install icingaweb2 icingacli icingaweb2-selinux
$ icingacli setup config webserver apache --document-root
/usr/share/icingaweb2/public
$ systemctl restart httpd.service
$icingacli setup token create
```

Kuvio 25. Web-palvelimen asentaminen ja konfiguroiminen

Lopuksi asennus suoritetaan loppuun Web- käyttöliittymän kautta. Asentaminen alkaa suoraan, kun avaa sivun http://<palvelin>/icingaweb2/setup. Asentaja kysyy web -käyttöliittymän käyttäjää API- käyttäjää sekä jo luodut tietokannat. Valinnaisia moduuleja voi myös asentaa, mikäli ne ovat tarpeellisia. /17/

Käyttöliittymä asentajan jälkeen Icinga2 on valmis käytettäväksi ja palvelimen kautta tai Icinga Director web -työkalun avulla voidaan lisätä uusia monitoroitavia laitteita.

4.8.5 Icinga2 monitoroinnin konfigurointi

Icinga2 avulla on mahdollista tarkkailla, joko laitteiden tilaa tai Windows- sekä Linux -laitteiden palveluita. Windowsin palveluiden tarkkaileminen vaatii erillisen Client- ohjelmiston asentamisen, jolloin on mahdollista kääntää Windows -lokitiedostot Linuxille natiiviin muotoon. Koska työn tarkoituksena on tarkkailla kriittistä IT -infrastruktuuria, keskitytään monitoroinnissa verkkolaitteiden sekä tärkeiden palvelimien tilan tarkkailuun.

Icinga2 hakemiston alta voidaan löytää kaikki kriittiset konfiguraatiot, mitä asennusvaiheessa on luotu. Hakemiston juuressa on constants.conf, joka määrittää pääsolmukohdan, eli Icinga2 monitorointipalvelimen FQDN:n (Fully Qualified Domain Name), sekä sisältää zones.conf tiedoston, jonka avulla voidaan määrittä Master-Slave-yhteyksiä eri solmukohtien välillä, esimerkiksi maantieteellisen sijainnin perusteella. Icinga2:ssa, kuten myös Nagioksessa, on mahdollisuus asentaa moduuleja ja ominaisuuksia. Nämä ominaisuudet voidaan aktivoida Web-käyttöliittymän kautta tai Icinga2 hakemiston features-available-kansiosta.

Tärkeimpinä päivittäisiä konfiguraatiota huomioiden on conf.d hakemiston konfiguroinnit mallipohjille sekä itse konfiguraatioille. Hakemistosta löytyy myös komentojen konfiguraatiot, käyttäjät, ryhmät, palvelut ja huomautusten konfiguraatiot. Konfiguraatiot verkkolaitteiden ja palvelimien tilan tarkkailuun määritellään hosts.conf tiedostossa (**Kuvio 26.**)

```
Object Host “device” {
  check_command = “hostalive”
  address = “xxx.xxx.xxx.xxx”
}
```

Kuvio 26. Esimerkki konfiguraatiosta

Hostalive -komento suorittaa tasaisin väliajoin tarkistuksen, että laite on käynnissä. Koska Icinga2 käyttää REST APIa näkyy web -käyttöliittymässä reaaliajassa laitteiden tila.

```
/**
 * The constants.conf defines global constants.
 */
include "constants.conf"
/**
 * The zones.conf defines zones for a cluster setup.
 * Not required for single instance setups.
 */
include "zones.conf"
/**
 * The Icinga Template Library (ITL) provides a number of
useful templates
 * and command definitions.
 * Common monitoring plugin command definitions are includ-
ed separately.
 */
include <itl>
include <plugins>
include <plugins-contrib>
include <manubulon>
/**
 * This includes the Icinga 2 Windows plugins. These com-
mand definitions
 * are required on a master node when a client is used as
command endpoint.
 */
include <windows-plugins>
include <nscp>
```

Kuvio 27. Esimerkki Icinga2.conf-kirjastoista

Kuviossa 27 on esimerkki kirjastoista, joita Icinga2 käyttää. Huomioitavaa on windows-plugins-kirjasto. Tämä kirjasto mahdollistaa Windows -laitteiden palveluiden monitoroinnin. Kirjasto nscp mahdollistaa taas NSClient++ ohjelman lähettää dataa monitoroitavalta laitteelta palvelimelle.

```
$ firewall-cmd --permanent --add-port=5665/tcp
$ firewall-cmd --reload
```

Kuvio 28. Portin 5665 avaaminen

Windows-palvelinta monitoroidessa täytyy Windows-laitteelle asentaa Icinga2 monitorointipalvelu. Monitorointipalvelinta asentaessa asennukseen annetaan tarkkailtavan laitteen FQDN sekä valinnainen asennustiketti, joka auttaa varmentaa palvelimen ja palvelun välisen interaktion (**Kuvio 28.**) Palveluun tulee syöttää Icinga2 palvelimen FQDN sekä portti, jonka kautta liikenne toimii (oletusportti 5665).

```
$ icinga2 pki ticket --cn *instance name*
4sa65fjdjkndf8384848hjf83

$ nano /etc/icinga2/conf.d/host.conf

Object Endpoint ”*instance name*” {
  Host = “xxx.xxx.xxx.xxx”
}

Object Host ”*instance name*” {
  import ”generic-host”
  address = “xxx.xxx.xxx.xxx”
  ……
```

Kuvio 29. Tiketti ja esimerkkikonfiguraatio

Palveluiden tarkkailuun löytyy useita komentoja (”check_command”, **Kuvio 26.**) ja näille komennoille myös tarkennuksia (**Taulukko 5.**), kuten eri varoitukset ja huomautukset, palveluiden selite ja esimerkiksi määre millä esitysmuodolla data näytetään monitorointipalvelimella (esim. aika millisekunteina tai sekunteina ja tila tai datan määrä megatavuina tai gigatavuina).

Taulukko 5. Esimerkkejä monitorointikomennoista

Komento	**Kuvaus**
hostalive4/hostalive6	Lähettää ping:n tasaisen väliajoin tarkistaakseen, onko palvelin päällä
http	Tarkistaa onko palvelimen web-palvelin käynnissä
ldap	Tarkistaa LDAP:n toiminnan
nrpe	Kysely NSClient++ ohjelmalle
nscp	Datan keräys NSClient++ ohjelmalta
procs	Prosessien valvonta
ssh	SSH:n tarkkailu
network	Tulevan ja lähtevän liikenteen määrä
memory	Muistinkäyttö
tcp	TCP monitorointi/laitteiden porttien tarkkailu
load	Esim. prosessorin kuorma
disk	Levynkäyttö
disk-windows	(Windows) laitteiden levynkäyttö
memory-windows	(Windows) laitteden muistinkäyttö
network-windows	(Windows) Tulevan ja lähtevän liikenteen määrä
procs-windows	(Windows) Prosessien valvonta
service-windows	(Windows) Palveluiden tarkkailu
update-windows	(Windows) Windows update-kysely

4.8.6 Icinga2 Director

Icinga Director helpottaa laitteiden konfiguraatioita, kun ne voi suorittaa suoraan web -käyttöliittymän kautta. Dirctorin asennus on erittäin suoraviivaista ja vaatii vain tietokannan, sekä Director -moduulin toimiakseen (**Kuvio 30.**) /18/

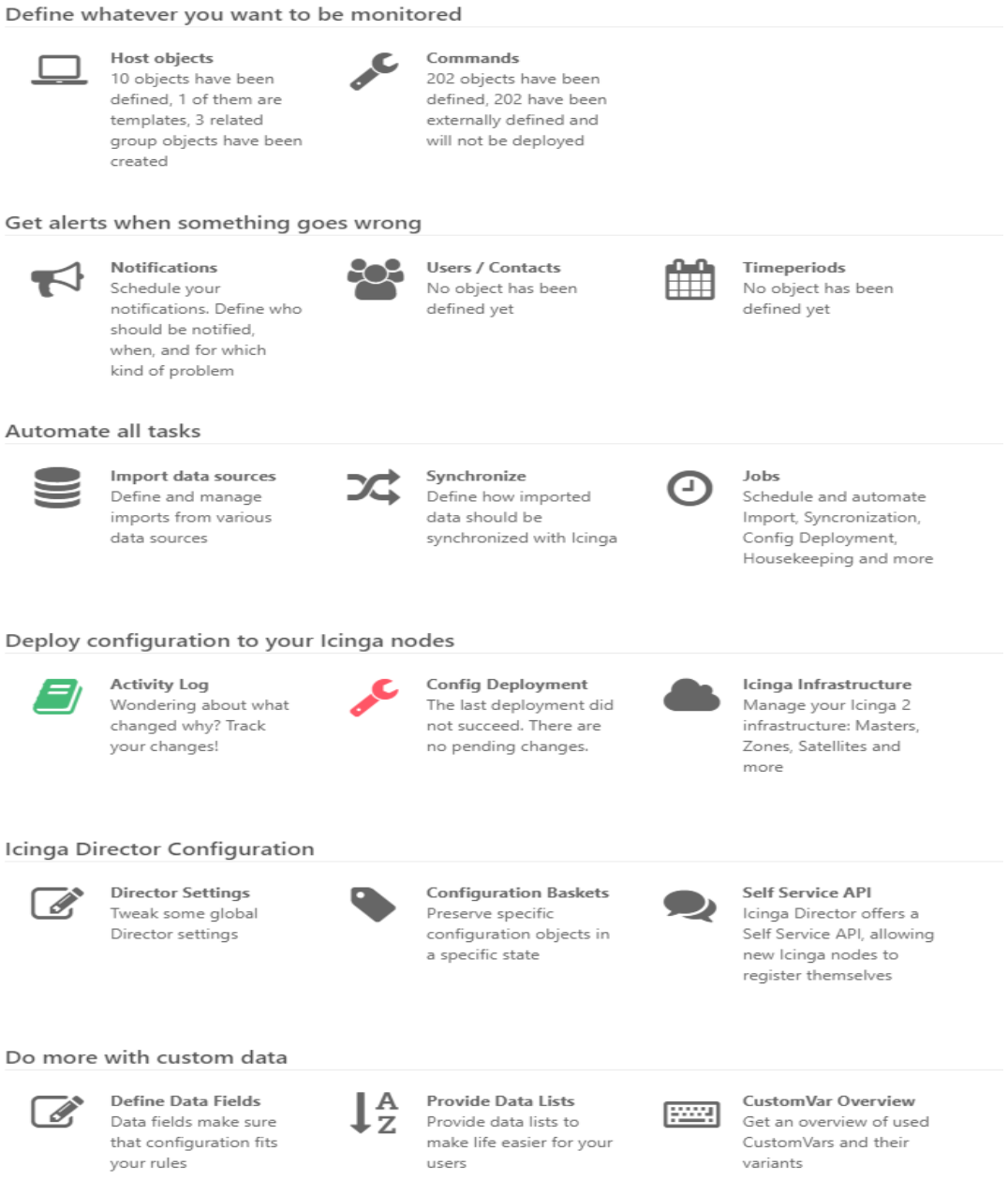
```
mysql -e "CREATE DATABASE director CHARACTER SET 'utf8';
   GRANT ALL ON director.* TO director@localhost IDENTIFIED
BY 'xxxxx;"

$./install.sh
ICINGAWEB_MODULEPATH="/usr/share/icingaweb2/modules"
REPO_URL="https://github.com/icinga/icingaweb2-module-
director"
TARGET_DIR="${ICINGAWEB_MODULEPATH}/director"
MODULE_VERSION="1.6.2"
git clone "${REPO_URL}" "${TARGET_DIR}" --branch
v${MODULE_VERSION}

$ icingacli module enable director

$ nano /etc/icinga2/conf.d/api-users.conf
object ApiUser “director” {
  password = “xxxxxxxxxxxxx”
  permissions = [ "*" ]
}
```

Kuvio 30. Director-asennus

Tietokannan luonnin jälkeen voidaan Icinga Director asentaa, joko suoraan GitHubista tai tar -paketista. Kuviossa 19 oleva install.sh on shell skripti, joka ajaa asennuspolun ja paketin hakemisen GitHubista. Kun paketti on ladattu, voidaan icingacli -komennolla käynnistää Director.

Director löytyy web -käyttöliittymästä vasemmasta sivupalkista ja sen käyttö eroaa muutamalla tavalla perinteisestä tekstieditorin kautta suoritettavasta konfiguraatiosta. Esimerkiksi Director vaatii aina jonkin mallipohjan, kun sen kautta luodaan uusi monitoroitava laite. Mallipohja voidaan luoda myös Directorilla (**Kuvio 31**.)

Myöskin muutosten hyväksyminen tapahtuu Directorissa eri tavalla. Mikäli esimerkiksi valvottaviin palveluihin tai laitteisiin luodaan uusi valvottava kohde, täytyy muutos hyväksyä järjestelmänvalvojan toimesta ennen kuin valvontaprosessi aloitetaan. Tällä menetelmällä pyritään estämään virheellisten konfiguraatioiden luomista. /18/



Kuvio 31. Icinga Director

5 JOHTOPÄÄTÖKSET

Työn tarkoituksena oli kartoittaa nykyinen IT -infrastruktuuri ja luoda malliratkaisu kyseisen infrastruktuurin valvonnan helpottamiseksi. Useita kehityskohtia löytyi työn aikana.

Yrityksen kytkimien ja verkkokaavioiden uusiminen tulee tapahtumaan lähitulevaisuudessa. Nykyinen malli, jossa kytkimet on liitetty hyvin väylä tyyliseen tapaan, nostaa riskiä verkkokatkoista, mikäli jokin kytkin rikkoutuu tai tipahtaa pois päältä. Lisäksi kytkinten ikä huomioiden on niiden päivittäminen hyvin ajankohtaista. Työssä käytetty HPE OfficeConnect ei tule olemaan malli, jota ratkaisussa käytetään. Syynä tähän on telnet-yhteyden vajaat toiminnot sekä SSH- yhteyden puuttuminen. Lisäksi uusien kytkimien avulla voidaan karsia muutama kytkin pois hankkimalla kytkimiä, joissa on enemmän portteja.

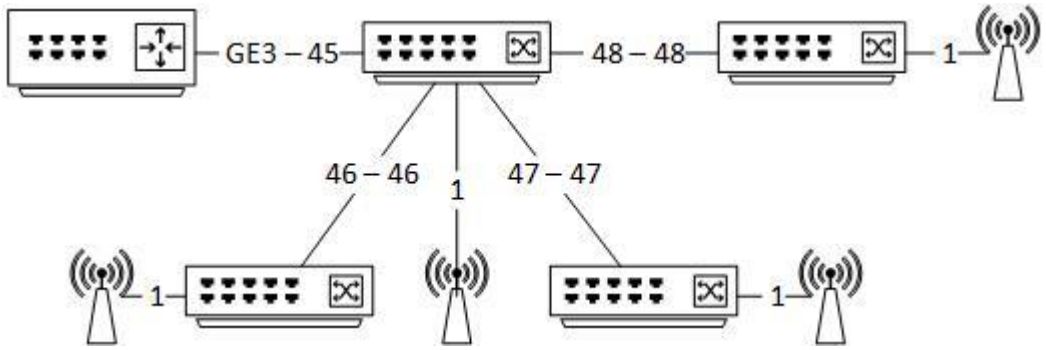
Nykyisessä VLAN-konfiguraatiossa portit on konfiguroitu sen mukaan missä laite on kiinni. Esimerkiksi SOPHOS APit voivat olla kytkimessä missä portissa tahansa, joka jälkeen portti on jälkikäteen konfiguroitu oikeille asetuksille. Uusissa kytkimissä portit konfiguroidaan kaikissa samoin, jolloin saavutetaan yhteneväinen kaava konfiguraatioiden suhteen. Esimerkiksi portit 1-4 vierasverkolle ja portit 45-48 toisten kytkinten liittämiseen. Kaikki kytkimet uusitaan samalla kertaa, jotta myös kytkimet ovat kaikki yhteneväisiä. Lisäksi nykyisen verkon kytkimistä vain osa on varustettu GigabitEthernet -porteilla ja uudet kytkimet tulevat kaikki tukemaan GigabitEthernet -portteja. Alun perin työn aikana oli tarkoitus tutkia mahdollista kytkinten kahdentamista, mutta työn aikana tehtiin huomio, ettei se ole kustannussuhteiltaan järkevää.

Palomuuripalvelu on tällä hetkellä ulkoistettu ja mikäli palomuuriin halutaan tehdä muutoksia, tulee ne suorittaa palveluntarjoajan kautta. Myös mahdollinen palomuuripalvelun sijoittaminen omaan hallintaan on noussut kehitysideaksi kartoittamisen aikana. Täten kontrolli palomuurin toiminnasta olisi yrityksellä, mutta nykyinen tukimalli jäisi pois. Tulevaisuuden kehityssuunnitelmassa tulee arvioida hyöty-haittasuhdetta tämän kaltaisessa tilanteessa.

Icinga2 -monitorointipalvelun ominaisuudet osoittautuivat hyödyllisiksi, mutta esimerkiksi verkkoliikenteen valvonnan ja palveluiden valvonnan testaaminen jäi vielä puutteelliseksi. Monitorointi on selvästi hyödyllinen osa nykyistä toimintamallia ja tulevaisuudessa Icingan testaamista jatketaan laajentamalla sen toimintaa palveluiden tarkkailua ajatellen. Koska yrityksen palvelimet ovat Windows -palvelimia ja niissä on räätälöidyt palvelut, kuten tuotehallintajärjestelmä ja ERP, täytyy ensin tutustua aiheuttaako Icingan monitorointipalvelu ongelmia kyseisissä palvelimissa.

Nykyisellään palvelimien tilan tarkkailu ei aiheuta ongelmia tuotantoympäristössä. Myöskin vaihtoehtoista monitorointiohjelmaa tarkkaillaan, koska nykyinen työasema ja palvelinympäristö on kolmea palvelinta lukuun ottamatta Windows-pohjainen, olisiko mahdollista löytää myös Windows-palvelimelle sopiva monitorointi järjestelmä ja mitkä sen kustannukset olisivat. Ilmaiseksi variantiksi Icinga2 ajaa asiansa loistavasti. Se on erinomainen työkalu esimerkiksi, kun ympäristön tarkkailuun tarvitaan kustannustehokas ja erittäin muokattavissa oleva työkalu.

Verkkoliikenteen yksityiskohtainen tarkkailun mahdollinen käyttöönotto voi vaatia toimenpiteitä laajentamalla ympäristö koko konsernin laajuiseksi. Huomioitavaa tässä mahdollisessa kehityssuunnassa on GDPR ja se, mitä dataa voidaan tarkkailla yrityksen sisäverkossa. Myös ajankohtainen koko konsernin tietoturvakartoitus on käynnissä ja näitä kyseisiä mietteitä ja tuloksia pyritään hyödyntämään kartoituksen tekemisessä.



Kuvio 32. Suunniteltu kytkinkaavio

Työn tekniikat olivat jo entuudestaan tuttuja. Verkkoympäristön teoriaa ja käytäntöä tuli kerrattua Ciscon ja HP:n erilaisista dokumentaatioista sekä myös kirjasta ”Networking Bible”. Linux -palvelimen käyttö oli myös tuttua, koska olin perustanut jo kolme Linux-palvelinta muihin projekteihin.

Ongelmakohdiksi ja haasteiksi muotoutui hahmotus, kuinka erilaisia hankintoja priorisoidaan yrityksessä. Työn alustus- ja suunnitteluvaiheessa puhuttiin esimerkiksi kytkinten kahdentamisesta ja verkon vikasietoisuuden parantamisesta, myöskin mahdollisesti osastojen jakaminen omiin VLAN oli mietinnässä ja on sitä myös edelleen. Lopulta tulee miettiä hinta-hyötysuhdetta kyseisissä hankinnoissa. Esimerkiksi yrityksen noin sadan PC:n ja kahden virtualisointialustan verkossa kytkinten kahdentaminen laskisi riskiä verkon putoamiselle, mutta hinta hyötysuhteiltaan se ei tämän kokoisessa ympäristössä olisi järkevää. Sama koskee myös verkon vikasietoisuutta. Nykyisten laskelmien pohjalta on järkevämpää karsia kytkinten määrää yhdellä ja jättää yksi valmiiksi konfiguroitu kytkin mahdollisia vikatilanteita varten varalle. Tämän takia kuten kehitysideoissa jo mainittiin, on tärkeää, että kaikki kytkimet on konfiguroitu samalla lailla.

VLAN jokaiselle osastolle omaksi parantaisi verkon tietoturvaa, mutta toisaalta vaatisi hallinnallisia muutoksia, jotta esimerkiksi IT-osasto pääsisi suoraan kaikkiin VLAN-ympäristöihin käsiksi.

Icinga2 valikoitui palvelimeksi, koska Nagios oli jo tuttu entuudestaan konseptina. Valinnassa suurin tekijä oli se, että se on ilmainen avoimenlähdekoodin ohjelmisto. Icinga mahdollisti hyvän ”proof of concept” tyyppisen ratkaisun, jotta mahdollisesti tulevaisuudessa, resurssit huomioiden, halutaan yritykselle hankkia maksullinen ja tuettu monitorointipalvelin.

Icinga2 on hyvä monitorointipalvelin, mutta kuten useasti Linux-palvelimilla, jos ei tiedä mitä tekee voi vahinko itse palvelimelle olla hyvin suuri. Muutamalla konfiguraatiovirheellä voi saada koko monitorointipalvelimen täysin sekaisin, mikä vie koko palvelimen idean toimia ns. ennaltaehkäisevänä työkaluna pois.

LÄHTEET

/1/Network Infrastructure – Cisco Viitattu 20.2.2019
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/srnd/design/guide/cmesrnd/nstrct.pdf

/2/Introduction to Computer Network Topology Viitattu 20.2.2019
https://www.lifewire.com/computer-network-topology-817884

/3/Sosinsky B. 2009 Networking Bible. Wiley India Pvt. Viitattu 20.2.019
https://books.google.fi/books?id=3DOREqRZejcC&pg=PA16&redir_esc=y#v=onepage&q&f=false

/4/Zabbix 4.0 LTS Manual Viitattu 22.1.2020
https://www.zabbix.com/documentation/4.0/manual

/5/Nagios 4 Manual Viitattu 22.1.2020
https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/index.html

/6/Observium Viitattu 22.1.2020
https://www.observium.org/

/7/Cacti Viitattu 22.1.2020
https://www.cacti.net/

/8/Elisa Kyberturvakeskus Viitattu 22.1.2020
https://yrityksille.elisa.fi/kyberturvakeskus

/9/HP:n viralliset spesifikaatiot (HPE OfficeConnect 1920S Switch Series Quick-Specs) Viitattu 20.2.2019.
https://h20195.www2.hpe.com/v2/GetDocument.aspx?docname=a00001630enw

/10/HP:n asennus ja konfiguraatio ohje (HPE OfficeConnect 1920S Switch Series – Configuring Switch) Viitattu 20.2.2019
https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00023092en_us

/11/IEEE Standards sivustolla sivustolla Viitattu 21.2.2019
https://standards.ieee.org/

/12/IEEE 802.x standardit sivustolla Viitattu 21.2.2019 https://1.ieee802.org/

/13/CentOS 7 asennusdokumentaatio (CentOS manuals) Viitattu 16.12.2019
https://docs.centos.org/en-US/centos/install-guide/getting-started/

/14/RPM:n virallisen sivun dokumentaatio (RPM documentatiton) Viitattu 21.2.2019 http://rpm.org/documentation.html

/15/Yum virallinen dokumentaatio (Yum’s documentation) Viitattu 21.2.2019
http://yum.baseurl.org/api/yum/

/16/Icinga2 Getting Started Viitattu 4.3.2019
https://icinga.com/docs/icinga2/latest/doc/02-getting-started/

/17/Icinga Web 2 Installation documentation Viitattu 4.12.2019
https://icinga.com/docs/icingaweb2/latest/doc/02-Installation/

/18/Icinga2 Director introduction and installation Guide Viitattu 4.12.2019
https://icinga.com/docs/director/latest/doc/02-Installation/