Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ATTE SANDROOS

Zero client -konesalivalvomo

Konesalivalvomoiden käyttöönotto zero client -teknologialla.

SÄHKÖ- JA AUTOMAATIOTEKNIIKAN
TUTKINTO-OHJELMA
2023

TIIVISTELMÄ

Sandroos, Atte: Zero client -konesalivalvomo. Konesalivalvomoiden käyttöönotto zero client -teknologialla.
Opinnäytetyö, AMK
Sähkö- ja automaatiotekniikan tutkinto-ohjelma.
Toukokuu 2023
Sivumäärä: 33

Tässä opinnäytetyössäni toteutettiin Verne Global Finlandin konesalien valvonnan näkyvyyden parantaminen, sijoittamalla valvontamonitoreita yrityksen eri toimipisteisiin. Valvontamonitorien avulla yrityksen työntekijöiden on helpompi valvoa konesalien toimintaa.

Konesalivalvomoiden luomisessa avainasemassa olivat zero client -teknologia, jonka avulla konesalivalvomon hallinnasta ja ylläpidosta tehtiin mahdollisimman helppoa ja kustannustehokasta keskittämällä molempien konesalivalvomoiden ylläpito palvelimille, sekä MonitorsAnyWhere -sovellus, jonka tarkoitus on hallita zero client -laitteisiin kytkettyjen näyttöjen sisältöä, ja näyttää näytöillä konesalivalvontaan käytössä olevia sovelluksia.

Opinnäytetyössäni tutustutaan konesalien toiminnan jatkuvuuden varmistamiseen konesaliliiketoiminnassa. Sekä hyvän tilanteen näkyvyyden merkitykseen tilannekuvan muodostamisessa ja sen kautta oikeanlaiseen ongelmiin reagointiin konesalien toiminnan jatkuvuuden varmistamisessa. Lisäksi tutustutaan zero client -teknologiaan, sen ominaisuuksiin, tuomiin etuihin ja mahdollisiin rajoituksiin.

Abstract

Sandroos Atte: Zero client data center control room. Data center control room setup using zero client technology.
Bachelor's thesis
Electrical and automation engineering
May 2023
Number of pages: 33

In my thesis, I aimed to improve the data center control of Verne Global Finland's two data centers by implementing control rooms in two different locations. Control rooms aim to improve the company's employee's ability to monitor the data center operations.

In key positions in creating the two datacenter control rooms was zero client technology, which makes the management and maintenance of the datacenter control room as easy and cost-effective as possible by centralizing the maintenance of both control rooms to servers, and MonitorsAnyWhere -application the purpose of which is to manage the content of the monitors connected to the zero client -devices and display on the screens the applications used for datacenter monitoring.

In my thesis, I write about ensuring the continuity of data center operations in the data center business. As well as the importance of good situational awareness in creating a picture of the situation and using the situational picture in the right way to help in proper reacting to problems and ensuring the continuity of data center operations. In addition, we will get to know zero client -technology, its features, advantages, and possible limitations.

SISÄLLYS

LYHENNELUETTELO

BSOD = Blue Screen of Death, Windows käyttöjärjestelmän virheilmoitusruutu virheille, joista käyttöjärjestelmä ei voi palautua.
DDoS = Distributed Denial of Service, hajautettu palvelunestohyökkäys.
DVI = Digital Visual Interface, digitaalinen visuaalinen käyttöliittymä.
HDMI = High-Definition Multimedia Interface, teräväpiirto multimedia käyttöliittymä.
IIS = Internet Information Services, Microsoftin kehittämä palvelinohjelmistokokonaisuus.
LAN = Local Area Network, lähiverkko.
MAWi = MonitorsAnyWhere web-based interface, MonitorsAnyWhere verkkopohjainen käyttöliittymä.
RDP = Remote Desktop Protocol, tietokoneen etähallinta protokolla.
SNMP = Simple Network Management Protocol, yksinkertainen verkon hallinta protokolla.
UPS = Uninterruptible Power Supply, keskeyttämätön virransyöttö.
VGA = Video Graphics Array, video grafiikka array.
VLAN = Virtual Local Area Network, virtuaalilähiverkko.
WAN = Wide Area Network, laajaverkko.

1 JOHDANTO

1.1 Opinnäytetyön tausta ja tavoitteet.

Tämän opinnäytetyön tavoitteena oli suunnitella ja toteuttaa opinnäytetyön toimeksiantajan Verne Global Finlandin tarpeisiin soveltuvat datakeskusvalvomot, joiden avulla yrityksen kolmen eri datakeskuksen valvominen ja ylläpito tulevat niistä vastaavalle operatiiviselle henkilökunnalle mahdollisimman helpoksi. Valvomot ovat suunniteltu ja toteutettu vuoden 2022 aikana.

Yrityksen kaikki konesalit ovat toiminnassa ympäri vuorokauden, vuoden jokaisena päivänä. Konesalien toiminnan kannalta on erittäin tärkeää välttää asiakkaille mahdollisia palvelukatkoksia. Näin onkin hyvä olla tietoinen konesalien toimintaan liittyvistä asioista, kuten konesalien lämpötiloista, UPS- (uninterruptible power supply) akuston toiminnasta, verkkoliikennemääristä sekä valvottavien palvelin- ja verkkolaitteiden toimivuudesta. Opinnäytetyössäni toteutettavien valvomoiden tarkoituksena on helpottaa esimerkiksi edellä mainittujen asioiden valvontaa, sekä nopeuttaa vikatilanteisiin reagointia. Opinnäytetyön valvomot toimivat yrityksellä ennestään käytössä olleiden valvontatyökalujen avulla mahdollistaen näiden helpomman ja nopeamman käytön sekä paremman tilannekuvan ja proaktiivisen reagoinnin.

Opinnäytetyössäni kerron ensin lisää Verne Global Finlandin nykytilanteesta konesalien valvonnassa ja selitän, mistä tarve konesalivalvomoille on peräisin. Tämän jälkeen käyn läpi syvemmin konesalivalvomoon käytettyjen laitteiden ja sovellusten toiminnallisuutta. Tämän jälkeen käydään läpi asennuksessa käytettävät laitteet ja vaatimukset, sekä läpi itse konesalivalvomon käyttöönotto.
Opinnäytetyössä esitettävissä kuvissa on piilotettu IP-osoitteita sekä muita tunnistettavia ja salassa pidettäviä tietoja tietoturvan takaamiseksi.

1.2 Verne Global Finland

Verne Global Finland on vuonna 2011 perustettu yritys, jonka keskeisin toiminta-ala on konesalitoiminta. Yrityksellä on kolme eri konesalia, jotka yritys on nimennyt: The Rock, The Deck ja The Air. Yrityksen ensimmäinen konesali The Rock sijaitsee Ulvilassa olevassa kallioluolastossa, jonka yritys hankki aloittaessaan toimintansa vuonna 2011. The Deck -konesali sijaitsee Tampereella ja sen yritys hankki vuonna 2018. The Air on vuonna 2020 pääkaupunkiseudulle rakennettu cloud delivery center.

Verne Global Finland tarjoaa asiakkailleen useita eri palveluita, joista tärkeimmät ovat colocation, public-, HCI-, Private- ja Shared platform -pilvipalvelut. Verne Global Finlandin asiakkaat voivat olla esimerkiksi IT-palveluntarjoajia, ohjelmistoalan yrityksiä ja pilvipalvelujen tuottajia.

2 NYKYTILANNE

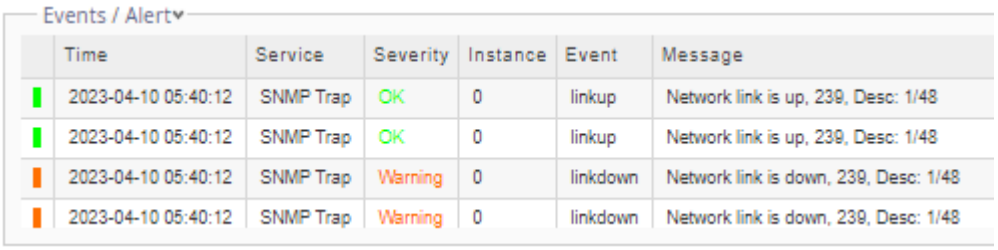
Verne Global Finlandin konesalien toiminnasta vastaa yrityksen operatiivinen henkilökunta, joka koostuu lähinnä verkkoasiantuntijoista, ICT-tukihenkilöistä ja järjestelmäasiantuntijoista. Operatiivisen henkilökunnan käytössä on useita työkaluja, joilla konesalien toimintaa voidaan valvoa sekä hallinnoida. Konesaleista valvotaan esimerkiksi palvelinten ja verkkolaitteiden toimivuutta, verkkoliikenteen määrää, konesalien lämpötiloja ja UPS-akuston kapasiteettia sekä toimivuutta.

Operatiivisesta henkilökunnasta aina vähintään yksi henkilö toimii varallaolijana, jonka tehtävänä on huolehtia konesaliympäristön valvonnasta saataviin hälytyksiin reagoinnista ympäri vuorokauden. Varallaolijan ei kuitenkaan tarvitse olla koko varallaolovuoroaan työpaikalla. Konesalien valvontaa on automatisoitu siten, että jos esimerkiksi palvelin tai verkkolaite rikkoutuu tai kokee muita häiriöitä, laitteen valvonta lähettää varallaolijalle tekstiviestin, josta varallaolijalle käy ilmi, mikä laite on rikkoutunut tai millaisia häiriöitä laite kokee. Varallaolijan on siis pystyttävä siirtymään konesalille määrätyssä ajassa. Mikäli päivystäjä itse asuu liian kaukana konesalista, on varallaolijalle nimettävä takapäivystäjä, jonka tehtäviin ei kuulu suoranaisesti valvoa konesalien toimintaa, vaan tarvittaessa lähteä konesalille korjaustoimenpiteisiin. Koska Verne Global Finlandilla on useita konesaleja kaukana toisistaan ja kerrallaan vain on yksi varallaolija, tarvitsee muiden konesalien operatiivisesta henkilökunnasta aina yhden toimia takapäivystäjänä.

		Start time	End time	Site	Equipment	Service
		05:40	05:40	0000-Ficolo Ulvila	[redacted]	SNMP Trap
		04:47	04:47	0000-Ficolo Ulvila	[redacted]	SNMP Trap
		02:45	02:46	[redacted]	[redacted]	Juniper vMX Route Monitoring
		02:45	02:45	[redacted]	[redacted]	Juniper vMX Route Monitoring
		02:44	02:44	[redacted]	[redacted]	Juniper vMX Route Monitoring

Kuva1: Lista automaattisen konesalilaitteiston valvonnan saamista hälytyksistä. Asiakkaiden laitteiden nimet piilotettu.

Kuvassa yksi on lista yhden automaattisen konesalivalvontaa suorittavan palvelun saamista hälytyksistä. Listassa näkyy aika, kun hälytys on tapahtunut, ”site” eli konesali, asiakas ketä hälytys koskee, laitteen nimi ja palvelu tai protokolla, joka hälytyksen aiheutti.


Events / Alert

Time	Service	Severity	Instance	Event	Message
2023-04-10 05:40:12	SNMP Trap	OK	0	linkup	Network link is up, 239, Desc: 1/48
2023-04-10 05:40:12	SNMP Trap	OK	0	linkup	Network link is up, 239, Desc: 1/48
2023-04-10 05:40:12	SNMP Trap	Warning	0	linkdown	Network link is down, 239, Desc: 1/48
2023-04-10 05:40:12	SNMP Trap	Warning	0	linkdown	Network link is down, 239, Desc: 1/48

Kuva 2: Lista kuvan yksi listan ylimmäisen laitteen hälytyksistä.

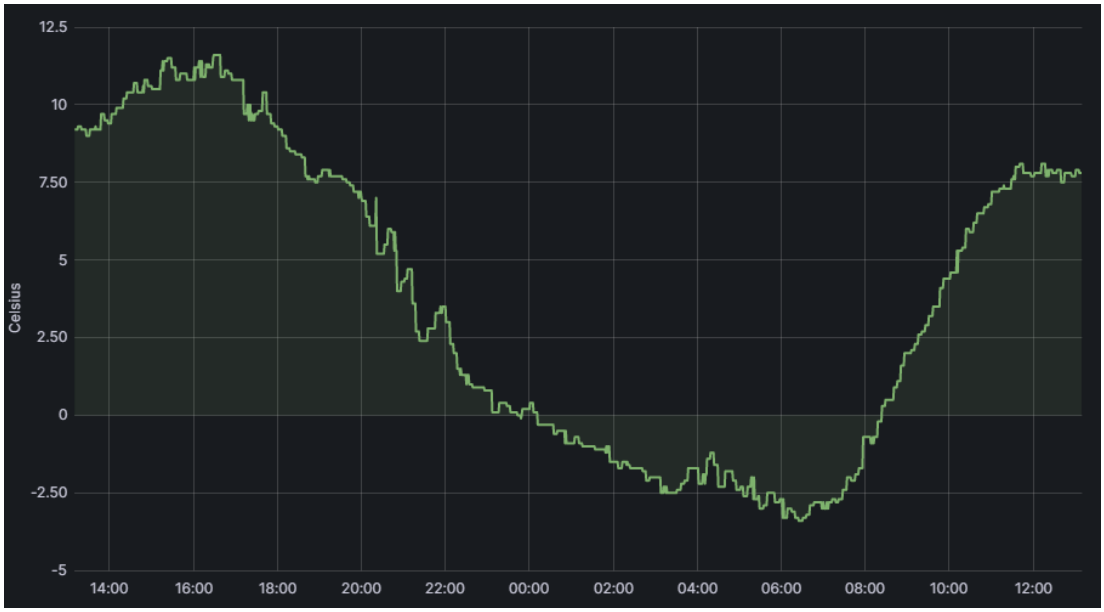
Kuvassa kaksi on nähtävillä vielä tarkemmin, miltä laitteen aiheuttama hälytys voi näyttää. Listasta on nähtävillä tarkka aika, jolloin hälytys on tapahtunut, palvelu, joka hälytyksen on aiheuttanut, sekä tarkempi tieto hälytyksen aiheuttajasta. Kuvassa kaksi hälytykset ovat aiheutuneet niin sanotusta porttifläpistä. Tämä on havaittavissa hälytysten kellonajoista, jotka ovat identtisesti samat. Porttifläppi on tilanne, jossa kytkimen portin linkki menee alas ja nousee lähes heti takaisin ylös. Linkin ollessa alhaalla data ei kulje kytkimen ja laitteen välillä. Porttifläpit ovat yksi yleinen hälytysten aiheuttaja, ja ne voivat olla merkki huonosta kaapelista tai kytkinportin toisessa päässä olevan laitteen viasta. Samalla periaatteella on nähtävissä myös, jos kytkinportin linkki putoaa, eikä nousekaan takaisin ylös. Molemmat tilanteet ovat lähtökohtaisesti vakavia ja vaativat lisäselvityksiä linkin putoamisen aiheuttajan selvittämiseksi.

Konesalien hälytyksiin reagoinnista toimistoaikana vastaa aina ensisijaisesti nimetty henkilö, mutta myös muu operatiivinen henkilökunta seuraa konesalien olosuhteita ja hälytyksiä toimistoaikana. Kuitenkin edelleen vain varallaolija vastaanottaa automaattiset häiriöviestit tekstiviestillä. Muut operatiivisen henkilökunnan jäsenet joutuvat pitämään silmällä konesaleja valvovaa järjestelmää, josta hekin voivat nähdä järjestelmän lähettämät virheilmoitukset.

Henkilökunnan käytössä on myös konesalien eri olosuhteita mittaava graafi palvelu Grafana, joka visualisoi konesalin antureista tietokantaan tallennetun

pistedatan avulla erilaisia kaavioita, joista on yleensä helposti nähtävillä konesalissa mitatut normaalista poikkeavat arvot.

Grafanassa on mahdollisuus käyttää hälytysominaisuutta, jonka avulla voidaan luoda erilaisia kriiteereitä, joiden täyttyessä Grafana lähettää tilanteesta hälytyksen (Grafana N.d.). Verne Global Finland ei kuitenkaan käytä Grafanaa hälytysten luomiseen, vaan Grafana vain visualisoi tilannetta reaaliajassa. Grafanassa ei kuitenkaan ole mitään sellaista, mitä ei valvottaisi myös automaattisesti, joten asetetuista hälytysrajoista poikkeavista arvoista esimerkiksi lämpötiloissa, saa varallaolija ilmoituksen automaattiselta valvonnalta. On kuitenkin hyödyksi nähdä myös muutokset, jotka eivät välttämättä ylitä hälytysrajoja. Näin voidaan esimerkiksi reagoida aikaisemmin mahdollisissa ongelmatilanteissa. Lisäksi on mahdollista, että jokin ongelma, joka ei vielä aiheuta hälytystä, on nähtävissä jo Grafanan kaavioista; tämä myös parantaa ongelmiin reagointia.



Kuva 3: Grafana ulkolämpötilaa kuvaava kaavio.

Kuva kolme avaa hieman minkälaista informaatiota Grafana -palvelu sisältää. Kuvassa on nähtävillä Ulvilan konesalin ulko-oven läheisyydessä sijaitsevan lämpötila-anturin antaman lämpötilan kehityksen vuorokauden aikana. Samalla periaatteella Grafanassa on nähtävissä esimerkiksi lämpötiloja eri

puolilta konesaleja. Konesalien lämpötilan kaavioista voidaan havaita, mikäli konesalin lämpötilat lähtevät eroamaan normaaleista arvoista, tällaiset mahdolliset erot voivat johtua esimerkiksi jäähdytyslaite viasta.

Grafana piirtää myös kaavioita UPS-akuston kapasiteetista. Normaali olosuhteissa kapasiteetti on 100%. Sähkökatkossa, kun sähkönsyöttö konesaliin sähköverkosta katkeaa, voidaan havaita UPS-akuston kapasiteetin lasku, ennen kuin konesalien varavoimageneraattorit lähtevät käyntiin ja aloittavat sähköntuoton. On kuitenkin tärkeä huomioida, että automaattinen valvonta havaitsee sähkökatkoksen ja UPS-akuston kapasiteetin varaan siirtymisen välittömästi, ja informoi siitä automaattisesti varallaolijaa tekstiviestillä, joten Grafana ei ole ensisijainen palvelu, josta vastaavat ongelmat tulevat ilmi. Grafana kuitenkin tukee automaattista valvontaa, sekä helpottaa myös muuta operatiivista henkilökuntaa, joka ei sillä hetkellä toimi varallaolijana, ja jotka eivät saa automaattisen valvonnan lähettämiä tekstiviestihälytyksiä. Grafanan graafeilla on tärkeä rooli oikeanlaisen tilannekuvan muodostamisessa esimerkiksi poikkeamatilanteissa ja täten se toimii myös poikkeamatilanteiden päätöksentekoa ohjaavana työkaluna.

Datakeskuksista mitataan suuria määriä erilaista dataa, esimerkiksi olosuhdevalvontaa, kuten lämpötiloja ja ilmankosteutta, virrankulutusta, verkkoliikennettä ja UPS-akustoa. Grafanan tehtävä on tuoda mitattu data helposti nähtäville yhteen palveluun kaikista konesaleista ja erilaisista valvonta rajapinnoista. Mittauksista tietokantaan tallennettuun dataan sisältyy paljon kriittistä tietoa konesalien toimivuudesta ja siten datan tuominen helposti nähtäville on tärkeää. Grafana -palvelusta on siis suuri apu konesalien valvonnalle. Konesalivalvomoissa voidaan tuoda palveluita, kuten Grafanaa, vielä paremmin operatiivisen henkilökunnan nähtäväksi helpottaen konesalien valvontaa.

3 TAVOITTEET

Internetissä sijaitsee valtavia määriä dataa. Usein puhutaan, että data sijaitsee ns. pilvessä. Tämä pilvi on kuitenkin harhaanjohtava käsite, sillä kaikki data kuitenkin sijaitsee ihan tavallisilla fyysisillä laitteilla, jotka eivät eroa kovinkaan paljon tavallisesta tietokoneesta. Pilvellä usein tarkoitetaankin datakeskuksia eli paikkoja, joissa iso määrä internetissä olevasta datasta sijaitsee. (Koistinen, 2015).

Verkkopankeista sosiaaliseen mediaan lähes kaikki data sijaitsee datakeskuksissa, eli kun käytät verkkopankkiasi, käytät samalla tiedostamattasi datakeskuksen palveluita. Kun verkkopankki ei jostain syystä toimi, on yhtenä mahdollisuutena se, että verkkopankin datakeskuksessa on käynnissä vikatilanne. Datakeskukset ovat siis lähes aina osa valtioiden kriittistä infrastruktuuria, joka tarkoittaa, että datakeskusten on oltava toiminnassa jatkuvasti ilman palvelukatkoksia (Huoltovarmuuskeskus N.d.).

Palvelut pyritään aina tuottamaan ilman palvelukatkoksia, mutta johtuen useammasta eri tekijästä palvelukatkoksilta ei aina voida välttyä. Palvelukatkoksien aiheuttajana voivat olla suunnitellut huoltotoimenpiteet, kuten järjestelmäpäivitykset tai aiheuttajana voi myös olla täysin odottamaton vikatilanne, jossa esimerkiksi jokin datakeskuksen laite hajoaa ja kyseisen laitteen kahdennus ei toimi suunnitellulla tavalla tai laitetta ei ole riittävällä tavalla kahdennettu. On siis erittäin tärkeää, että mahdollisia palvelukatkoksia on mahdollisimman vähän ja siinä tilanteessa, jossa niitä ilmenee, ne olisivat mahdollisimman lyhyitä. Datakeskusvalvomoiden tavoitteena on edistää datakeskuksen toimivuuden varmistamista ja mahdollisiin vikatilanteisiin reagointia joko ennen kuin vikatilanne aiheuttaa palvelukatkoksia, tai auttaa paremman tilannekuvan muodostamisessa häiriön aikana ja täten nopeuttaa häiriön ratkaisemista.

Tässä opinnäytetyössäni asennettavien konesalivalvomoiden pääasiallinen tehtävä on parantaa, nopeuttaa ja helpottaa Verne Global Finlandin operatiivisen henkilökunnan mahdollisuuksia valvoa konesalien toimintaa, sekä

proaktiivisen havainnoinnin tehostaminen. Ennen valvomoiden asennusta operatiivisen henkilökunnan oli itsenäisesti kirjauduttava omilla tunnuksilla konesalia valvoviin järjestelmiin ja pitää silmällä siellä olevia hälytyslistoja sekä kaavioita samalla, kun henkilö suorittaa omia päivittäisiä työtehtäviään. Tämä ei ole ideaali tilanne, sillä valvontaa suorittavia palveluita on useita, ja niissä on lukuisia eri valvontaan tarvittavia sivuja, listoja sekä kaavioita. On siis mahdotonta pitää kaikkia vaadittavia ikkunoita auki työpisteen näytöillä samalla kun henkilö suorittaa lisäksi omia työtehtäviään.

Valvomot sijaitsevat yrityksen toimistotiloissa, joissa iso määrä myös operatiivista henkilökuntaa suorittaa omia työtehtäviään. Valvomoiden avulla henkilökunnan ei tarvitse avata omalle työkoneelleen valvontaa suorittavia sovelluksia, jolloin he voivat paremmin keskittyä omiin työtehtäviinsä. Valvomot ovat sijoitettu paikkoihin, joista henkilökunta näkee valvomoiden näytöt helposti omalta työpisteeltään, sekä kävelleessään työpisteeltään muualle yrityksen tiloihin. Tällöin henkilökunta voi helposti ja nopeasti vilkaista valvomoiden näytöistä konesaleja valvovien sovelluksien kaaviot ja muut tiedot.

Verne Global Finlandilla on kaksi toimistotilaa, yksi pääkaupunkiseudulla sijaitsevan The Air -konesalin kanssa samassa rakennuksessa, ja toinen Porissa lyhyen ajomatkan päässä Ulvilan konesalista. Molemmissa toimistotiloissa on omat valvomot. The Air -konesalin yhteydessä sijaitsevassa toimiston valvomossa valvotaan lähinnä The Air -konesalin toimintaa, kun taas Porin toimiston valvomossa on nähtävissä kaikkien konesalien toimintaan liittyvää tietoa.

On kuitenkin tärkeä huomioida, ettei valvomoiden tarkoituksena tässä opinnäytetyössä ole korvata yrityksen muita konesalien valvontaratkaisuita, vaan tuoda nuo ennestään käytössä olevat ratkaisut paremmin ja helpommin henkilökunnan nähtäväksi. Valvomot eivät siis itsessään valvo konesalien toimintaa, eikä valvomoihin liity mitään automaattista valvontaa. Valvomot toimivat uutena visualisoinnin työkaluna valvontaa suorittavien sovellusten sekä yrityksen henkilökunnan välillä.

4 THICK, THIN JA ZERO CLIENT

4.1 Mikä on zero client

Tietokoneet voidaan jakaa kolmeen ryhmään, thick clients, thin clients ja zero clients, niiden autonomisen toimivuuden perusteella, eli kuinka paljon tietokone kykenee suorittamaan toimenpiteitä yksinäisesti ilman muiden tietokoneiden, esimerkiksi palvelinten avustusta. Aina ei kuitenkaan ole täysin selvää mihin ryhmään tietokone kuuluu. Esimerkiksi Applen iPad voidaan luokitella thick clientiksi sen tehokkaan käyttöjärjestelmän ansioista, mutta samalla voidaan sanoa, että se on thin client, koska laite käyttää paljon pilvipalveluita ja pilveen yhdistettyjä sovelluksia. (CDW, 2022).

4.1.1 Thick client

Thick clients, joita kutsutaan myös heavy clients tai rich clients, ovat verkkoon kytkettyjä tietokoneita, joissa on kaikki tietokoneelle tyypilliset ominaisuudet riippumatta keskuspalvelimesta. Esimerkiksi normaali pöytätietokone tai kannettava tietokone luokitellaan usein thick clientiksi.

Vaikka thick client toimii täysin ilman verkkoyhteyttä, se on kuitenkin luokiteltu vain asiakkaaksi (Client). Verkkoyhteyden avulla thick client voi olla yhteydessä verkon kautta palvelimeen, joka voi tarjota asiakkaalle ohjelmia ja tiedostoja, joita ei ole tallennettu asiakkaan paikalliseen kiintolevyyn. Työpaikat usein tarjoavat työntekijöilleen thick client -ryhmän tietokoneita, joilla on mahdollista käyttää paikallisen palvelimen tiedostoja tai käyttää konetta ilman verkkoyhteyttä. Thick client -ryhmän tietokonetta, joka ei ole verkossa, kutsutaan usein työasemaksi. (TechTerms.com. 2006).

4.1.2 Thin client

Thin client eroaa thick clientista eniten siinä, että thin client käyttää palvelimessa olevia resursseja oman kiintolevyn sijaan. Thin client muodostaa yhteyden palvelimeen, jossa suurin osa käyttäjän tarvitsemista sovelluksista, muistista ja tiedostoista sijaitsee. Thin client -koneessa kuitenkin on käyttöjärjestelmä asennettuna, mutta se ei kykene toimintaan ilman yhteyttä palvelimeen. (Fortinet. N.d).

Thin client -koneet ovat usein yritysmaailmassa thick client -koneita kustannustehokkaampi ratkaisu. Thin client -koneet mahdollistavat helpomman tietoturvan keskittämisen, sillä tietoturvamielessä ei tarvitse keskittyä yhtä paljon asiakaskoneisiin, vaan pystytään suojaamaan palvelinta, johon thin client -koneet ottavat yhteyden. (Forcepoint. N.d)

4.1.3 Zero client

Zero client eroaa thin clientistä siinä, että kun thin clienteissa on usein oma käyttöjärjestelmä ja sitä varten pieni määrä omaa tallennustilaa, zero clienteissa ei ole edes käyttöjärjestelmää, eikä ollenkaan omaa tallennustilaa tai prosessoria, vaan kaikki toiminnot tapahtuvat suoraan palvelimelta. Käynnistyessään zero client käyttää laiteohjelmistoa ja verkkoyhteyttä palvelimeen yhdistämiseen, jonka jälkeen se lataa kaiken tarvitsemansa tiedon palvelimelta suoraan omalle keskusmuistilleen oman kiintolevyn sijaan. Zero clientit eivät siis sisällä omaa käyttöjärjestelmää tai mitään asetuksia, vaan on kokonaan palvelimen vastuulla tunnistaa zero client ja päättää, mitä se tekee. (Onlogic blog. 2022).

Zero client -teknologia sopii erinomaisesti VDI (virtual desktop infrastrukture) ympäristöihin, joissa zero client -päätelaite toimii linkkinä käyttäjän ja palvelimella sijaitsevan virtuaalisen työpöydän välillä. Zero clienttejä voidaan käyttää myös mainosnäyttöjen hallintaan. Mainosnäytön sisälle asennettu zero client saa palvelimelta kuvan tai videon, jonka sitten zero client laittaa mainosnäytölle. Näin näytön sisältöä voidaan hallita etänä koska tahansa.

4.1.4 Zero clientin hyödyt

Zero client ja thin client jakavat useita hyötyjä keskenään, koska erot laitetyyppien välillä ovat pienet. Erot kuitenkin zero ja thin clienttien sekä thick clienttien välillä ovat suuret. Riippuukin paljon tilanteesta ja käyttötarkoituksesta, joihin laitetta suunnitellaan käytettäväksi, ovatko erot hyötyjä vai haittoja. Joissakin tilanteissa esimerkiksi Zero ja thin clienttien riippuvuus palvelimesta tuo käyttäjälle ja yritykselle suuriakin hyötyjä, mutta on mahdollista, että toisille käyttäjille ja yrityksille erot tuovatkin haittoja.

Kuitenkin Zero clienttien hyötyinä yleisesti pidetään niiden kustannustehokkuutta. Riippuen laitteen mallista on mahdollista, että jokainen thin tai zero client maksavat käyttäjää kohti vähemmän kuin perinteiset thick client -koneet. Mikäli yrityksellä ei ole käytössä yksittäiseen työasemaan sidottavia ohjelmistolisenssejä, käyvät zero ja thin client -koneet halvemmiksi.

Thin ja zero client -koneita on myös huomattavasti helpompi hallita kuin perinteisiä thick client -työasemia. Koska thin ja zero client käyttävät ohjelmistoja suoraan palvelimelta, riittää kun ohjelmistoa ylläpidetään ja hallitaan palvelimelta, eikä silloin tarvitse esimerkiksi huolehtia jokaisen työaseman ohjelmistopäivityksistä erikseen. Tämä tietenkin vähentää huomattavasti IT-tuen vaatimia resursseja. (Knerl, 2021).

Koska thin ja zero clientit käyttävät ohjelmistoja keskitetyllä palvelimella ja jopa käyttöjärjestelmiä zero clienttien kohdalla, paranee myös tietoruvallisuus huomattavasti. Kun thick clienttien kanssa yrityksen täytyy pitää parempaa huolta jokaisen yksittäisen työpisteen tietoturvasta, thin ja zero clienttien kanssa usein on mahdollista keskittyä enemmän palvelimen ja vähemmän jokaisen yksittäisen työpisteen tietoturvallisuuteen. Koska thin ja zero clienttien käyttämä data sijaitsee palvelimella itse työpisteen tallennustilan sijaan, käytettävän datan suojaaminen on helpompaa ja se pysyy paremmin suojassa, kun sen ei tarvitse koskaan poistua palvelimelta. (Zeetim, 2020).

4.1.5 Zero clientin rajoitukset

Zero client ei suinkaan taivu kaikkeen. Koska zero client ei kykene toimimaan yksinäisesti ilman yhteyttä palvelimeen, voi esimerkiksi pienyritykselle olla kustannustehokkaampaa käyttää thick client -tietokoneita, välttyen palvelimen hankinta- ja ylläpitokustannuksilta. Myös mikäli yrityksessä ei ole palvelin- ja zero client -teknologiaa osaavaa henkilökuntaa, voi pienyritykselle olla mahdotonta ottaa käyttöön ja ylläpitää zero client -pohjaista järjestelmää.

Myös kasvanut etätöiden määrä saattaa olla ongelma zero client -pohjaisen järjestelmän käyttöönotossa. Yritykselle on huomattavasti helpompaa tarjota työntekijöille kannettavia tietokoneita, joilla työnteko voi olla mahdollista täysin ilman yhteyttä yrityksen palvelimille, tai mahdollisesti virtuaalisen erillisverkon (VPN) avulla ottaa yhteys mistä vain yrityksen palvelimelle. Zero client kuitenkin vaatii jatkuvan lähiverkkoyhteyden palvelimeen pystyäkseen mihinkään toimintaan.

Zero clienttin tehokkuus on myös täysin riippuvainen verkkoyhteyden nopeudesta ja laadusta. Hidas verkkoyhteys haittaa huomattavasti zero clienttien toimivuutta, kun liikenne zero clientin ja palvelimen välillä takkuilee, vaikuttaa zero client toimivan hitaasti, vaikka kyse onkin verkkoyhteyden nopeudesta. Lisäksi mahdolliset verkon katkeamiset ovat iso ongelma zero clienttien kanssa. Mikäli verkkoyhteys palvelimen ja zero clientin välillä on poikki, ei zero client kykene toimimaan. (Rajesh. 2014).

5 KONESALIVALVOMO

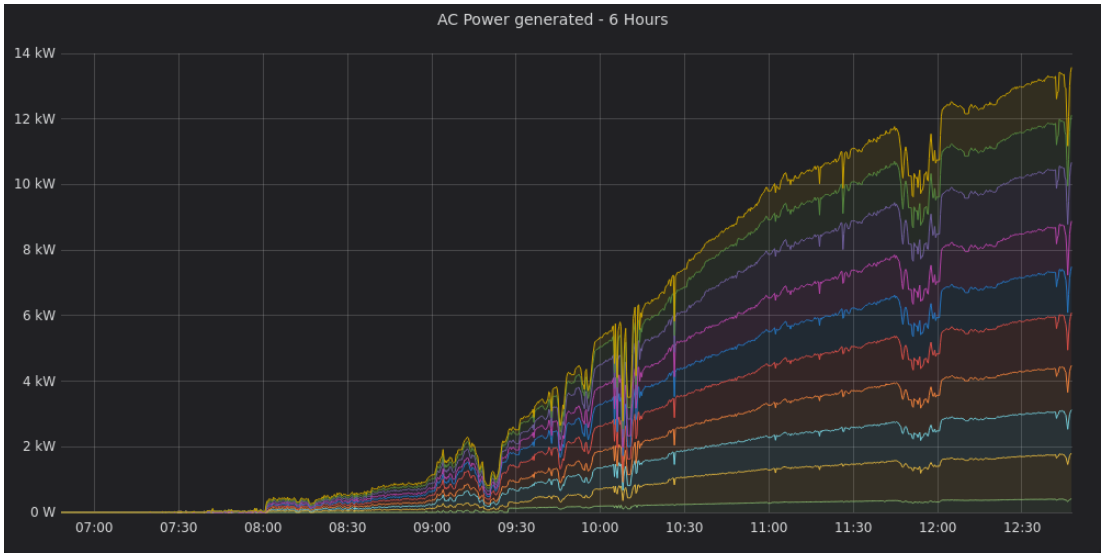
Konesalit ovat usein osa yritysten ja jopa valtioiden kriittistä infrastruktuuria, mikä tarkoittaa, että niiden tulisi olla jatkuvasti toiminnassa ja häiriöajat tulisi olla mahdollisimman pienet. Tämän vuoksi konesalien jatkuva valvonta on äärimmäisen tärkeää, jotta mahdolliset ongelmatilanteet voidaan havaita jo ennen kuin niistä koituu haittaa konesalin toimivuudelle, tai että jo olemassa olevan vian diagnosointiprosessi nopeutuu ja saadaan pidettyä mahdolliset häiriöajat mahdollisimman lyhyinä. Konesalien valvontaa voidaan suorittaa esimerkiksi SNMP- (simple network management protocol) protokollalla, ping-valvonnalla ja datan keruu konesaleihin asennetuista olosuhdeantureista. Konesalivalvomon tehtävä on usein tukea muuta olemassa olevaa valvontaa, tai tuoda olemassa oleva valvonta paremmin nähtäville sitä tarvitseville henkilöille. Jos esimerkiksi laite lopettaa vastaamasta ping-kyselyihin, muodostaa ping-valvonta tästä hälytyksen, joka on nähtävissä valvomossa.

Valvomoiden tehtävä on toimia keskeisenä paikkana valvonta- ja johtamiskäytännöille. Valvomo on paikka, jossa teknikot ja johtajat hoitavat jokapäiväistä toimintaa, sekä ylläpitävät ja toteuttavat tuotannon valvontaa ja kriisitoimintoja tietylle kokonaisuudelle. (Vestal, 2022).

Tässä opinnäytetyössäni toteutettava valvomon idea ei ole toimia konesalin pääasiallisena valvontatyötyökaluna. Valvomo on sijoitettu toimistoissa näkyville paikoille, joista kaikkien työntekijöiden on helppo nähdä valvomon näytöt ja siten helpompi monitoroida konesalien toimintaa. Valvomon idea ei tässä ole, että se on miehitetty vuorokauden ympäri, vaan sen tehtävä on toimia tukena jo olemassa oleville datakeskuksen valvontatyökaluille, ja helpottaa yrityksen työntekijöiden konesalien valvontatyötä ja antaa työkalut parempaan proaktiiviseen reagointiin.

Tämän opinnäytetyön valvomon pääsääntöinen valvonta tapahtuu Grafanan avulla. Grafana piirtää esimerkiksi konesalien lämpötiloista, virrankulutuksesta, tietoliikenteen määrästä omat graafit joka datakeskuksesta, laitetilasta

ja yksittäisestä sensorista. Graafien perusteella on helppo ja nopea tehdä havaintoja esimerkiksi suurista lämpötilavaihteluista. Tietoliikenteen tai palomuurin graafeista on mahdollista havaita esimerkiksi DDoS (palvelunestohyökkäyksiä), jolloin niihin voidaan reagoida mahdollisimman nopeasti. Grafanaa käytetään myös seuraamaan Ulvilan datakeskuksen katolla sijaitsevan aurinkovoimalan tuotantoa. Alla kuvassa näkyy kuinka auringon noustessa sähköntuotto alkaa. Graafissa havaittavat pudotukset ovat esimerkiksi pilvien varjojen aiheuttamia pudotuksia sähköntuotannossa.



Kuva 4: Ulvilan datakeskuksen aurinkovoimalan tuottama sähkö graafina.

Kuvasta neljä käy hyvin ilmi, miten graafit helpottavat esimerkiksi edellä mainittujen asioiden, kuten konesalien lämpötilojen valvontaa. Suuret vaihtelut lämpötiloissa eivät yleensä ole normaaleja, vaan ne saattavat olla merkki esimerkiksi jäähdytyslaitteiston vikatilasta. Graafien avulla pienetkin vaihtelut ovat helposti havaittavissa.

6 TOTEUTUKSESSA KÄYTETYT LAITTEET

6.1 Monitors AnyWhere

Valvomon hallintaan otettiin Monitors AnyWhere:n MAWi -sovellus. Sovellus valittiin, koska se oli opinnäytetyöni toimeksiantajan työntekijälle jo entuudestaan tuttu ohjelmisto, ja yrityksellä oli käytettävissä lukuisia zero client -koneita.

MonitorsAnyWhere MAWi (web-based interface) -sovelluksen avulla käyttäjät saavat vietyä sisältöä useille eri näytöille näyttöjen olinpaikasta riippumatta. MAWin avulla näyttöjen sisältöä on helppoa ja yksinkertaista hallita verkkopohjaisen hallintakonsolin avulla. MAWi on on-premise -ratkaisu, jolla useat näytöt voidaan liittää palvelimeen LANin, WANin tai internetin kautta. MAWi hallinta palvelin voidaan asentaa PC tietokoneelle sekä joko fyysiselle tai virtualisoidulle palvelimelle. (MonitorsAnyWhere N.d).

MonitorsAnyWhere MAWi zero mahdollistaa HDMI over LAN teknologian avulla HDMI-kuvasignaalin viennin LAN-verkon yli zero client -laitteelle, johon liitettyyn näyttöön saadaan kuva. HDMI-kuvasignaali LAN-verkon yli mahdollistaa näyttöjen lisäämisen palvelimeen ilman, että näytöt ovat fyysisesti kiinni HDMI- tai VGA-kaapelilla palvelimessa. Tämä mahdollistaa suuretkin välimatkat palvelimen ja näyttöjen välille. Teknologia alun perin suunniteltiin USB laitteiden kuten tulostimien jakamisen verkon yli. (MonitorsAnyWhere N.d).

MAWi server -järjestelmävaatimukset:
Käyttöjärjestelmä: Windows 10/11, Server 2012/16/19/22
MAWi server voidaan asentaa joko fyysiselle palvelimelle tai virtuaalikoneelle
Prosessori: Intel dual core tai vastaava AMD prosessori, uusimman generaation Intel Core i5 on suositeltu, virtuaalikoneella vähintään 2 vCPU prosessoria.
Muisti: vähintään 4GB
(MonitorsAnyWhere, N.d.).

6.2 Zero client

Zero client -teknologia valittiin, koska se helpottaa konesalivalvomoiden ylläpitoa. Teknologian ansioista itse konesalivalvomoissa ei tarvitse tehdä juurikaan mitään ylläpitoon liittyviä toimenpiteitä, vaan lähes kaikki toimenpiteet voidaan tehdä etänä palvelimilla, joihin zero client -laitteet ovat yhdistetty. Tämä myös lisää kustannustehokkuutta, kun molempia konesalivalvomoita voidaan hallita ja ylläpitää samasta keskitetystä paikasta, vaikka itse konesalivalvomot sijaitsevatkin kaukana toisistaan.

Zero clientit toimivat tässä konesalivalvomossa HDMI over LAN teknologian avulla tuoden niitä hallitsevilta palvelimilta HDMI video signaalin verkon yli näytöille. Zero client -laitteiden kautta ei tässä toteutuksessa pystytä juurikaan hallitsemaan näytöillä näkyviä asioita, vaan näyttöjen hallinta tapahtuu MAWi server -ohjelmiston kautta. Joten selvänä rajoituksena tässä toteutuksessa on, että konesalivalvomossa ei suoraan pystytä vaikuttamaan konesalivalvomossa nähtäviin asioihin, mikäli konesalivalvomon asioita halutaan muuttaa, on aina kirjauduttava MAWi server -ohjelmistoon. Rajoituksen vaikutus on kuitenkin pieni tämän opinnäytetyön toteutuksessa, jossa ei ole tarvetta muokata konesalivalvomon näyttöjen sisältöä kovin usein, ja tilanteissa, joissa näyttöjen sisällön vaihtaminen tulee tarpeen, onnistuu sisällön vaihtaminen edelleen nopeasti ja yksinkertaisesti MAWi server -ohjelmiston avulla.

Asennuksessa käytettiin toimeksiantajan olemassa olevia Phistek ZE6000 zero client -koneita. Jokaisella valvomon näyttöä hallitsee oma zero client, joten laitteiden määrä riippuu siitä, montako näyttöä valvomoon halutaan. Phistek ZE6000 zero client tukee DVI-videosignaalia. Lisäksi laitteessa on 1 Ethernet portti, 4 USB porttia sekä kuuloke ja mikrofoni 3.5 mm portit.

6.3 Palvelinlaitteisto

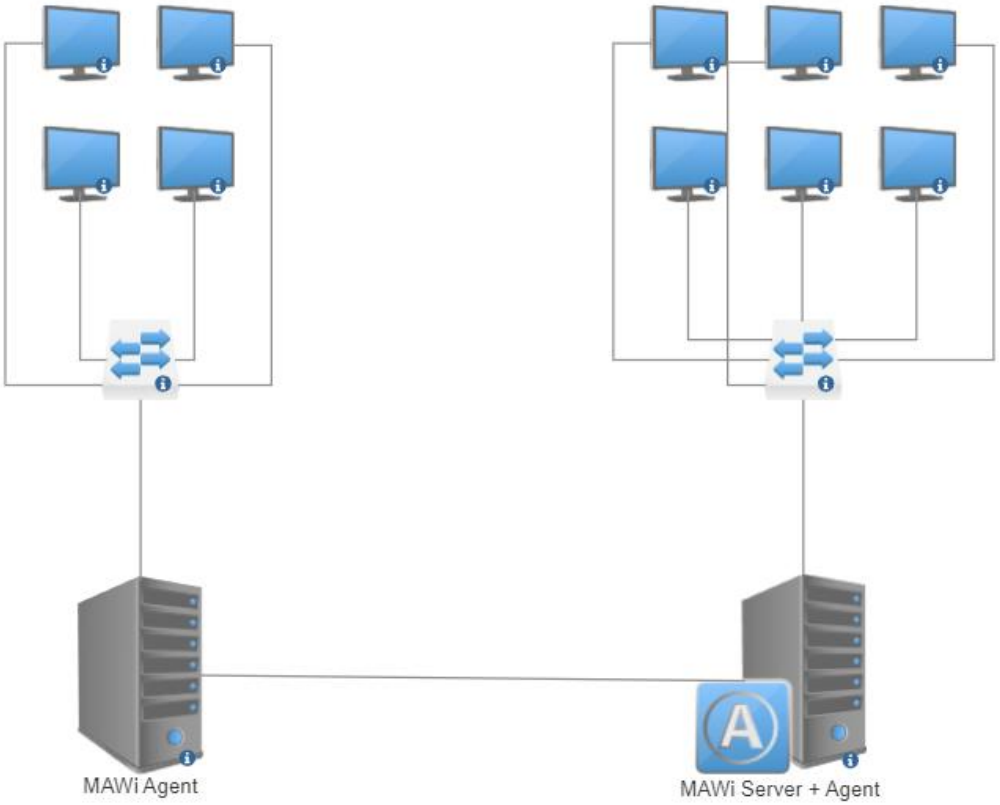
Palvelimina käytettiin kahta toimeksiantajan varastosta saatua palvelinta. Asennuksessa tarvittiin kahta palvelinta, koska käytettävä käyttöjärjestelmä Windows Server 2019 tukee maksimissaan vain kymmentä eri näyttöä. Mikäli

palvelimeen lisätään enemmän kuin 10 näyttöä, ei uusia näyttöjä tule näkyviin Windowsin näyttöasetuksiin, eikä näyttöihin tule kuvaa. MAWi -sovelluksiin ylimääräiset näytöt tulevat näkyviin, mutta ne ovat käytettävissä vain MAWi spacewall -ominaisuudella, joka luo useista näytöistä yhden ison näytön.

Asennuksen testausvaiheessa kokeiltiin myös, miten MAWi-sovelluksien toimii virtualisoidussa palvelimessa VMware-ympäristössä. VMwaren virtuaalikonsoli ei kuitenkaan toiminut odotetusti, kun palvelimessa oli käytössä useita näyttöjä. Virtuaalikoneen etähallintakonsolin hiiren kursori ei ollut synkronoitu todellisen kursorin kanssa, jolloin pienikin hiiren liike todellisuudessa siirsi kursoria etäkonsolissa huomattavasti suuremman matkan, tehden palvelimen käytöstä erittäin vaikeaa. Windows käyttöjärjestelmän remote desktop protocol (RDP) -etähallintaominaisuus ei sovi hyvin tähän toteutukseen, koska RDP yhteyden muodostuessa palvelimen muut näytöt pimenevät ja sisäänkirjautunut käyttäjä uloskirjataan RDP-session ajaksi, jolloin valvomon näytöt lakkaavat toimimasta. Ongelma oli kuitenkin mahdollista kiertää käyttämällä virtuaalikoneen hallintaan jotain muuta työkalua, kuten esimerkiksi TeamViewer -sovellusta, jolloin hiiri toimi normaalisti. Opinnäytetyössäni ei kuitenkaan päädytty käyttämään tätä ratkaisua tietoturvasyistä.

Ensimmäinen fyysinen palvelin toimii MAWi server-palvelimena, johon asennetaan MAWi IIS (Internet Information Services) verkkopohjainen sovellus, SQL palvelin ja tietokanta, sekä MAWi agent -ohjelmisto. Ensimmäiseen palvelimeen on yhdistetty 10 näyttöä, jotka sijaitsevat yrityksen Porin toimipisteissä. Toiseen palvelimeen asennetaan vain MAWi agent, joka yhdistetään ensimmäisen palvelimen MAWi server -ohjelmistoon. MAWi agentin avulla saadaan palvelimeen 2 yhdistetyt näytöt MAWi serverin hallintaan, täten kiertäen Windows käyttöjärjestelmän 10 maksiminäytön rajan. Toiseen palvelimeen on yhdistetty yrityksen Vantaan toimipisteen näytöt.

7 ASENNUS JA KÄYTTÖÖNOTTO



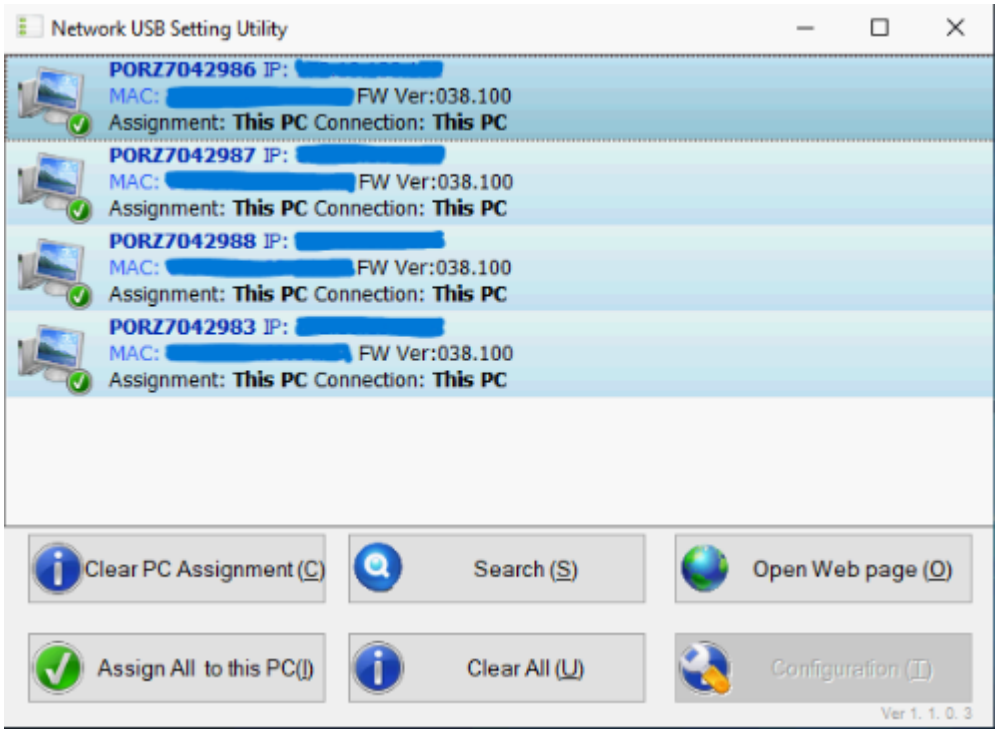
Kuva 5: Yksinkertaistettu verkkokuva. Näytöt kuvaavat samalla zero client laitteita.Yksi zero client jokaista näyttöä kohden.

7.1 Verkot

Asennuksessa käytettiin kolmea eri virtuaalilähiverkkoa (VLAN). VLAN 10 toimii palvelimien hallintaverkkona, joka mahdollistaa mm. etätyöpöytäsovelluksen, Internetin käytön sekä toimii verkkona MAWi server -palvelimelle. VLAN 10 avulla palvelin myös on yhteydessä yrityksen yksityisiin palveluihin, kuten esimerkiksi Grafanaan, joka ei ole Internetissä. VLAN 11 ja 12 toimivat verkkoina Porin (VLAN 11) ja Vantaan (VLAN 12) zero client -laitteiden ja niitä hallitsevien palvelimien välillä. Palvelin 1 hallitsee Vantaan zero client -laitteita ja palvelin 2 Porin zero client -laitteita.

7.2 Zero client -laitteiden yhdistäminen palvelimelle

Zero client -laitteiden yhdistäminen Windows-palvelimeen tapahtuu Network USB Utility -ohjelmalla.



Kuva 6: Network USB Utility. IP ja MAC osoitteet piilotettu.

Yllä kuvassa on palvelimen 1 Network USB Utility ohjelman ikkuna. Ikkunassa näkyy neljä eri zero client -laitetta, sekä niiden tämänhetkinen omistaja ja yhteys. Kun laitteita ollaan ensimmäistä kertaa yhdistämässä palvelimeen, laitteiden assignment ja connection kohdassa lukee ”Clear” tai ”Other PC”, jolloin laitteet eivät ole vielä käytettävän palvelimen hallussa. Jokaisen zero clientin tulee olla vapaa, eli niillä ei saa olla merkittynä assignment tai connection kohdassa ”Other PC”, jos näin on, pitää zero client vapauttaa Network USB Utility ohjelmasta painamalla Clear PC Assignment nappia. Zero clientin ollessa ”Clear” tilassa voidaan painamalla Assign to this PC nappia yhdistää zero client palvelimeen, nappi tulee näkyviin vasta kun zero client näkyy ohjelmassa ”Clear” tilassa.

Ohjelmalla voidaan myös muokata zero client -laitteiden nimitunnisteita sekä IP osoitteita. Haluttu laite tulee olla ”Clear”-tilassa ja valittuna, jonka jälkeen ohjelman ”Configuration”-nappi tulee saataville.

Mikäli zero client -laitteeseen on jo kytketty näyttö kiinni, tulee näyttö saman tien Windows palvelimen näyttöasetuksiin näkyville, ja näyttöön tulee Windows työpöytä. Zero client on nyt yhdistetty palvelimeen ja valmiina käytettäväksi.

7.3 MonitorsAnyWhere MAWi sovelluksen asennus

MAWi -sovelluksen asennuksessa on kaksi vaihetta. Ensimmäisessä vaiheessa asennetaan MAWi agent -ohjelmisto. Agent -ohjelman asennuksen yhteydessä on valittava valinnaiset MAWi zero -ajurit, joiden avulla MAWi agent hallitsee zero client -laitteita. MAWi agent asennetaan palvelimelle, jolle zero client -laitteet ovat yhdistetty. Koska tämän opinnäytetyöni projektissa molempiin kahteen käytössä oleviin palvelimiin on yhdistetty zero client -laitteet ja niiden takana olevat näytöt, tuli molempiin palvelimiin asentaa MAWi agent. Haluttaessa MAWi agentin asennuksen yhteydessä voidaan asentaa VLC-media player, videon toisto-ohjelmisto sekä PowerPoint-diaesitysohjelmisto.

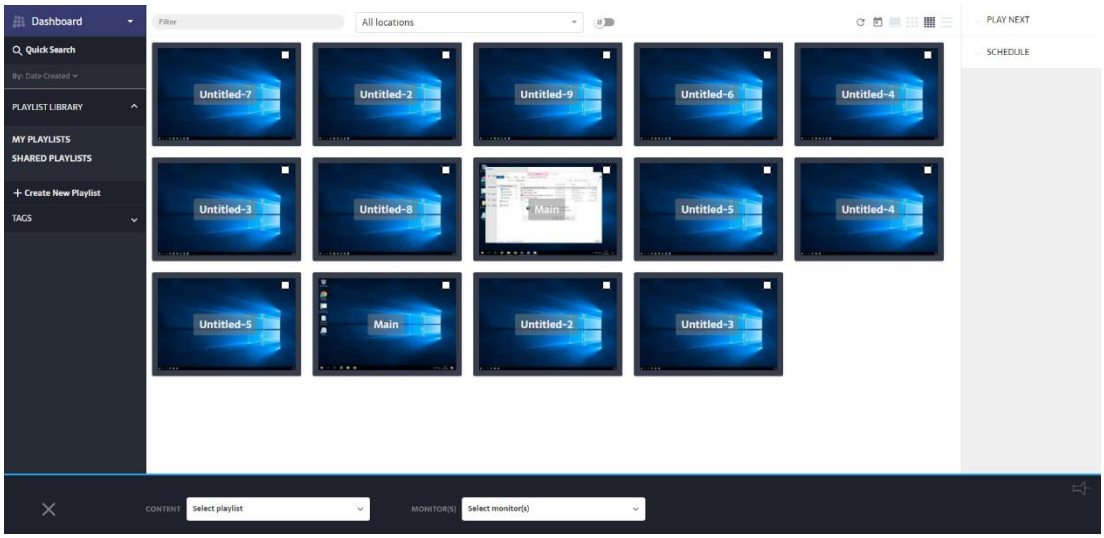
Toisessa vaiheessa asennetaan MAWi server -ohjelmisto. Tässä asennuksessa MAWi server asennetaan vain toiselle palvelimista. MAWi server -ohjelmiston yhteydessä voidaan asentaa MAWi server -ohjelmistolle tarvittava SQL-tietokantapalvelin, tai yhdistää jo olemassa olevaan SQL-tietokantapalvelimeen. Asennuksen yhteydessä luodaan MAWi server -ohjelmiston ylläpitokäyttäjä. Käyttäjän luomiseen tarvitaan sähköpostiosoite mahdollista salasanan palautusta varten. Sähköpostiosoite toimii myös käyttäjätunnuksena kirjautuessa MAWi server -ohjelmistoon, samalla käyttäjälle luodaan salasana.

MAWi server -asennuksen yhteydessä kannattaa ottaa rasti pois ruudusta, jossa kysytään, haluaako asennuksen suorittaa suositetuilla asetuksilla. Täten päästään varmistamaan, että MAWi server asentuu oikeaan IP-osoitteeseen. Mikäli palvelimessa on enemmän kuin yksi verkko, suosituilla asetuksilla

MAWi server asentuu helposti väärään verkkoon, jolloin yhteys palvelimien välillä, sekä yhteys MAWi server -hallintaan yrityksen hallintaverkosta ei toimi. Samassa yhteydessä voidaan myös halutessa vaihtaa asennuksen kansion sijainti kiintolevyllä.

Asennuksessa, jossa asennetaan pelkkä MAWi agent, korvautuu MAWi server asennusvaihe palvelimeen yhdistämisellä, asennus kysyy MAWi server -palvelimen IP-osoitetta sekä porttinumeroa, mikäli se on vaihdettu MAWi server -palvelimen asennuksen yhteydessä oletusasetuksen 60668-portista joksikin muuksi. Samassa yhteydessä voidaan jo testata, pystytäänkö muodostamaan yhteys palvelimeen, siksi onkin järkevää aloittaa asennukset MAWi server -palvelimella, jotta yhteys MAWi agent asennuksessa pystytään todentamaan, mutta agentin asennus onnistuu ilmankin yhteyttä MAWi server -palvelimelle.

7.4 MonitorsAnyWhere -sovelluksen konfigurointi

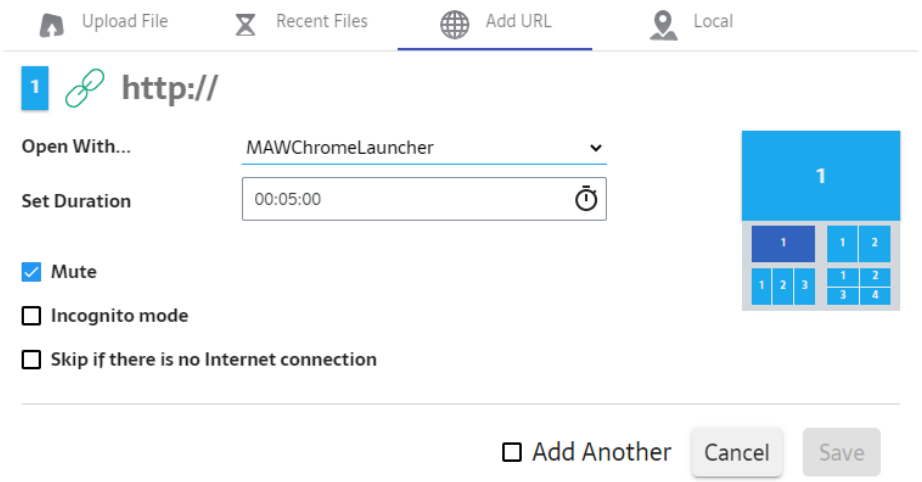


Kuva 7: MonitorsAnyWhere MAWi server -hallintaikkuna.

MAWi server -ohjelmiston hallinta on selainpohjainen ja siihen päästään käsiksi kirjoittamalla MAWi server asennuksessa annettu IP-osoite sekä portti selaimen URL-kenttään. Mikäli MAWi server on asennettu julkiseen verkkoon, joka on avoin internettiin, voidaan MAWi server -hallintaan päästä käsiksi mistä tahansa, missä on internet-yhteys ja millä tahansa laitteella, josta löytyy

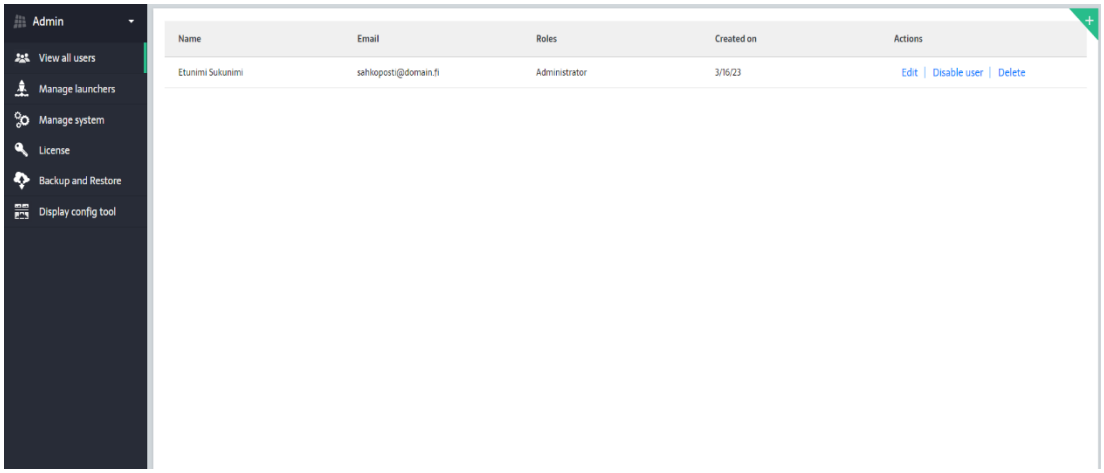
internet-selain. Tässä opinnäytetyössäni MAWi server ei kuitenkaan ole tietoturvasyistä asennettu julkiseen verkkoon, joten MAWi server -hallintaan pääsemiseksi tulee käyttäjän olla yhteydessä opinnäytetyön toimeksiantajan sisäiseen verkkoon. Tämä vähentää huomattavasti riskiä, jossa ulkopuolinen taho onnistuu pääsemään käsiksi MAWi server -ohjelmistoon. Hallinnassa on nähtävillä kaikki palvelimiin yhdistettyjen zero client -laitteiden näytöt. Aluksi näytöt ovat nimetty ”Untitled-X”. Näyttöjen hallintaa varten on järkevää uudelleennimetä näytöt esimerkiksi näyttöjen sijainnin mukaan. Sekä MAWi -serverissä, että Windows-käyttöjärjestelmässä on ominaisuus, jolla jokaiseen näyttöön piirtyy näytön numero, jonka avulla saadaan selville mikä näyttö on mikäkin. Hallinnassa olevat 2 ”Main” -nimiset näytöt ovat MAWi agent -palvelinten työpöydät.

Näyttöjen sisältö määritellään playlist- eli soittolistaominaisuudella. Soittolistan sisältö voi olla esimerkiksi videotiedosto, PowerPoint -diaesitys, nettisivu tai mikä tahansa zero client -laitteita hallitsevalla palvelimella sijaitseva ohjelma.



Kuva 8: Soittolistan asetukset.

Lopuksi valitaan kuvan seitsemän alareunan valikoista näyttö sekä luotu soittolista, ja MAWi käynnistää halutun ohjelman tai nettisivun avoimeksi valitulle näytölle. Jokaisella näytöllä on myös oma kalenteri, johon voidaan ajastaa eri soittolistoja, jolloin MAWi automaattisesti vaihtaa näytöllä esitettävän soittolistan kalenterin mukaisesti.



Kuva 9: MAWi server järjestelmävalvojan asetukset.

MAWi server -ohjelmiston järjestelmänvalvojan asetuksista löytyy käyttäjien-, launcher- sekä järjestelmähallinnat. Käyttäjien hallinnassa voidaan luoda, hallita, poistaa kokonaan tai poistaa käytöstä eri käyttäjiä. Käyttäjille on saatavilla kaksi roolia: Admin- tai Editor- roolit. Admin-roolilla käyttäjällä on oikeudet kaikkiin MAWi server ominaisuuksiin ja asetuksiin. Editor-roolin oikeuksia voidaan muokata jopa yksittäistä näyttöä ja soittolistaa myöden. Vain admin käyttäjällä on oikeudet järjestelmävalvojan asetuksiin. Launcher-asetuksissa voidaan lisätä soittolistojen saataville lisää palvelimilla sijaitsevia ohjelmistoja, jos MAWi ei itse löydä haluttua ohjelmistoa.

Järjestelmäasetuksissa voidaan nähdä kaikki MAWi server -ohelmistoon yhteydessä olevat MAWi agentit, ja suorittaa niille eri toimenpiteitä, kuten MAWi agent -sovelluksen päivityksiä, sekä agentin uudelleenkäynnistyksen tai sammutuksen esimerkiksi mahdollisissa ongelmatilanteissa. Järjestelmäasetuksista voidaan myös katkaista agentin ja serverin välinen yhteys, jolloin agentin näytöt poistuvat serverin näkymästä.

Backup- and Restore- valikossa voidaan suorittaa MAWi server -ohjelmiston asetusten varmuuskopiointi. Varmuuskopiointi suoritetaan pakattuun kansioon, joka salataan salasanalla. Varmuuskopio latautuu selaimella, joka on käytössä. Palautuksessa annetaan aikaisemmin ladattu varmuuskopio sekä sille luotu salasana.

8 HAASTEET

Teknisen toteutuksen osalta aluksi tuotti vaikeuksia saada MAWi -sovellus toimimaan Windows Server 2019 -käyttöjärjestelmällä. Ensimmäisellä kerralla, kun konesalivalvomoa oltiin ottamassa käyttöön, MAWi -sovellus aiheutti useita BSOD (blue screen of death) Windows -käyttöjärjestelmän kaatumisia, ja lukuisista vianmäärityksistä huolimatta ongelmaan ei keksitty toimivaa ratkaisua. Ongelma korjaantui kuitenkin myöhemmin, kun MAWi -ohjelmistoon julkaistiin uusi päivitys. On todennäköistä, että BSOD-ongelman aiheuttajana oli MAWi -ohjelmistossa ollut bugi, jonka uusi versio korjasi. Tulevaisuudessa MAWi -ohjelmistoa päivittäessä on syytä pitää varmuuskopio toimivasta versiota, mikäli uudet päivitykset tuovat mukanaan lisää odottamattomia ongelmia.

Windows Server 2019 -käyttöjärjestelmän toimivuus yli kymmenen näytön kanssa tuotti haasteita. Lisättäessä yli kymmenen näyttöä ei Windows enää tunnista lisättyjä näyttöjä, eikä anna näytöillä kuvaa. Suoranaista ratkaisua tähän ongelmaan ei löytynyt Windows Server 2019 -käyttöjärjestelmälle. Joten ongelma päädyttiin ratkaisemaan lisäämällä MAWi server -palvelimen rinnalle toinen palvelin, joka toimii vain MAWi agent -roolissa, tuoden yli kymmenen näyttöä MAWi server -sovelluksen hallintaan.

Valvontasovellukset, joita valvomossa halutaan nähdä, käyttävät selainpohjaista käyttöliittymää ja niiden käyttäminen vaatii kirjautumista. Oli haasteena saada MAWi -sovelluksen soittolistan luoma selainikkuna kirjautumaan sisään. Ratkaisuna valvontasovelluksiin luotiin uusi käyttäjä, jonka käyttöoikeudet ovat vain nähdä sovellusten sisältö, mutta ei tehdä sovelluksiin mitään muutoksia. Luodulla käyttäjällä kirjauduttiin sisään ja MAWi -soittolista laitettiin näyttöjen kalenteriominaisuudella toimintaan vuorokauden ympäri, jolloin valvontasovellus on käytettävissä jatkuvasti. Mikäli valvontasovellukset päivitetään tai niihin tehdään konfiguraatiomuutoksia, jotka uloskirjaavat kaikki palveluun kirjautuneet käyttäjät, kirjautuu myös MAWi -soittolistan selainikkuna ulos vaatien uudelleen kirjautumisen.

MAWi -sovelluksen uusi versio v2 toi uudeksi ominaisuudeksi yksittäisten näyttöjen etähallinnan. Näyttöjen etähallintaominaisuus helpottaa huomattavasti esimerkiksi valvontasovelluksiin sisäänkirjautumista tai pienten muutosten tekemistä, kuten valvontasovellusten graafien koon muuttamisen valvontasovelluksien sisällä.

9 YHTEENVETO

Zero client -konesalivalvomon tavoitteena oli luoda yrityksen toimistotiloihin konesalien valvontaa helpottavat konesalivalvomot. Zero client -teknologian tavoite konesalivalvomoiden asennuksessa oli saada valvomoista helposti ylläpidettäviä. Zero client -konesalivalvomoiden avulla nämä tavoitteet on onnistuttu täyttämään hyvin. Zero client -teknologian avulla ei toimiston työntekijöiden tarvitse huolehtia konesalivalvomon ylläpidosta toimistossa, koska kaikki toimivat keskitetysti samoilla palvelimilla voidaan helposti hallita kerralla molempien toimistotilojen konesalivalvomoita mistä käsin tahansa, eikä hallintaa suorittavan henkilön tarvitse käydä paikan päällä toimistoissa, jotka sijaitsevat yli kolmen tunnin ajomatkan päässä toisistaan. Konesalivalvomo on helpottanut varsinkin konesalien olosuhdevalvontaa. Valvomot sijaitsevat toimistoissa näkyvillä paikoilla, joissa toimistojen työntekijöiden on helppo päivän aikana katsoa konesalien tilannetta, ja siten havaita mahdollisia muutoksia ja ongelmatilanteita. Konesalivalvomoissa on useita näyttöjä, joihin saadaan näkyville huomattavasti enemmän informaatiota kuin yksittäinen työntekijä saa omalle työpisteelleen, valvomon avulla työntekijä saa nopeasti suuren määrän tietoa konesalien toiminnasta. Zero client -konesalivalvomo on siis helpottanut konesalien valvontaa toivotulla tavalla.

LÄHTEET

CDW. (2022). Thick vs. Thin vs. Zero Clients: Which Model Is Right for You? https://www.cdw.com/content/cdw/en/articles/hardware/thick-vs-thin-vs-zero-clients.html

Fortinet. (n.d.) What is a Thin Client? Haettu 12.1.2023 osoitteesta https://www.fortinet.com/resources/cyberglossary/thin-client

Forcepoint. (n.d.) What is a Thin Client? Thin clients defined, explained and explored. Haettu 19.1.2023 osoitteesta https://www.forcepoint.com/cyber-edu/thin-client

Grafana. (n.d.) Alerting. Haettu 11.5.2023 osoitteesta https://grafana.com/docs/grafana/latest/alerting/

Huoltovarmuuskeskus (n.d.) Tietoyhteiskunta. Haettu 19.1.2023 osoitteesta https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta

Knerl, L. (2021). Why use a thin client for my business? https://www.hp.com/us-en/shop/tech-takes/why-use-thin-client-business

Koistinen, A. (2015). Datakeskukset – Mitä ne ovat? https://yle.fi/a/3-8396487

MonitorsAnyWhere. (n.d.) MAWi. Haettu 16.2.2023 osoitteesta https://monitorsanywhere.com/mawi

MonitorsAnyWhere. (n.d.) Quick Installation Guide – MAWi Standalone. Haettu 16.2.2023 osoitteesta https://monitorsanywhere.com/quick-installation-guide-mawi-standalone/

MonitorsAnyWhere. (n.d.) What is HDMI over LAN? Haettu 16.2.2023 osoitteesta https://monitorsanywhere.com/hdmi-over-lan-explained/

Onlogic blog. (2022). What is a Zero Client? https://www.onlogic.com/company/io-hub/what-is-a-zero-client/

Rajesh, K. (2014). Zero Clients – Advantages and Limitations https://excitingip.com/4401/zero-clients-advantages-and-limitations/

TechTerms.com. (2006). Thick Client Definition. https://techterms.com/definition/thickclient

Vestal, M. (2022). What is a control room?: five different types of control rooms. https://www.saravalindustries.com/what-is-a-control-room/

Zeetim. (2020). What are the security benefits of thin clients and zero clients? https://www.zeetim.com/what-are-the-security-benefits-of-thin-clients-and-zero-clients/