Tampereen ammattikorkeakoulu

Hajautetun automaatiojärjestelmän palautumissuunnitelman testaus

Atte Haavisto

OPINNÄYTETYÖ
Maaliskuu 2021

Sähkö- ja automaatiotekniikan koulutus
Automaatiotekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Sähkö- ja automaatiotekniikan koulutus
Automaatiotekniikka

HAAVISTO, ATTE:
Hajautetun automaatiojärjestelmän palautumissuunnitelman testaus

Opinnäytetyö 52 sivua, joista liitteitä 8 sivua
Maaliskuu 2021

Valmet Automation Oy on suunnitellut asiakkailleen, kuten voimalaitoksille ja muille teollisuuden tuotantolaitoksille, palautumissuunnitelman Valmet DNA automaatiojärjestelmän vikaantumisten ja haittaohjelmien aiheuttamien häiriöiden varalle. Palautumissuunnitelman tarkoituksena on määritellä mahdolliset järjestelmän vikatilanteet ja korjaavat toimenpiteet niistä palautumiseen. Tämän opinnäytetyön aiheena oli täydentää palautumissuunnitelmaa testausosiolla, jolla tarkastetaan palautumissuunnitelman paikkansapitävyys tietyillä aikaväleillä sekä todennetaan järjestelmän palautumiskyky erilaisilla testauksilla.

Palautumissuunnitelman testausosion laatiminen toteutettiin perehtymällä nykyisen palautumissuunnitelman sisältöön ja Valmet DNA:n varmuuskopiointimenetelmiin. Lisäksi tutustuttiin tietoturvallisuusmenetelmiin ja -toimintatapoihin tutkimalla Valmetin sisäisiä materiaaleja sekä haastattelemalla Valmetin tietoturva- ja järjestelmäasiantuntijoita. Myös puolen vuoden työkokemus järjestelmätöistä auttoi opinnäytetyössä.

Palautumissuunnitelman testauksesta laadittiin raportointipohja, jonka on tarkoitus toimia tarkastuslistana ja testausohjeena vuoden tai puolentoista vuoden välein toistettavissa testauksissa. Laaditun testaussuunnitelman avulla suoritettiin erään Valmet Automation Oy:n asiakkaan palautumissuunnitelman testaus, jonka tulokset ovat raportoituna tässä opinnäytetyössä.

Palautumissuunnitelman testausosion avulla Valmet Automation Oy voi laajentaa tietoturvapalvelujaan entisestään. Tässä työssä laaditun testauspohjan avulla voidaan ylläpitää palautumissuunnitelmaa laitoksien järjestelmien muuttuessa aika ajoin. Asiakkaan etuna on palautumissuunnitelmalla ja sen testauksella saavutettava vikatilanteiden keston minimointi, jolloin tuotannon keskeytymisestä tai hidastumisesta aiheutuvat tappiot saadaan mahdollisimman vähäisiksi. Palautumissuunnitelma ja sen testaaminen voi myös toimia hyvänä lähtökohtana yrityksen vakuutusneuvotteluissa, joissa palautumissuunnitelmalla voidaan osoittaa tuotantolaitoksen valmius poikkeustilanteisiin.

Asiasanat: palautumissuunnitelma, järjestelmän palauttaminen, Valmet DNA

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Electrical and Automation Engineering
Automation Engineering

HAAVISTO, ATTE:
Testing of Distributed Control System's Recovery Plan

Bachelor's thesis 52 pages, appendices 8 pages
March 2021

Valmet Automation Oy has developed a recovery plan for its customers such as power and industrial plants for fault and cyber security situations. The Recovery plan's purpose is to specify potential system fault situations and the procedures to recover from them. This thesis' objective was to complement the recovery plan with a testing part to verify periodically that the recovery plan is up-to-date, and the system is recoverable by doing different tests.

The planning of the recovery plans testing section was done by getting acquainted with the current recovery plan's content, Valmet DNA's backup concept and by interviewing Valmet's cyber security and system specialists. The author's half a year work experience as a system specialist also helped with the thesis.

An Excel based test report document was created for the recovery plan test section to work as a check list and as a guide for the personnel carrying out the recovery plan testing every year or year and a half. This thesis also included testing of a recovery plan for a certain Valmet Automation's customer. The testing results were reported in this thesis.

With the recovery plan testing section, Valmet Automation can widen the recovery plan service. With the testing report developed in this thesis, the recovery plan can be maintained up to date as Valmet's customers' systems change from time to time. For the customer, the recovery plan and its testing improve the recovery times from fault situations which lowers the cost of production downtime. The recovery plan and its testing can also be an advantage for the customer in acquiring certain insurances as the recovery plan is a proof that the production plant is prepared for different fault situations and they have prepared themselves in advance for them.

Key words: recovery plan, system recovering, Valmet DNA

SISÄLLYS

LYHENTEET JA TERMIT

BU	DNA-järjestelmän varmennuspalvelin, backup server
EAC	DNA-järjestelmän suunnittelutyöasema, engineering activity client
EAS	DNA-järjestelmän suunnittelupalvelin, engineering activity server
I/O	Kenttälaitteiden tulo- ja lähtösignaalit, input / output
NAS	Verkkoon liitetty tallennuspalvelin, network-attached storage
RTO	Tavoiteltu toipumisaika, recovery time objective
RPO	Tavoiteltu toipumispiste, recovery point objective
Valmet DNA	Valmetin hajautettu automaatiojärjestelmä, Valmet dynamic network of applications

1 JOHDANTO

Valmet DNA on Valmet Automation Oy:n hajautettu automaatiojärjestelmä, jota käytetään muun muassa energiantuotantolaitoksilla, laivojen ohjausjärjestelmänä, sellu- ja paperitehtaissa sekä muissa teollisuuden tuotantolaitoksissa. Valmetin asiakkaille laadittavassa palautumissuunnitelmassa on dokumentoitu toimenpiteet ja roolitukset, joilla järjestelmä saadaan palautettua toimintakuntoon häiriötilanteissa.

Tämän opinnäytetyön tarkoituksena oli laatia vielä kehitysvaiheessa olevalle palautumissuunnitelmalle testausosuus, joka täydentäisi palautumissuunnitelmaa. Palautumissuunnitelman testauksella ylläpidettäisiin palautumissuunnitelmaa, todennettaisiin sen toimivuus ja tarkastettaisiin järjestelmän palautumiskykyyn vaikuttavia toimintoja.

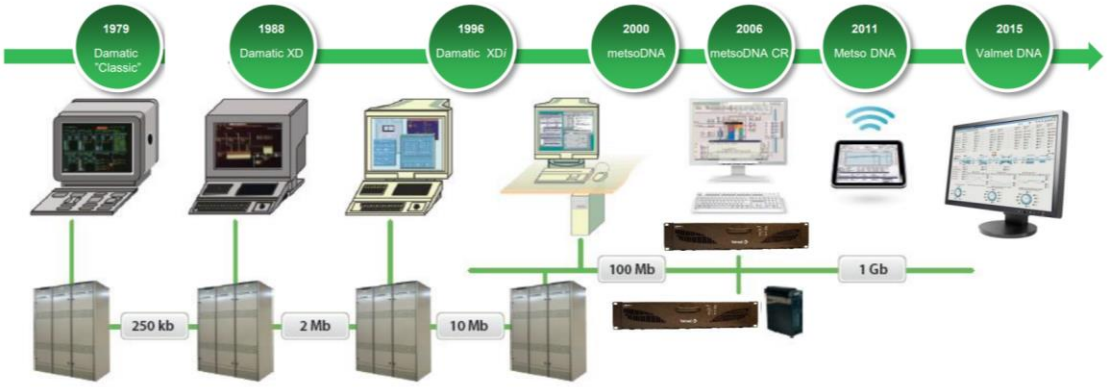
Työssä perehdyttiin Valmet DNA:n järjestelmän toimintaan ja rakenteeseen sekä selvitettiin DNA:n palautumiskyky ja sitä tukevat toimenpiteet. Työssä tutustuttiin myös Valmet DNA:n kyberturvallisuuteen. Edellä mainittu tieto hankittiin Valmetin sisäisestä materiaalista sekä kyberturvallisuus- sekä järjestelmäasiantuntijoiden haastatteluilla. Opinnäytetyötä edeltänyt noin puolen vuoden työkokemus Valmet Automationin järjestelmäasiantuntijana auttoi työn suunnittelussa ja testauksen suorittamisessa.

Opinnäytetyön tavoitteena oli laatia raportointipohja sisältöineen palautumissuunnitelman testausta varten. Suunnitelma toimisi osittain oppaana ja muistilistana testauksessa. Sen lisäksi testattaisiin erään Valmetin asiakkaan järjestelmä, jolle oli jo laadittu palautumissuunnitelma. Palautumissuunnitelman täydentäminen testausosiolla laajentaisi Valmetin tarjoaman palautumissuunnitelman palvelukuvausta. Testausosiolla täydennetty palautumissuunnitelma valmistaa asiakasta paremmin varautumaan häiriötilanteisiin ja pystyy palautumaan niistä nopeammin, jolloin tuotannon pysähtymisestä tai viivästymisestä aiheutuvat tappiot saadaan minimoitua.

2 VALMET DNA

2.1 Järjestelmä

Valmet DNA on Valmet Automationin hajautettu automaatiojärjestelmä, jonka juuret ovat vuonna 1979 julkaistussa Damatic ”Classic” -järjestelmässä (kuva 1). Sittemmin järjestelmä on kehittynyt eri nimenmuutosten myötä Valmet DNA:ksi, joka on edelleen vuoden 1988 Damatic XD -järjestelmästä eteenpäin yhteensopiva aikaisempien versioiden kanssa. Valmet DNA:n nimi tulee englannin kielen sanoista ”Dynamic Network of Applications”, joka tarkoittaa suomeksi sovellusten dynaamista verkkoa. (Forsman 2020.)

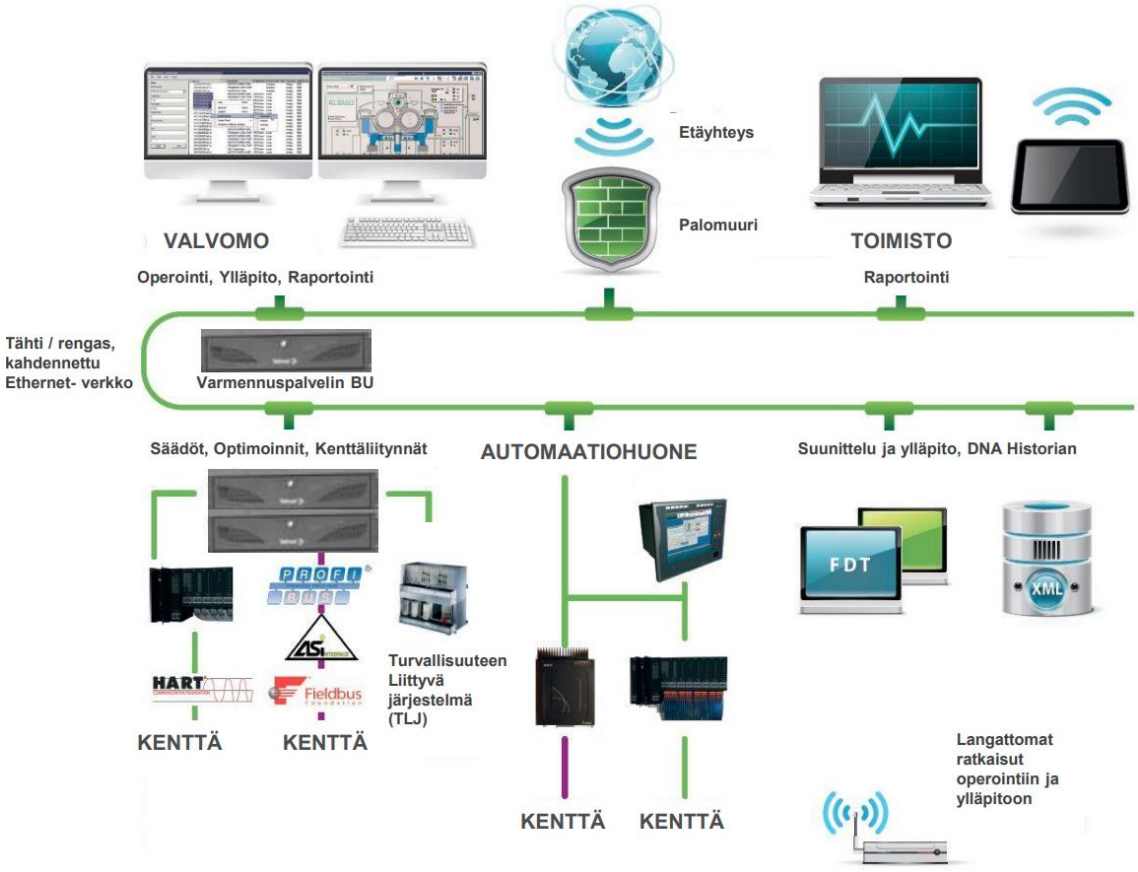


KUVA 1. Valmet DNA -järjestelmän historia ja yhteensopivuus (DNA yleisesittely 2015)

Valmet DNA:n vahvuus on sen sovellettavuus prosessi-, kone- ja moottoriohjauksiin sekä laatusäätöihin (Valmet DNA system architecture 2021). Valmet DNA -järjestelmään on integroitu turvallisuuteen liittyvä järjestelmä sekä kunnossapitosovellukset, kuten värähtelyn valvonta ja älykkäiden kenttälaitteiden hallinta. DNA:n kattavan yhden järjestelmän tarjonnan hyötyjä ovat muun muassa yksi käyttöliittymä, hälytystenkäsittely, historiatietokanta ja trenditys. Yhtä järjestelmää käytettäessä ei myöskään tarvitse huolehtia usean järjestelmän ja laitteiden välisestä linkityksestä toisiinsa. Valmet pystyy myös tarjoamaan kaikki varaosat ja koulutuksen asiakkaan automaatiojärjestelmän käyttöön. (DNA yleisesittely 2015.)

2.1.1 Rakenne

Kuvassa 2 on esitelty DNA-järjestelmän rakenne, joka perustuu Ethernet-pakettipohjaiseen tähti- tai rengasmalliseen, yleensä kahdennettuun automaatioverkkoon. Verkkoon kytketään useita eri palvelimia, joilla on oma tehtävänsä. Toimistoverkosta ja internetistä voidaan kytkeytyä automaatioverkkoon palomuurin yli. (DNA Yleisesittely 2015.) Tässä opinnäytetyössä käytetään järjestelmän palvelimista myös nimityksiä asema ja solmu.



KUVA 2. Valmet DNA rakenne (DNA yleisesittely 2015)

Operointipalvelimen (Operator Server, OPS) kautta operaattori saa tietoa prosessista ja voi ohjata sitä. Hälytyspalvelin (Alarm Server, ALS) kerää ja ylläpitää prosessin hälytystietoja ja lähettää hälytykset operointipalvelimen kautta operaattorille. Historiapalvelimen (Info Server) tehtävä on kerätä prosessi-, operointi- ja hälytystietoja muistiin, jotta prosessin tilaa ja järjestelmän toimintaa voidaan tutkia jälkikäteen. (DNA Yleisesittely 2015.)

Prosessin ohjauksesta vastaavat prosessinohjauspalvelimet (Process Control Server, PCS). Niihin liitetään erilaisia kenttäväyliä kuten esimerkiksi Profibus, Profinet ja Foundation Fieldbus, I/O-ohjaimilta tuleva tieto sekä turvallisuuteen liittyvä järjestelmä. Järjestelmään voidaan myös lisätä liityntäpalvelimia (Interface Server, LIS), mikäli DNA:han tulee liittää jokin toinen järjestelmä. (DNA Yleisesittely 2015.)

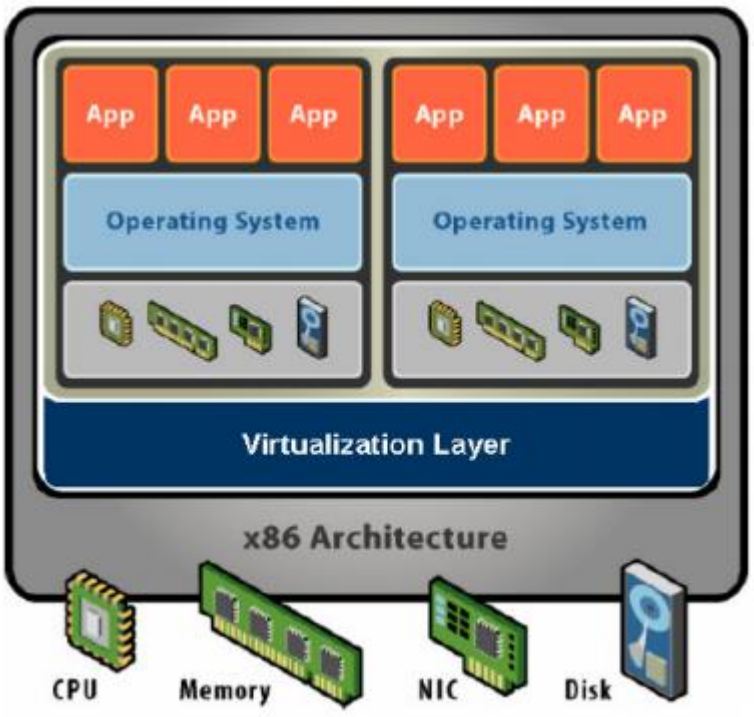
Suunnittelua varten järjestelmässä on suunnittelupalvelin ja siihen tarvittaessa lisättäviä suunnittelutyöasemia (Engineering Activity Server/Client, EAS/EAC). Suunnittelutyöasemilla voidaan tehdä automaatiosovellukseen muutoksia, ladata ne järjestelmään ja käyttää diagnostiikkaan sekä kenttälaitteiden ja mekaaniseen kunnonvalvontaan tarkoitettuja sovelluksia. (Valmet DNA Suunnittelu- ja ylläpitotyökalut 2015.)

Varmennuspalvelimelle (Backup Server, BU) ladataan kaikki järjestelmän sovellusmuutokset. Järjestelmän palvelimet noutavat varmennuspalvelimelta kaikki sovellukset ja tiedot, joita ne tarvitsevat. (DNA Yleisesittely 2015.)

2.1.2 Virtualisointi

Valmet Automation on myös kehittänyt DNA-järjestelmästä virtualisoidun mallin, jota käytetään tapauskohtaisesti. Virtualisoinnilla DNA:ssa tarkoitetaan usean fyysisen Microsoft Window -pohjaisen palvelimen kuten EAS:n, OPS:n, ALS:n, BU:n tai Infon korvaamista yhdellä suorituskykyisellä tietokoneella. Fyysiset palvelimet jaetaan virtualisoidussa koneessa loogisiksi resursseiksi, jolloin virtuaalikone sisältää siis monta eri käyttöjärjestelmää. (Virtualized DNA in VMware 2021.)

Kuvassa 3 on esitelty virtuaalipalvelimen rakenne. Valmet Automationin käyttämä virtualisointialusta on VMware ESXi. Virtualisointialustaa kutsutaan isännäksi ja sen alaisuudessa ajettavia tietokoneita, eli DNA:n tapauksessa esimerkiksi OPS:ia tai EAS;ia, kutsutaan vieraiksi. Vieraille jaetaan fyysisen koneen suoritinytimet, välimuisti ja massamuisti vieraskoneen tarpeiden mukaan. (Virtualized DNA in VMware 2021.)



KUVA 3. Virtuaalipalvelimen rakenne (Virtualized DNA in VMware 2016)

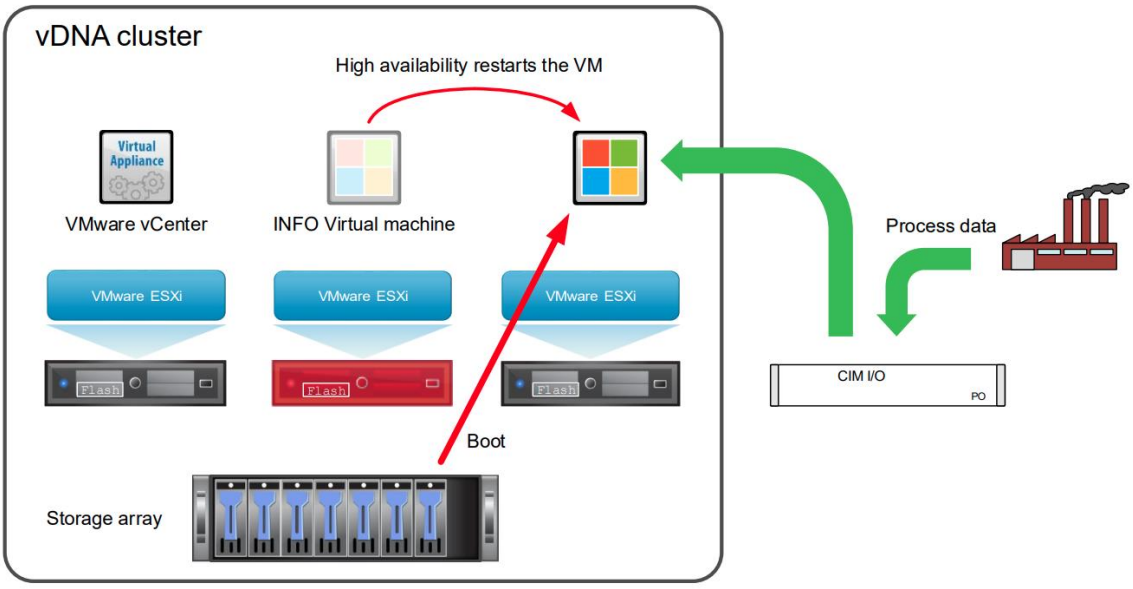
Laitoksen kannalta virtualisoinnin etuna on erilaisten kulujen ja infrastruktuuritarpeiden vähentäminen. Virtualisoinnilla fyysisen laitteiston määrä vähenee, jolloin laitteisto vie vähemmän tilaa palvelinhuoneissa, verkkoinfrastruktuuri pienenee ja sähkökulut sekä jäädytyksen tarve laskevat. Sen lisäksi järjestelmän palauttaminen helpottuu esimerkiksi VMwaren Snapshot-työkalulla. (Virtualized DNA in VMware 2021.)

Virtualisoinnin hyötynä on vieraiksi asennettavien käyttöjärjestelmien helpompi hardenointi sekä virustorjunnan ja Windows-päivitysten helpompi hallinta. Virtualisoidussa ympäristössä myös sovellusten asentaminen sekä päivittäminen helpottuu ja esimerkiksi Valmetin tukipalvelun on vaivatonta työskennellä etänä. DNA:n versiopäivityskin helpottuu, koska vain virtuaalikone pitää päivittää. (Virtualized DNA in VMware 2021.)

Useasta fyysisestä virtuaalipalvelimesta voidaan rakentaa klusteri, jossa VMwaren vSphere -hallintatyökalulla valvotaan ESXi-alustoja ja niiden toimintaa. Klusterirakenteella ja vCenterin avulla virtuaalikoneet voidaan siirtää toiselle palveli-

melle ja sen ESXi-alustalle. Tällaista huoltoa helpottavaa ja järjestelmän vikatilanteiden kestoa minimoivaa toiminnallisuutta kutsutaan korkeaksi saatavuudeksi (high availability).

Kuvassa 4 on esitetty korkean saatavuuden toimintaa vikatilanteessa. Kuvan keskimmäinen punaiseksi merkattu palvelin ei enää vastaa, jolloin siinä suoritettu INFO-virtuaalikone siirretään levypakalta toiselle ESXi:lle, jossa sen suoritusta jatketaan. Samalla DNA:n CIM I/O -palvelin puskuroi sen omaan tallennustilaan prosessidataa, joka puretaan INFO-virtuaalikoneelle sen käynnistyessä. (Virtualized DNA in VMware 2021.)

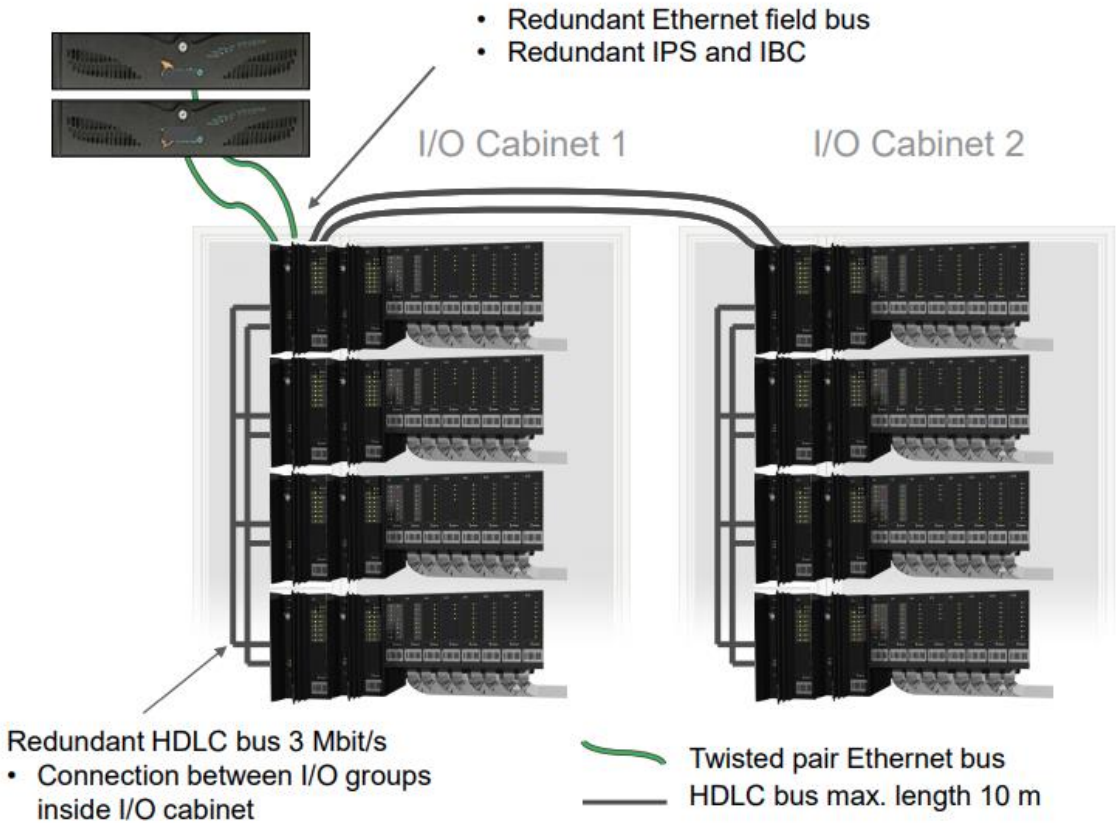


KUVA 4. Korkean saatavuuden toiminta vikatilanteessa (Virtualized DNA in VMware 2021)

2.1.3 Kahdennus

Kuvassa 5 on esimerkki I/O-laitteiston sekä prosessiohjainten kahdennuksesta. Valmet DNA järjestelmä kahdennetaan yleensä verkon, verkkolaitteiden, prosessiohjainten ja I/O-laitteiston osalta. Myös palvelinten verkkokaapelointi kahdennetaan. Kahdennetussa järjestelmässä kaikkia laitteiston osia on kaksi, niin että toinen laitteista toimii varalla ja se otetaan käyttöön siinä tapauksessa, että pää-

laite ei vastaa järjestelmään. Niin voi käydä esimerkiksi laiterikon takia. Rikkoutunut laite voidaan vaihtaa, vaikka prosessia ajettaisiin, koska varalaite suorittaa rikkoutuneen laitteen tehtävää. Myös johdotukset kahdennetaan. (Forsman 2020.)

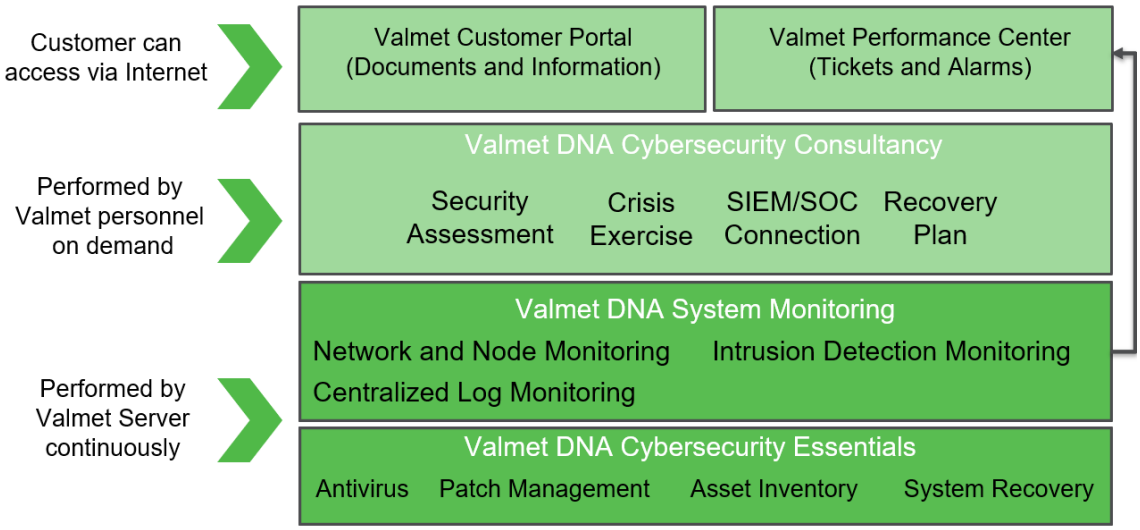


KUVA 5. Prosessiohjainten ja I/O:n kahdennus (Valmet DNA Automated Process 2015)

2.2 Järjestelmän kyberturvallisuus

Automaatiojärjestelmien kyberturvallisuuteen ja sen kehittämiseen panostetaan koko ajan enemmän teknologian ja it-palveluiden kehittyessä. Kyberturvallisuuden kannalta tulee kiinnittää huomiota järjestelmän määrittelyihin siitä, kuinka siihen pääsee verkon ulkopuolelta käsiksi, kuinka verkon sisällä toimitaan ja miten järjestelmän saastuminen havaitaan. Tämän hetken suurimpia uhkia automaatiojärjestelmille ovat internet-verkko, sähköposti ja ulkoiset massamuistilaitteet kuten USB-tikut.

DNA:n kyberturvallisuuden ylläpito on esitelty kuvassa 6. Asiakkaalla on pääsy Valmetin asiakasportaaliin, josta löytyy DNA:n dokumentointia ja informaatiota sekä mahdollisuus tehdä hälytys- ja vikailmoituksia. Asiakkaan pyynnöstä Valmet voi tehdä kyberturvallisuuskonsultointia, johon sisältyy turvallisuusarviointi, kriisiharjoitusten järjestäminen, yhteyksien luominen tietoturvakeskuksiin ja palautumissuunnitelman laatiminen. Valmetin palvelimet vastaavat jatkuvasta DNA-järjestelmän seurannasta monitoroimalla ja lokittamalla järjestelmän verkkoa ja solmuja. Antiviruskuvaukset ja päivitykset ladataan automaattisesti järjestelmään. (Valmet DNA Cyber Security 2019.)



KUVA 6. DNA:n kyberturvallisuuden ylläpito (Valmet DNA Cyber Security 2019)

2.2.1 Hardenointi

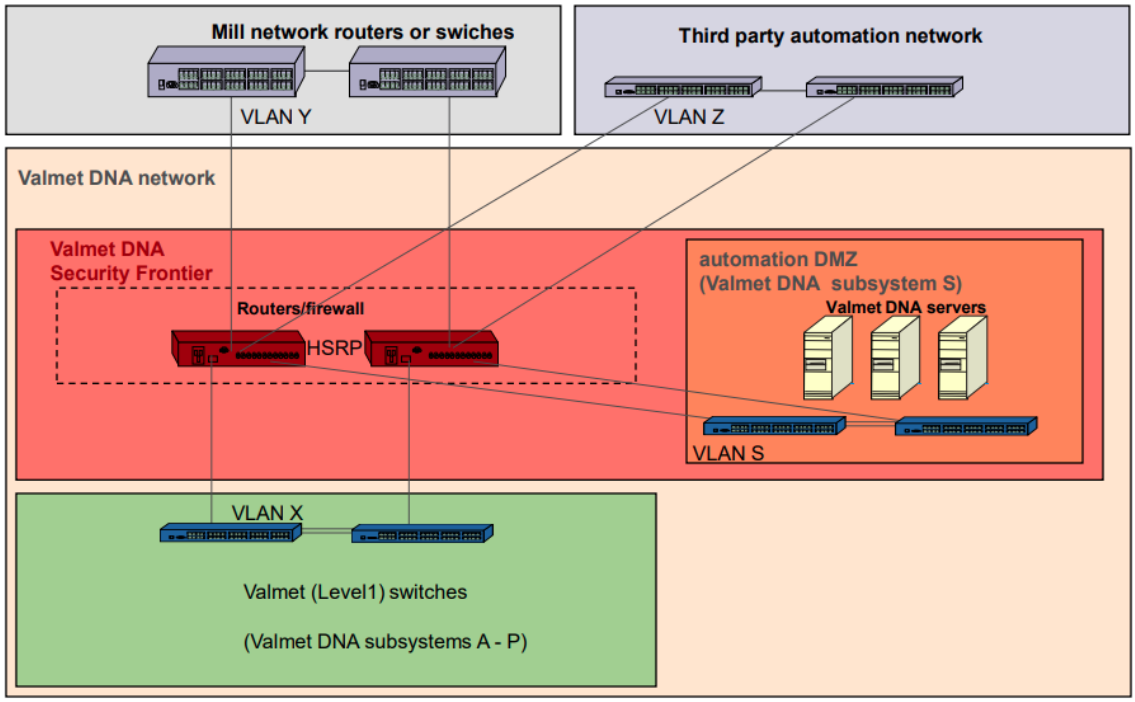
Hardenoinnilla tarkoitetaan tarpeettomien toimintojen, palveluiden, ohjelmien tai komponenttien käytöstä poistamista. Turhat toiminnot heikentävät järjestelmän kyberturvallisuutta. Tyypillisiä toimintoja ovat esimerkiksi ylimääräisten käyttöjärjestelmien tai ohjelmien poisto ja käyttämättömien porttien sulkeminen. (Valmet DNA Cyber Security White Paper 2020.)

DNA-ympäristössä hardenointia tehdään kaikilla tasoilla: verkkolaitteiden konfiguroinnissa, palvelinten ja työasemien komponenteissa, käyttöjärjestelmissä ja kyberturvallisuuteen liittyvissä päivityksissä. Esimerkiksi Microsoft Windows -käyttöjärjestelmien osalta hardenoinnissa poistetaan käytöstä tiettyjä Windows-

palveluita ja rajataan käyttäjätilien sekä tallennuslevyjen käyttöoikeuksia. Myös USB-porttien käyttö estetään ja automaattiset toistotoiminnot poistetaan käytöstä. Salasanat asetetaan käyttäjille Valmetin salasanapolitiikan mukaisesti. (Valmet DNA Cyber Security White Paper 2020.)

2.2.2 Security frontier

DNA-verkon ulkopuolelta tuleville yhteyksille käytetään palomuurillista reititintä. Usein halutaan, että automaatioverkon ulkopuolelta voidaan seurata prosessia tai käyttää esimerkiksi DNA:n suunnitteluympäristöä, jolloin palomuurin käyttö on tarpeen. DNA:n verkkorakenteessa voidaan käyttää mallia, jossa automaatioverkosta eristetään osa palvelimista niin sanotulle DMZ-alueelle (kuva 7). DMZ tulee sanoista demilitarized zone eli suomeksi demilitarisoitu alue. DMZ-mallia kutsutaan myös englanninkielisellä termillä security frontier. Palomuurin läpi sallitaan tietty liikenne DMZ-alueelle, mutta suoria yhteyksiä ei voida ottaa toimistoverkosta DNA-verkkoon. Palomuurissa käytetään sellaisia Valmetin kehittämiä protokollia, jotka eivät ole yleisessä tiedossa, jolloin tuntemattomien yhteyksien on lähes mahdotonta päästä DNA-verkkoon. (Forsman 2020.)



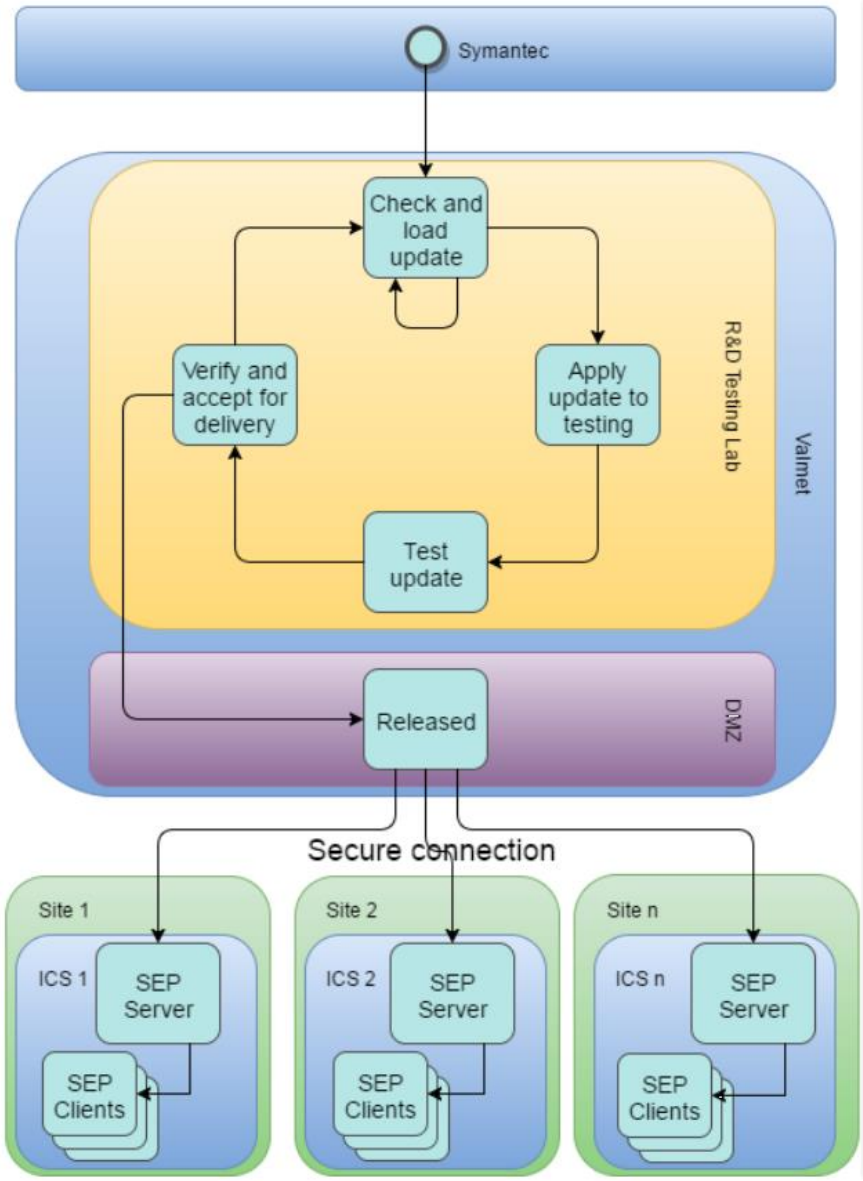
KUVA 7. Security Frontier (Valmet DNA Network Architecture DMZ)

DMZ-alueen käytön ensisijainen tarkoitus on suojata automaatioverkkoa, mutta se myös estää turhaa liikennettä prosessinohjausverkossa. DMZ-alueelle sijoitetaan yleensä niin sanottu turvallisuuspalvelin, jossa on virustorjunnan ja Windows-päivitysten ylläpitopalvelimet, suunnittelupalvelin ja DNA:n infopalvelin. Viruskuvaukset ja Windows-päivitykset haetaan Valmetin palvelimilta internetin kautta, jolloin turvallisuuspalvelin on syytä sijoittaa DMZ-alueelle. (Forsman 2020.)

2.2.3 Haittaohjelmien torjunta

Valmet käyttää DNA:n Windows-solmuissa lähtökohtaisesti Symantec Endpoint Protection -suojausohjelmaa. Asiakas voi myös halutessaan käyttää muita ohjelmia haittaohjelmien varalle, mutta Valmet ei vastaa niiden käytöstä. Suurin osa olemassa olevista haittaohjelmista on suunnattu Windows-käyttöjärjestelmään, joten sitä käyttävät palvelimet on syytä suojata. Olemassa olevien haittaohjelmien kirjo on laaja ja uusia viruksia syntyy tiheään tahtiin, joten suojausohjelmistoa ja sen viruskuvauksia tulisi ylläpitää. (Valmet DNA Security - Malware Protection 2016.)

Viruskuvauksien tehtävä on toimia tunnisteina, joilla haittaohjelmat havaitaan järjestelmästä. Symantec Endpoint Protection on Broadcom:n omistama tuote, jota se myös ylläpitää ja jolle se tarjoaa viimeisimmät viruskuvaukset (Broadcom). Valmet tarkistaa päivittäin julkaistavat uudet viruskuvaukset ja niiden yhteensopivuuden DNA-järjestelmän kanssa. Tarkistuksen jälkeen viruskuvaukset ladataan Valmet:n palvelimelle, josta asiakkaan turvallisuuspalvelin noutaa automaattisesti uusimmat viruskuvaukset ja jakelee ne DNA-järjestelmän Windows-solmuille. Solmujen Symantec Endpoint Protection Client-ohjelmisto ottaa viruskuvaukset käyttöön. (Valmet DNA Security - Malware Protection 2016.) Kuvassa 8 on esitelty viruskuvausten ylläpitoprosessi, jossa ylin jakelija Symantec on nykyään Broadcom.



KUVA 8. DNA-järjestelmän viruskuvausten ylläpitoprosessi (Valmet DNA Security - Malware Protection 2016)

2.2.4 Etäyhteydet

Etäyhteyksien ottaminen internetin kautta ja esimerkiksi viruskuvausten siirtäminen DMZ-alueelle vaatii suojattua yhteyttä. VPN-pohjaisella Valmet SCS:n (Secure Connection Solution) avulla vain tunnistetut ja luvalliset yhteydet voivat ottaa yhteyden laitoksen verkkoon internetin kautta. Yhteyksien toiminnasta pidetään myös kirjaa SCS:n avulla. (Valmet DNA Cyber Security White Paper 2020.)

SCS:n lisäksi voidaan käyttää lisäpalveluna IDS:ää (Intrusion Detection System). IDS-palvelimella seurataan DNA-verkon ulkopuolelta tulevaa liikennettä ja se estää kaiken tuntemattoman tai häiritsevän verkkoliikenteen. (Valmet DNA Cyber Security White Paper 2020.)

2.2.5 Ulkoiset massamuistilaitteet

Ulkoiset massamuistilaitteet tulisi tarkistaa haittaohjelmien varalta ennen liittämistä automaatioverkon laitteisiin. Valmetin valikoimassa on USB Cleaner -tuotenimeä kantava FitSec:n tablettitietokone (kuva 9), jolla voidaan tarkistaa muistilaitteet haittaohjelmien varalta ennen niiden liittämistä DNA:han (Valmet DNA Cyber Security White Paper 2020). Lähtökohtaisesti vastuu massamuistilaitteiden käytöstä on asiakkaalla. Asiakkailla voi myös olla omia ratkaisuja haittaohjelmien tarkistukseen.

KUVA 9. USB Cleaner -tietokone (Valmet DNA C2019 Cyber Security 2019)

3 TIETOTURVASTANDARDIT

3.1 Sertifikaatit ja standardit

Valmet Automation on sertifioitu useiden standardien mukaan. Yksi sertifikaateista on tietoturvaan liittyvä IEC-62443-4-1-standardin mukainen sertifiointi. Valmet noudattaa myös muita tietoturvaan ja palautumiseen liittyviä standardeja.

3.1.1 IEC 62443-4-1:2018

Valmet Automation on IEC 62443-4-1-sertifioitu yritys. Sertifikaatti määrittelee automaatiojärjestelmän tuotteille ja niiden kehitykselle tietoturvavaatimukset. Ohjelmistokehityksessä käytettäviä tietoturvametodeja ovat esimerkiksi turvatut ohjelmointikäytännöt, turvallisuusmallien käyttö tuotteiden määrittelyissä, säännölliset tuotteiden tarkistukset, ohjelmistoanalyysit ja laajennettu testaaminen. (Valmet DNA Cyber Security White Paper 2020.)

Kolmannen osapuolen ohjelmistojen ja etenkin avoimen lähdekoodin ohjelmien käyttöä tulisi erityisesti hallita tarkasti. Kaikki Valmet DNA:ssa käytetyt ohjelmistot on arvioitu teknisestä ja kunnossapidollisesta näkökulmasta sekä tekijänoikeuksien ja lisensoinnin puolesta sopiviksi osana DNA-järjestelmää. (Valmet DNA Cyber Security White Paper 2020.)

3.1.2 NIST Special Publication 800-184

Valmet Automation soveltaa myös Yhdysvaltalaisen NIST:n (National Institue of Standards and Technology) julkaisemaa ohjetta 800–184 tarjoamalla DNA:n palautumissuunnitelman valmistelua sekä uhka- ja riskikartoituksia asiakkailleen (Valmet DNA Cyber Security White Paper 2020). Ohjeen tarkoitus on kehittää organisaatioiden riskienhallintakykyä ja palautumisvalmiutta. Sen avulla organisaatiot voivat luoda suunnitelmia vikatilanteiden varalle ja realistisia palautumisharjoittelutilanteita. (NIST Special Publication 800-184 2016, abstract)

Kriittinen osa vikatilanteista palautumista on siihen valmistautuminen suunnitelmalla. Palautumissuunnitelman laadinnalla, hallinnoija perehtyy tietojärjestelmänsä riippuvuuksiin, onnettomuustilanteiden hallintaan ja vastuurooleihin. Palautumissuunnitelman laadinta kehittää myös ”mitä jos” -ajattelua onnettomuuksien varalle. (NIST Special Publication 800-184 2016, 7.)

4 JÄRJESTELMÄN PALAUTTAMINEN

4.1 Järjestelmän palautus

Järjestelmän palauttamisella tarkoitetaan yleisesti niitä toimenpiteitä, joilla automaatiojärjestelmä saatetaan normaaliin, häiriötä tai laiterikkoa edeltävään toimintakuntoon. Tässä opinnäytetyössä käsitellään järjestelmän palauttamista pääasiassa ohjelmistojen ja tietokantojen osalta.

4.1.1 Palauttamisen periaatteet

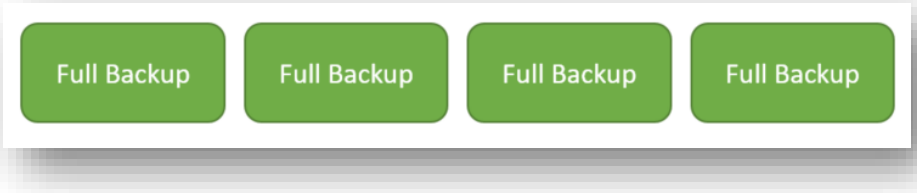
Kun jokin automaatiojärjestelmän osa hajoaa, tarvitaan jokin korvaava osa sen tilalle. Kriittiset laitteet voivat olla kahdennettuja, mutta suositus on pitää silloinkin laitteista varaosa laitoksella. Fyysisten laitteiden korvaaminen on yleensä helppoa, koska identtinen laite voidaan tilata valmistajalta vanhan tilalle. Automaatiojärjestelmän laitteiden ohjelmistojen ja konfigurointien palauttaminen voi olla sen sijaan monimutkaisempaa, koska usein tietokannat ja konfiguroinnit ovat uniikkeja. Tästä syystä DNA järjestelmästä ja tietokannoista otetaan varmuuskopioita.

4.2 Varmuuskopiointimenetelmät

Varmuuskopioinnin tarkoituksena on kopioida tieto yhteen tai useampaan eri sijaintiin, josta se voidaan palauttaa alkuperäiseen käyttötarkoitukseen. Varmuuskopion säilymisen kannalta se olisi hyvä siirtää eri tilassa sijaitsevaan tallennuskohteeseen, eri verkkoon tai mahdollisuuksien mukaan kokonaan irti verkosta, jolloin esimerkiksi tulipalo-, vesivahinko- tai verkon saastumistilanteessa varmuuskopio säilyy eheänä. Valmet DNA:n kaltaiseen automaatiojärjestelmään, jossa varmuuskopiointia toistetaan, on varmuuskopiointimenetelmiä neljä: täysi, inkrementaalinen, differentiaalinen ja synteettinen (full, incremental, differential ja synthetic backup).

4.2.1 Täysi varmuuskopio

Täydellä varmuuskopioinnilla kopioidaan aina kopiota otettaessa kaikki kohdesijainnin data toiseen sijaintiin. Jokaisesta luodusta varmuuskopiopisteestä voidaan palauttaa sellaisenaan kaikki tieto alkuperäiseen sijaintiin. Etuna on palautuksen nopeus verrattuna inkrementaaliseen tai differentiaaliseen varmuuskopioon. Täyden varmuuskopion ottamisen heikkous verrattuna muihin varmuuskopiointimetodeihin on sen hitaus, varmuuskopion suuruus sekä verkon kuormittuminen. (Valmet DNA Backup Concept 1.0 2021.)



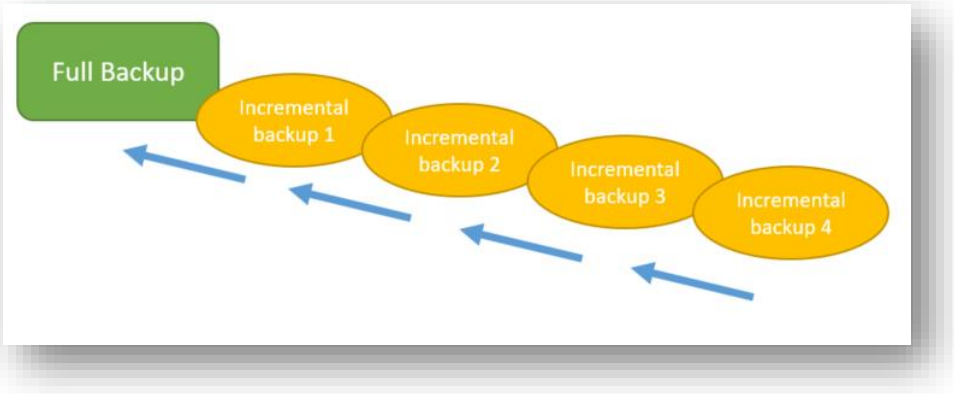
KUVA 10. Jaksotettu täysi varmuuskopiointi (Valmet DNA Backup Concept 1.0 2021)

4.2.2 Inkrementaalinen varmuuskopio

Inkrementaalinen varmuuskopiointi tarkoittaa, että edelliseen varmuuskopioon lisätään kaikki sen jälkeen lisätyt muutokset. Inkrementaalinen varmuuskopiointimenetelmä vaatii aina alkuun yhden täyden varmuuskopion. Täydestä varmuuskopiosta ja sen inkrementaalisista kopioista syntyy ketju, jonka kaikki osat tarvitaan viimeisimmän varmuuskopion palauttamiseen. (Valmet DNA Backup Concept 1.0 2021.) Kuvassa 11 on esitetty inkrementaalisen varmuuskopioinnin toiminta. Jos kuvan 11 varmuuskopiointimallin mukaan halutaan palauttaa varmuuskopiosta esimerkiksi palautuspiste ”Incremental backup 2”, vaaditaan siihen sen lisäksi varmuuskopiotiedostot ”Incremental backup 1” ja ”Full Backup”.

Inkrementaalisen varmuuskopioinnin heikkoutena on luotettavuus. Mikäli yksikin palautuspisteen aiemmista kopioista on korruptoitunut, ei kaikkia tietoja voida välttämättä palauttaa. Palauttamiseen kuluu yleensä myös enemmän aikaa kuin täydestä varmuuskopiosta. Sen etuna on kuitenkin pienet inkrementaalikopioiden

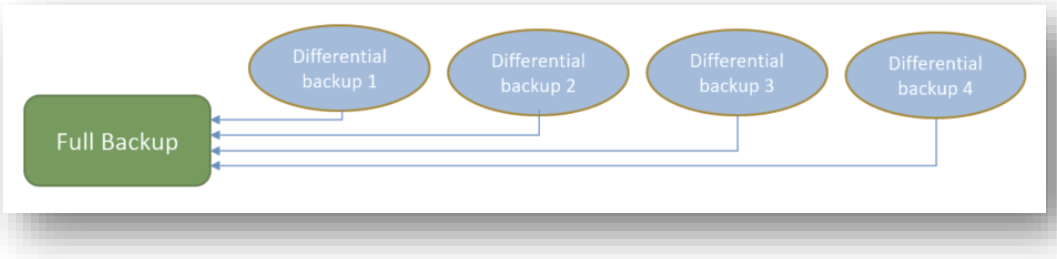
koot, jolloin myöskään verkkoa ei kuormiteta niin paljoa. (Valmet DNA Backup Concept 1.0 2021.)



KUVA 11. Inkrementaalisen varmuuskopioinnin malli (Valmet DNA Backup Concept 1.0 2021)

4.2.3 Differentiaalinen varmuuskopio

Differentiaalinen varmuuskopiointi perustuu yhteen täyteen varmuuskopioon ja sen jälkeisiin muutoskopioihin (kuva 12). Differentiaalisen varmuuskopion palautuksessa täysi varmuuskopio ja yksi differentiaalinen varmuuskopio toimivat pareina, minkä vuoksi se on luotettavampaa kuin inkrementaalinen varmuuskopiointi. Täyteen varmuuskopiontiin verrattuna säästetään tallennustilaa eikä verkko kuormitu yhtä paljoa. (Valmet DNA Backup Concept 1.0 2021.)



KUVA 12. Differentiaalisen varmuuskopioinnin malli (Valmet DNA Backup Concept 1.0 2021)

4.2.4 Synteettinen varmuuskopio

Synteettinen varmuuskopio luodaan yhdestä täydestä varmuuskopiosta ja sen inkrementaaleista, joista syntyy yksi täysi varmuuskopio. Siinä jalostetaan siis jo olemassa olevia varmuuskopiotiedostoja. Sillä on kuitenkin samat heikkoudet kuin inkrementaalisella varmuuskopioinnilla. Mikäli yksikin inkrementaalisista kopioista on korruptoitunut, ei synteettistä varmuuskopioita voida luoda. (Valmet DNA Backup Concept 1.0 2021.)

4.3 DNA-järjestelmän palauttaminen

DNA-järjestelmän palauttamisessa täytyy huomioida monia eri osa-alueita, kuten suunnitteluympäristö, historiatietokanta ja järjestelmän konfiguraatiot. Varmuuskopiointipolitiikka on sama perinteisessä ja virtualisoidussa ympäristössä. Virtuaaliympäristössä varmuuskopiointi tehdään isäntätasolta, ja fyysisiltä työasemilta otetaan varmuuskopio käyttöjärjestelmätasolla. Lähtökohta on, että kaikista solmuista otetaan täysi varmuuskopio joka sunnuntai ja inkrementaalinen tai differentiaalinen kopio joka toinen päivä. Synteettisiä varmuuskopioita ei suosita. (Valmet DNA Backup Concept 1.0 2021.)

4.3.1 Varmuuskopioiden tallennussijainti

DNA:sta otetut varmuuskopiot voidaan tallentaa NAS:lle, ulkoiselle kovalevylle, nauhalle, paikalliselle kovalevylle tai DVD:lle (Valmet DNA Backup Concept 1.0 2021). DVD-varmuuskopiointi ja nauhat ovat käytännössä kuitenkin jo poistuneet toteutettavista vaihtoehdoista.

NAS-asemat ovat yleistyneet verkon nopeuksien kasvun myötä. NAS-aseman etu on myös, että sinne tallennetut tiedostot ovat helposti saatavilla koko verkossa, mikä toki lisää myös tietoturvariskiä.

Paikallisella kovalevyllä tarkoitetaan johonkin fyysiseen palvelimeen asennettua toissijaista kovalevyä, jota käytetään sen palvelimen ensisijaisen tallennustilan

tietojen varmuuskopioiden sijaintina. Tällaista ratkaisua ei enää juurikaan käytetä, koska se ei ole luotettava tallennussijainti varmuuskopion sijaitessa fyysisesti samassa laitteistossa kuin varmuuskopioitava kohde.

Äärimmillään palautuspisteen kyberturvallisuus voidaan turvata irrottamalla järjestelmästä ja verkkovirrasta kokonaan varmuuskopiot sisältävä tallennuslaite, kuten NAS tai ulkoinen massamuistilaite. Tällaisen palautuspisteen varmuuskopioita päivitetään esimerkiksi kuukauden tai puolen vuoden välein. Tallennuslaitetta säilytetään turvallisessa paikassa kuten kassakaapissa, jolloin siihen ei voida päästä verkon kautta eikä fyysisesti käsiksi. Näin voidaan taata, että mikään ransomware-hyökkäys tai muu tietoturvauhka ei voi estää varmuuskopion palauttamista tallennuslaitteelta.

4.3.2 Varmuuskopiointityökalut

Valmet DNA -järjestelmän fyysisiä asemia varmuuskopioidaan agenttipohjaisella Veritas System Recovery -työkalulla. Virtuaaliympäristössä virtuaalikoneiden varmuuskopiointia tehdään isäntätasolla joko Dell EMC Avamar Data Protectionin avulla tai Quest vRangerilla. DNA Program Starter -ohjelmistolla tallennetaan palvelimien konfigurointitiedostoja automaattisesti BU-asemalle. Tietokantojen käsittelyyn ja niiden varmuuskopiointiin käytetään AspenTech InfoPlus.21 ja Microsoft SQL -työkaluja. (Valmet DNA Backup Concept 1.0 2021.)

4.3.3 Tärkeimmät palautuskohteet

DNA-järjestelmän suunnitteluympäristöä, EAS:ia voidaan pitää DNA-automaatiojärjestelmän ytimenä. Kaikki sovellukset ja ohjelmat ladataan EAS:n kautta järjestelmään BU-aseman kautta. EAS:n varmuuskopio onkin kaikista tärkein. Sen tietokanta tallennetaankin myös koneen täyden varmuuskopion lisäksi BU-asemalle tai muuhun kohteeseen käyttäen EAS:n sisäänrakennettua varmuuskopiointia.

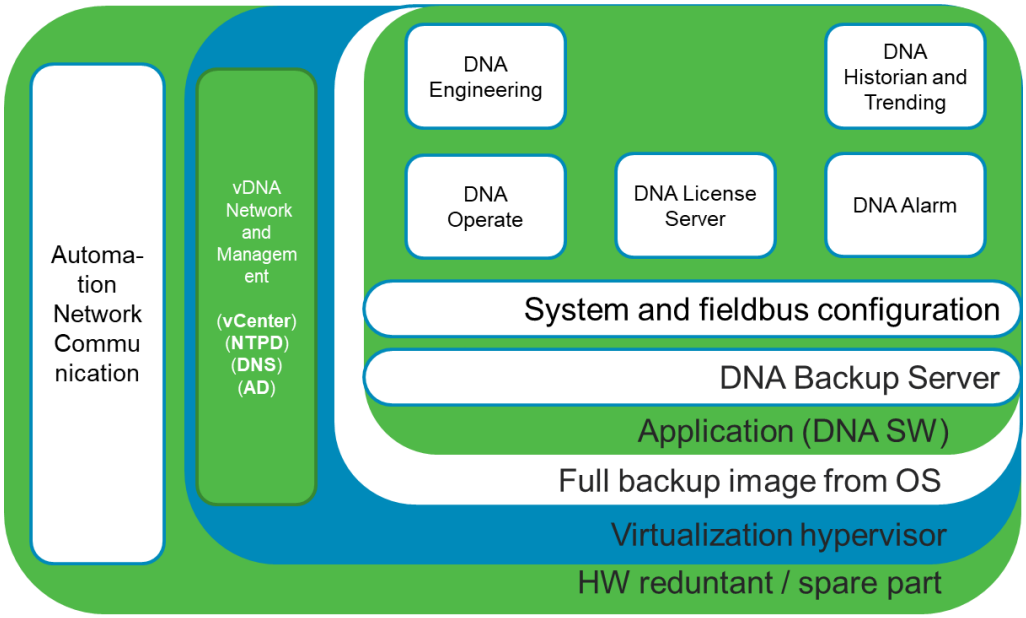
DNA:n backup-asemasta otetaan täyden varmuuskopion lisäksi kopio EAS:lle. BU-asemalle tallennetaan muun muassa operointiasemien ajoarvot sekä asemien konfigurointitiedostot. Tiedostot eivät ole järjestelmän palauttamisen kannalta elintärkeitä, mutta niiden avulla palauttaminen nopeutuu huomattavasti, mikäli BU-asema pitää palauttaa.

Historiapalvelin ei sisällä prosessin suorittamiseen vaadittavia tietoja tai toimintoja, mutta sinne tallennetaan muita tärkeitä tietoja, kuten kaikki laitoksen historian prosessiarvot. Jotta prosessin tilaa esimerkiksi ennen häiriöitä tai laiterikkoja voidaan seurata jälkeen päin, on tärkeää, että historiapalvelin voidaan palauttaa.

5 PALAUTUMISSUUNNITELMA

5.1 Tarkoitus ja sisältö

Valmet Automationilla on valmis palautumissuunnitelmapohja DNA-järjestelmälle, jota räätälöidään asiakaskohtaisesti sopivaksi. Palautumissuunnitelma toimii oppaana asiakkaalle ja Valmetin henkilöstölle. Siinä käydään läpi ne käytännön toimenpiteet, roolit ja vastuut, joilla järjestelmä saadaan palautettua toimintakuntoon hyökkäyksen tai laiterikon jäljiltä. Se sisältää muun muassa linkit järjestelmän varaosalistaan ja järjestelmäkaavioon ja Valmetin tuen yhteystiedot. Vikatilanteet ja kyberuhkat on määritelty ja niihin on suunniteltu palautustoimenpiteet sekä laitteisto- että ohjelmistotasolla. Palautumissuunnitelmassa ei ole eroteltu, onko palautustoimenpiteet määritelty laiterikkojen vai haittaohjelmien varalle, koska niistä palautumiseen vaadittavat toimenpiteet ovat jotakuinkin samat. Palautumissuunnitelmalla koitetaan vastata asiakkaiden haluun parantaa tuotannon jatkuvuuden hallintaa. Kuvassa 13 on leike palautumissuunnitelmasta, jossa kuvataan DNA:n eri tasot palautusalueiden hahmottamiseksi. DNA:n palautumissuunnitelman sisällysluettelo on liitteessä 2.



KUVA 13. DNA-järjestelmän tasoja kuvaava kaavio (Valmet DNA Recovery Plan 2020)

5.2 RTO ja RPO

Palautumissuunnitelman lopussa määritellään asiakaskohtaisesti suurpiirteiset RTO- ja RPO-ajat. RTO on lyhenne englannin kielen termistä recovery time objective. RTO:lla tarkoitetaan tavoiteltua toipumisaikaa häiriötilanteen alkamisesta (Wallenius 2021). Esimerkiksi EAS:lle voidaan määritellä 8 tuntia tavoitelluksi toipumisajaksi, jolloin häiriötilanteen alkamisesta saa enimmillään kulua 8 tuntia siihen, että EAS on uudelleen toimintakunnossa.

RPO tulee englannin kielen sanoista recovery point objective, ja sillä tarkoitetaan tavoiteltua toipumispistettä (Wallenius 2021). Mikäli halutaan, että palautuspiste on maksimissaan 24 tuntia vanha häiriötilanteen alkamishetkestä, pitää varmuuskopioita ottaa päivittäin 24 tunnin välein.

RTO- ja RPO-ajat sovitaan asiakkaan kanssa. Varmuuskopiointi varaa kuitenkin aina tallennustilaa ja mahdollisesti verkkoa tietojen siirtoon, jonka vuoksi järjestelmän suorituskyky ei välttämättä riitä haluttuihin RPO- ja RTO-aikoihin. Mikäli asiakas haluaa palautumisen olevan nopeaa ja palautuspisteen olevan mahdollisimman tuore, muutetaan järjestelmää tarvittaessa suorituskykyisemmäksi ja palvelusopimusta niin, että Valmet takaa tietyn huoltonopeuden järjestelmälle. Edellä mainitut muutokset vaikuttavat palvelun kiinteisiin kustannuksiin.

6 PALAUTUMISSUUNNITELMAN TESTAUS

6.1 Testauksen suunnittelu

Tämän opinnäytetyön aiheena oli täydentää palautumissuunnitelmapohjaa testausosiolla. Palautumissuunnitelman testauksella on tarkoitus osoittaa, että järjestelmä voidaan palauttaa palautumissuunnitelman mukaisilla toimenpiteillä. Sen lisäksi testauksessa tarkistetaan palautumissuunnitelman paikkansapitävyys. Valmetin järjestelmä- ja kyberturvallisuusasiantuntijoiden neuvoja ja havaintoja apuna käyttäen koottiin lista tarkastettavia asioita noin vuosittain suoritettavaan palautumissuunnitelman testaukseen.

Testauksesta tehtiin tarkastuslista, joka on tämän opinnäytetyön liitteenä 1. Tarkoituksena oli koota listaan sellaista sisältöä, jolla osoitettaisiin järjestelmän ja laitoksen varautuminen häiriöiden varalle. Sen lisäksi siinä tarkastetaan järjestelmän kuntoa sellaisilta osilta, joita ei tavallisessa ennakkohuollossa tai tilankartoituksessa tehdä. Samalla tarkastetaan myös, että palautumissuunnitelman sisältö on ajan tasalla. Listatut asiat on tarkoitus vain tarkastaa ja korjaustoimenpiteet sovitaan asiakkaan kanssa sen jälkeen. Tarkastuslista toimii muistilistana tarkastusta tekevälle Valmetin toimihenkilölle, joka soveltaa sen sisältöä järjestelmäkohtaisesti. Kaikkia testejä tai tarkastuksia ei voida suorittaa kaikille järjestelmille.

6.1.1 Dokumentoinnin tarkastus

Aluksi listaan koottiin erilaisten järjestelmään liittyvien dokumenttien tarkastuksia. Palautumissuunnitelman tarkastuksella pidetään huolta siitä, että dokumentti ja sen sisältö on edelleen saatavilla. Järjestelmäkaavion tarkastuksella taas voidaan varmistaa, että se on saatavilla kaikille osapuolille ja että kaavion sisältö on ajan tasalla. Epäkohdat järjestelmäkaaviossa voivat aiheuttaa sekaannuksia häiriötilanteiden ratkaisuissa ja palautumisessa, etenkin jos sitä tutkiva Valmetin toimihenkilö ei ole ennen ollut tekemisissä kyseisen järjestelmän kanssa.

Varaosalistan ja -varaston tarkastuksella varmistutaan siitä, että häiriötilanteessa oikea varaosa on heti saatavilla paikan päällä tai mikäli sellainen pitää tilata, on se listattuna valmiiksi tilausta varten. Lisenssien ja sertifikaattien tallennus erilliseen sijaintiin on myös hyvä tarkastaa. Sen lisäksi, että ne ovat nopeasti saatavilla, on olennaista myös tarkistaa, että ne eivät ole vanhentumassa. Esimerkiksi OPC-sertifikaatille on myös asetettavissa järjestelmähälytys, joka on hyvä tarkastaa samassa yhteydessä. Valmet pyrkii lisäämään kaikkien sertifikaattien ja lisenssien tarkastuksen tilankartoituksen yhteyteen, jossa ohjelmalla kerätään järjestelmän diagnostiikka automaattisesti luotuun raporttiin. Toistaiseksi OPC:n ja vCenterin lisenssien tarkastus on kuitenkin tehtävä manuaalisesti.

Varmuuskopioiden kuntoa suositellaan tarkistettavan säännöllisesti, ja sitä varten on myös Valmetilla palvelu saatavilla. Kuukausittain tarkistetaan esimerkiksi BU-aseman ja NAS:n levytila ja kunto sekä niille siirrettävien varmuuskopioiden eheys ja onnistuminen, koska niistä ei ole järjestelmähälytystä saatavilla. Mikäli varmuuskopiointi epäonnistuu tai sen ajoitettu ottaminen ei ole käytössä, se voi jäädä huomaamatta pitkäksikin aikaa. Palautumissuunnitelman testauslistaan lisättiin kohta, että säännöllistä varmuuskopioiden tarkistusta on tehty ja että tarkistukset on dokumentoitu. Varmuuskopiotarkistuksista tarkastetaan myös, että kaikki tärkeät kohteet käydään tarkistuksessa läpi. Olennaiset tarkistuskohteet ovat järjestelmäkohtaisia, ja palautumissuunnitelman testaajan on selvitettävä ne.

6.1.2 Virustorjunnan ja varmuuskopioiden tarkastus

Tarkastuslistaan lisättiin virustorjunnan tilan tarkastaminen. Järjestelmän virustorjunnan hallinnointityökalulla nähdään, ovatko kaikki järjestelmän laitteet yhteydessä hallinnoijaan ja ovatko viruskuvaukset järjestelmässä ajan tasalla. Epäkohdat virustorjunnassa ovat selkeä puute tietoturvassa.

Varmuuskopioinnin osalta testauksessa tarkastetaan:

- DNA-varmuuskopiointi
  - eaBackupin kunto
  - BU-aseman db-pakettien kopiointi
  - EAS:lle tallennettavan BuBackup cpio -tiedoston kunto
  - ovatko verkkokytkinten ja reitittimien konfiguroinnit tallennettu erilliseen sijaintiin

- NAS / levykehikko
  - yleinen kunto
  - tallennustilan määrä
  - varmuuskopioiden kunto

- Avamar / vRanger
  - varmuuskopiointien ajoitus on kunnossa
  - kaikki tärkeät kohteet varmuuskopioidaan
  - varmuuskopiotiedostot ovat silmämääräisesti kunnossa

- Veritas System Recovery
  - varmuuskopioiden ajoitus kunnossa
  - kaikki tärkeät kohteet varmuuskopioidaan
  - tarkastetaan ohjelmiston virheilmoitukset
  - tarkastetaan jokin varmuuskopiotiedosto ohjelmiston sisäänrakennetulla tarkistustyökalulla.

Varmuuskopioiden tarkastuksen ajatuksena on varmistaa, että kaikki varmuuskopiointi on onnistunut. Näin laajaa varmuuskopioiden tarkastusta ei yleensä suoriteta. Sen lisäksi tarkastuksen tekijä voi huomata puutteita varmuuskopioinnissa. Esimerkiksi järjestelmään tehtyjen muutoksien myötä kaikkia tärkeitä varmuuskopiota ei välttämättä ole asetettu otettavaksi ja puutteita varmuuskopioinnissa ei usein havaita ennen kuin niitä olisi tarve käyttää.

6.1.3 Käytännön tekniset harjoitukset

Varsinaiseen käytännön testaukseen listattiin neljä testiä, joilla voidaan osoittaa, että järjestelmän palautuminen onnistuu käytännössä. Käytännön testaukset vaativat yleensä paljon aikaa, joten montaa testiä ei liene järkevää suorittaa jokaisella testauskerralla. Seuraavat testaukset ovat esimerkkejä testeistä, joita voidaan soveltaa järjestelmäkohtaisesti.

Varmuuskopiosta palauttaminen

Ensimmäisen testin tarkoituksena on, että jokin fyysinen tai virtuaalinen kone palautetaan varmuuskopiosta. Palautus on kannattavaa tehdä turvalliseen ympäristöön, ettei palautuksen mahdollisista virheistä synny haittaa laitoksen toiminnalle. Virtuaalikone voidaan palauttaa vaikkapa Valmetin omaan virtuaaliympäristöön tai fyysinen kone erilliseen verkosta pois kytkettyyn koneeseen. Palautustesti toimii osoituksena siitä, että varmuuskopiotiedosto on eheä ja sen palauttamisprosessi voidaan toteuttaa käytännössä. Samalla harjoitellaan myös palautustoimenpiteitä. Palautestin etu on, että se voidaan suorittaa häiritsemättä tuotantolaitoksen toimintaa.

Varaosan vaihtotesti

Varaosan vaihtotestissä vaihdetaan jokin järjestelmän osa, kuten prosessiasema tai verkkokytkin. Vaihto tulee suorittaa seisokin tai muuten sopivana aikana. Joillakin laitoksilla ei ole kahdennettua prosessinohjausta, jolloin valmiiksi konfiguroitu prosessiasema on syytä olla varalla, valmiiksi vaihdettavana tilanteen tullen. Vaihtotestillä voidaan osoittaa, että vaihtoa on harjoiteltu, ja varmistutaan, että varaosa on valmiiksi saatavilla ja oikein konfiguroituna.

Korkean saatavuuden testaus

Virtuaaliympäristön korkeaa saatavuutta voidaan testata aiheuttamalla jokin häiriö tai katkos yhdelle ESXi-alustalle esimerkiksi sammuttamalla kyseinen alusta. Alustassa olevien virtuaalikoneiden tulisi sen jälkeen automaattisesti latautua levypakalta toiselle ESXi-alustalle, josta ne voidaan käynnistää ja ottaa käyttöön.

Palomuurin/kytkimen kahdennustestaus

Lopuksi lisättiin vielä testi palomuurillisen reitittimen kahdennukselle. Sen tarkoituksena on testata kahdennuksen toimintaa, mikäli toinen palomuureista vikaantuu tai ylikuormittuu. Testi voidaan toteuttaa esimerkiksi irrottamalla reitittimestä kaapeli tai kaapeleita, jolloin siitä pitäisi aiheutua järjestelmähälytys ja varalla oleva reititin otetaan automaattisesti käyttöön.

6.1.4 Kriisiharjoittelu teoriassa

Testauslistan viimeinen osa on tarkoitettu keskustelupohjaisille, niin sanotuille tabletop-harjoituksille. Osuuteen lisättiin kaksi kuivaharjoitteluesimerkkiä, joissa asiakkaan organisaation kanssa käydään läpi skenaario, jossa jokin laite rikkoutuu tai haittaohjelma saastuttaa järjestelmän. Keskustelussa on tarkoitus selvittää yhteistyössä ongelman ratkaisu ja sen kulku todellisessa tilanteessa. Keskustelussa on myös syytä käydä läpi osallistujien roolit tilanteessa.

7 PALAUTUMISSUUNNITELMAN TESTAUKSEN KOESTUS

7.1 Testauksen järjestäminen

Testauksen suunnittelun lisäksi sitä koestettiin eräällä Valmetin asiakkaan järjestelmällä. Asiakkaalle oli suunniteltu palautumissuunnitelma keväällä 2020, ja sen testauksesta oli ollut jo silloin puhetta. Testaus valmisteltiin Valmetin ja asiakkaan välillä Teams-palaverissa. Palaverissa sovittiin, että testaus tehtäisiin kehitysyhteistyössä, jolloin osapuolet vastaisivat vain omista kuluistaan. Tarkastuslistan läpikäynnin lisäksi suoritettaisiin Info-virtuaalikoneen palautus Valmetin Servicen testiympäristöön. Asiakkaan laitos ei järjestä suunniteltuja seisakkeja vaan tuotanto pidetään käynnissä ympäri vuoden, jonka takia käytännön harjoittelu on rajallista. Siitä syystä ainoa suunniteltu käytännön harjoitus, joka voitiin suorittaa riskeittä, oli virtuaalikoneen palautus. Tarkistukset tehtäisiin etäyhteydellä ja infopalvelimen palautustiedosto siirrettäisiin Tampereelle palautusta varten.

7.2 Testaustulokset

Dokumentaatio

Palautumissuunnitelmasta löytyi muutamia epäkohtia. Kuvassa 14 on esitelty palautumissuunnitelman kohta, joka sisältää linkit järjestelmäkaavioon, varaosalistaan, varmuuskopioiden tarkistuslistaan ja elinkaaren seurantalistaan. M-Files -tiedonhallintajärjestelmässä olevien PDF-tiedostojen nimet ovat muuttuneet palautumissuunnitelman laatimisen jälkeen, joten linkit eivät johda mihinkään. Linkit voisi korvata esimerkiksi niin, että ne johtaisivat siihen hakemistoon, missä tiedostot sijaitsevat. Palautumissuunnitelman yleinen toiminta on hyvä pitää kunnossa, että se toimii asianmukaisena dokumenttina ja toimivana oppaana.

Appendix	Description	Document ID
System part list	parts and spare parts	[redacted] Installed_base.pdf (Desktop, Web, Mobile) [redacted] Spare_part_list.pdf (Desktop, Web, Mobile)
System layout		Järjestelmäkaavio_17.2.2020.pdf (Desktop, Web, Mobile)
Backup list	Follow up list for backup's	SH01- ja [redacted] EAS1-palvelinten varmistuksien seurantapäiväkirja - 10.1.2020.xls (Desktop, Web, Mobile)
Life cycle plan		[redacted] elinkaarisuunnitelma 31.01.2020.xlsx (Desktop, Web, Mobile)

KUVA 14. Asiakkaan palautumissuunnitelman liitelista

Palautumissuunnitelmassa oli myös huomio siitä, että verkkokytkinten ja reitittimien konfigurointeja ei ole tallennettu erilliseen sijaintiin, kuten BU-asemalle. Sen lisäksi myös suunnitelman loppuun ei ollut kirjattu RTO- ja RPO-aikoja (kuva 15), jotka tulisi selvittää ja sopia asiakkaan kanssa. Sen sijaan RPO-kohtaan oli merkattu vain sijainti, josta palautus voidaan tehdä.

Component	RTO (time)	RPO (recovery point)	Notes (Start point / findings)
DNA EAS	8h	Vranger backup	vaihto työ
DNA Info	8h	Vranger Backup	vaihto työ
DNA Alarm	2h	BU station	vaihto työ
DNA PCS	2h	BU station	vaihto työ
DNA OPC	8h	Vranger Backup	vaihto työ

Virtualization	RTO (time)	RPO (recovery point)	Notes (Start point / findings)
ESXi host		Running ESXi host	
vSphere hypervisor		vCenter manage	
Storage		external backup	
Storage network		BU station backup	
Management Network		BU station backup	
NTP Daemon		external backup	
DNS		external backup	

KUVA 15. Asiakkaan RTO- ja RPO-listaus

Asiakkaan varaosalistassa kahden operointiasemien nimet olivat vielä oletusarvoissa, ja ne tulisi muuttaa. Järjestelmän varaosalista luodaan tilankartoituksen

yhteydessä automaattisesti, joten nimenvaihto pitää tehdä muuttamalla Windows-työaseman nimeä.

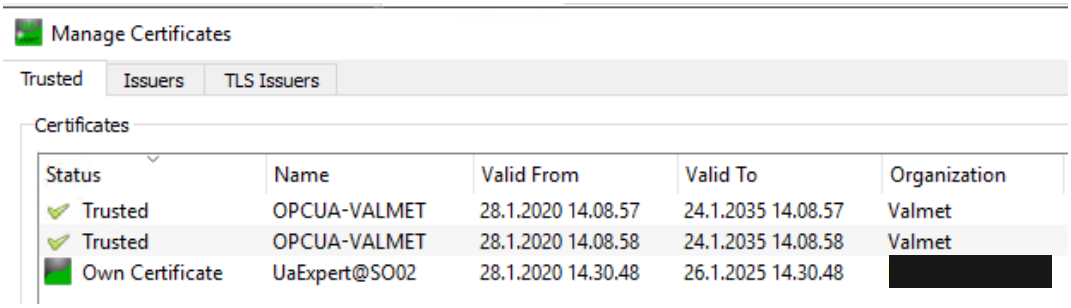
DESKTOP-DNBJL6T	Operator station	ACN PO DC G5 ([redacted]) Windows 10 Enterprise LTSC DNA C2018
DESKTOP-DNBJL6T	Operator station	ACN PO DC G5 ([redacted]) Windows 10 Enterprise LTSC DNA C2018
M1O1	Operator station	ACN PO DC G5 ([redacted]) Windows 10 Enterprise LTSC DNA C2018
M1O4	Back-up station	ACN PO DC G5 ([redacted]) Windows 10 Enterprise LTSC
M1O5	Operator station	1.0 CP62xx-0060 ([redacted]) Windows 10 Enterprise 2015 LTSB DNA C2018

KUVA 16. Leike asiakkaan varaosalistasta

Asiakkaan omien varaosien tilanne tulisi myös kartoittaa. Vaikka järjestelmä onkin kahdennettu, olisi syytä tutkia, mitä kriittisiä varaosia, kuten kytkimiä tai reitittimiä, olisi syytä olla valmiina varastossa.

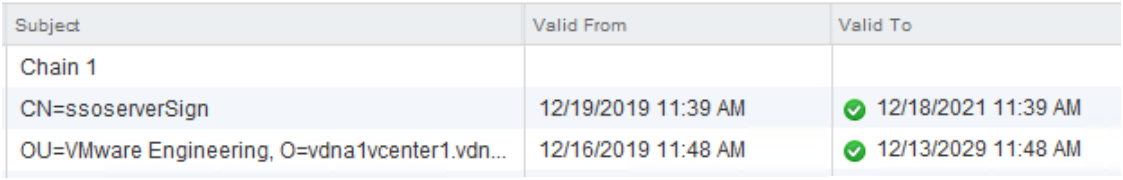
Myös järjestelmäkaaviosta löytyi muutama puute, joka olisi syytä korjata. Virtuaaliympäristön toista ESXi-alustaa ei ollut merkattuna järjestelmäkaavioon. Kyseisellä alustalla tehdään vRanger-varmuuskopiointia virtuaalikoneista. Sen merkitseminen kaavioon on olennaista, jotta vikatilanteessa järjestelmän korjaaja näkee alustan olemassaolon ja sen osoitteen suoraan kaaviosta. Järjestelmäkaaviossa olisi myös hyödyllistä olla jokin merkintä sille koneelle, joka toimii etäyhteyskoneena.

Lisenssien ja sertifikaattien osalta todettiin, että ne ovat tallennettuna oikeaoppisesti M-Files -järjestelmään. OPC UA:n sertifikaatit ovat vielä vuosia voimassa (kuva 17). Sertifikaatin vanhenemisesta voisi asettaa järjestelmään hälytyksen.



KUVA 17. OPC UA -virtuaalikoneen sertifikaatti-ikkuna

VMware vCenterin konfigurointityökalujen lisenssi on vanhenemassa 10 kuukauden päästä testauksesta (kuva 18). Lisenssin uusiminen tulisi sopia ennen sitä.

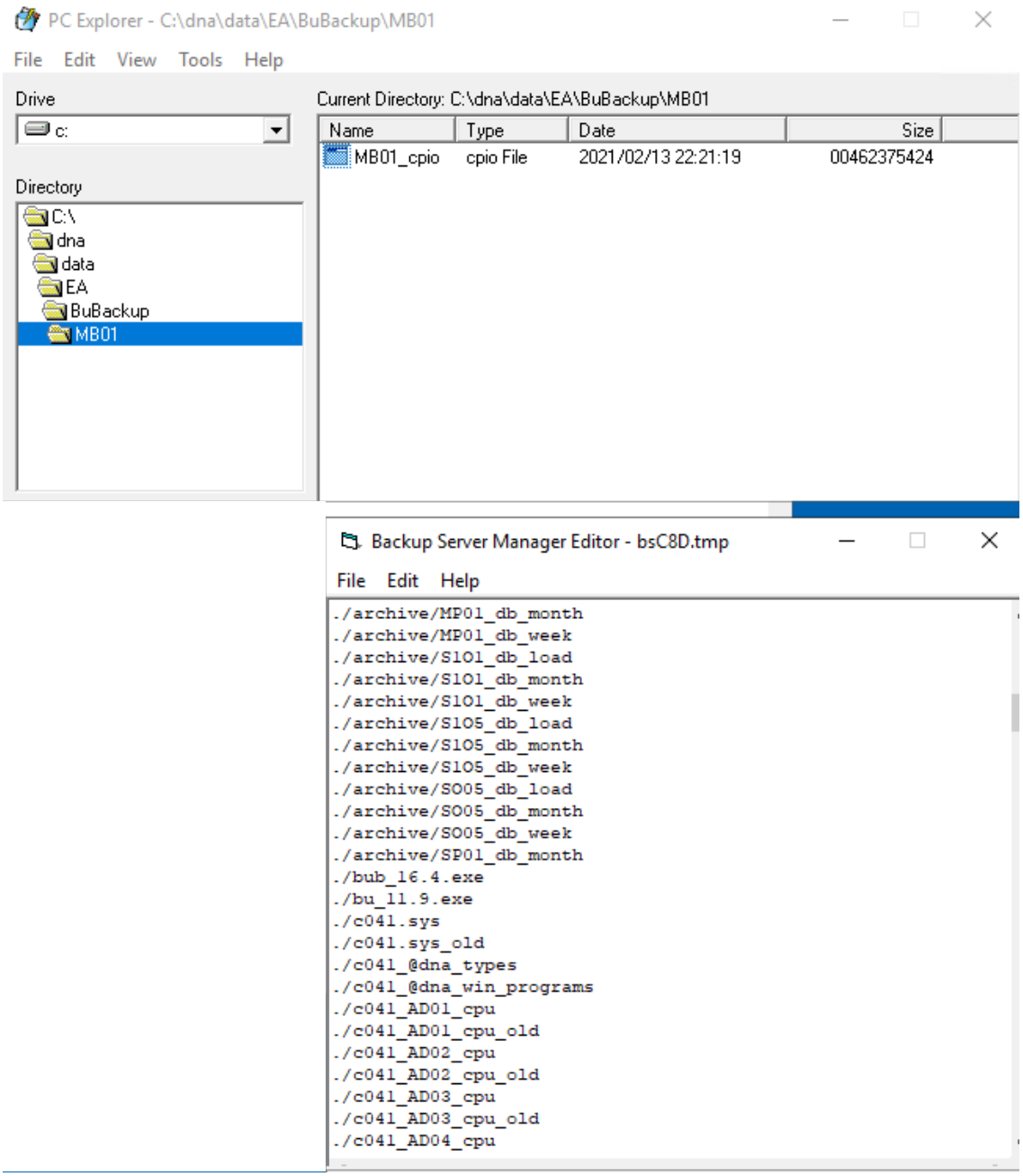


KUVA 18. VMware vCenter -ohjelmiston lisenssien voimassaoloaika

Varmuuskopioiden tarkistusta on tehty säännöllisesti kuukauden välein raporttien perusteella. Tarkistuksessa käydään läpi EAS- ja INFO-virtuaalikoneiden varmuuskopioiden onnistuminen. Varmuuskopiot otetaan vRanger-ohjelmistolla ja ne siirretään myös erilliselle NAS:lle. Tiedostojen kunnon tarkistus tehdään molemmista kohteista ja samalla tarkistetaan asemien levytila. Varmuuskopioinnille tehtävä säännöllinen tarkistus on tarpeeksi kattava kyseiselle järjestelmälle.

DNA-varmuuskopiointi

DNA:n varmuuskopioinnin osalta järjestelmä oli hyvässä kunnossa. BU-aseman db-pakettien viikko- ja kuukausikopiot oli otettu onnistuneesti. Cpio-tiedostoon tallennettava BU-asemasta EAS:lle otettu varmuuskopio oli onnistunut. BU-aseman cpio-tiedosto tarkastettiin DNA:n Backup Server Manager -ohjelmistolla (kuva 19). Samalla tarkastettiin BU-aseman resurssien käyttö, vaikka ylikuormituksesta on myös järjestelmähälytys asetettuna. Resurssiarvot olivat hyvät: CPU-käyttö 17 % ja 5,5 GB välimuistia käytettävissä. Ainoa puute oli jo aiemmin mainittu verkkokytkinten konfigurointien kopioiden puuttuminen.



KUVA 19. Leike cpio-tiedoston sisällön tarkastuksesta

NAS

Asiakkaalla oli käytössä erillinen NAS, jonne talletettiin vRangerin varmuuskopiot. NAS:n varmuuskopiot olivat silmämääräisesti kunnossa ja levytilaa oli vielä reilusti vapaana.

vRanger

Virtuaaliympäristössä käytettävä vRanger oli asetettu ottamaan täydet varmuuskopiot kaikista virtuaalikoneista joka yö. Tilankäytön puolesta täydet varmuuskopiot sopivat järjestelmään, koska tallennustilaa oli riittävästi sekä vRanger:n käytössä, että NAS:lla. vRangerin varmuuskopioinnissa ei huomattu virheitä.

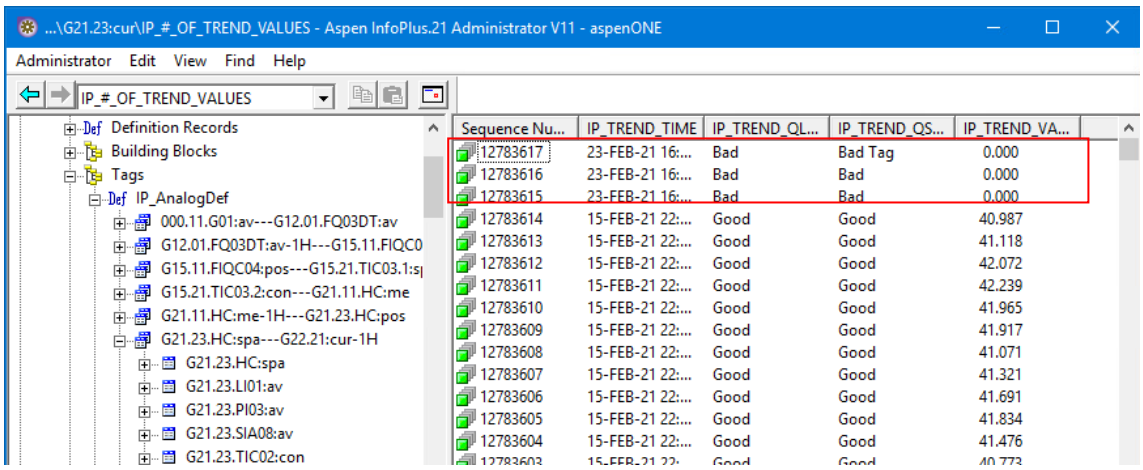
Palautustesti

INFO-palvelimen palautus toistettiin Valmetin virtuaalitestiympäristöön kahdesti eri palautustiedostoista. Palautukseen kului aikaa molemmilla kerroilla noin 1 tunti ja 20 minuuttia (kuva 20), joka on hyvä tulos verraten palautumissuunnitelmassa ilmoitettuun RTO-aikaan, joka on kahdeksan tuntia.

Destination	Start Time	End Time	Duratio
172.20.131.10->SH02	2/23/2021 4:38:45 PM	2/23/2021 6:02:26 PM	01:23:40
172.20.131.10->SH02	2/23/2021 2:06:48 PM	2/23/2021 3:24:42 PM	01:17:54

KUVA 20. Testiympäristön palautustöiden tiedot

Palauttamisen jälkeen virtuaalikone käynnistettiin ja todettiin, että Windows-käyttöjärjestelmä ja Aspen-tiedonkeruusovellus toimivat normaalisti. Kuvassa 21 on esitelty tiedonkeruusovelluksen keräämiä prosessiarvoja tietystä positiosta. Viimeisimmät kolme arvoa on korostettu ja niistä huomataan, että sovellus yrittää kerätä prosessidataa, jota ei testiympäristöstä löydy. Näin ollen voidaan todeta, että tiedonkeruu toimii.



KUVA 21. Palautetun INFO-koneen tiedonkeruusovelluksen arvoja

7.3 Yhteenveto

Testitulokset raportoitiin vielä erilliseen Word-dokumenttiin Excel-tarkastuslistan lisäksi, jossa kuvailtiin ja analysoitiin tarkemmin testien tulokset. Tärkeimmät korjausehdotukset olivat:

- palautumissuunnitelman ja järjestelmäkaavion päivitys
- M1O2- ja M1O3-operointiasemien isäntänimien päivitys
- verkkokytkinten ja reitittimien konfigurointien lisäys esimerkiksi BU-asemalle
- vCenterin konfigurointityökalujen lisenssin uusiminen
- asiakkaan varastoon tarvittavien varaosien kartoitus

Tulokset käytiin läpi asiakkaan henkilöstön kanssa. Yhteenvetona todettiin, että yllä olevan listan mukaiset korjaustoimenpiteet tehdään. Etenkin kytkinten ja reitittimien konfigurointien tallennusta sekä varaosien kartoittamista pidettiin tärkeänä. Testaus koettiin sekä Valmetin, että asiakkaan puolesta hyödylliseksi. Jatkossa testausta sovittiin tehtäväksi noin vuoden välein. Testauksen tarkastuslistan sisältöä arvioitaisiin jatkossa uudelleen. Kaikkia tässä työssä tarkastettavia asioita ei ole tarpeen tarkastaa vuosittain. Testaus voisi esimerkiksi olla minimissään palautumissuunnitelman tarkastus ja jokin keskustelupohjainen harjoitus.

8 JOHTOPÄÄTÖKSET JA POHDINTA

Opinnäytetyön tuloksena Valmet DNA -automaatiojärjestelmän palautumissuunnitelmalle saatiin kehitettyä alustava testaussuunnitelma, jota voidaan käyttää palautumiskyvyn testauksessa ja sen ylläpidossa apuna. Testauksen avulla voidaan osoittaa, että palautumissuunnitelma on ajan tasalla ja että suunnitelman palautustoimenpiteet ovat toteutettavissa myös käytännössä.

Palautumissuunnitelmaan testaukseen kehitetty suunnitelma saatiin toteutettua odotetulla tavalla. Kokonaisuudessaan työn tuloksena syntyi Excel-tarkastuslistapohja Valmetille ja täydennetty versio asiakkaan palautussuunnitelman testauksesta. Asiakkaalle luotiin myös erillinen raportti testauksesta, ja sen lisäksi asiakkaan palautumissuunnitelman dokumentaatiota täydennettiin testauksen osalta. Valmet Automation Oy jatkokehittää testauspohjaa jatkossa eri asiantuntijoiden näkemysten ja asiakkaiden palautteiden perusteella.

Palautumisen testauksella pitää vastata asiakkaan vaatimuksiin, joihin vaikuttaa yhä enemmän yritysten halu parantaa toiminnan jatkuvuuden hallintaa. Yleisesti palautumissuunnitelman tarkoitus on vähentää palautumiseen kuluvaa aikaa ja toimia osoituksena siitä, että järjestelmästä huolehditaan. Kokemus palautumissuunnitelman testauksen tärkeydestä ja sisällöstä voi kuitenkin olla subjektiivinen, minkä vuoksi palautumissuunnitelma ja sen testaus pitää käsitellä asiakaskohtaisesti. Asiakkaan täytyy kokea, että palautumissuunnitelman testauksesta on jotain hyötyä.

Työn ydin ja myös sen haastavin osuus oli määrittää testauskokeet ja tarkastuskohteet. Niiden kartoittamisessa tuli perehtyä järjestelmään tarkasti, jotta voitiin valita toteutettavia, palautumiskykyyn liittyviä ja merkityksellisiä testausmetodeja. Oman haasteensa loi myös se, että ne laitokset, jotka haluavat erilaisia kyberturvallisuuspalveluita kuten palautussuunnitelman laadinnan, käyttävät myös Valmetin järjestelmähuoltopalveluja ja noudattavat elinkaarisuunnitelmia. Näin ollen laitoksille tehdään järjestelmän vuosihuoltoja ja tilankartoituksia, joissa tarkistetaan ja huolletaan järjestelmää. Sen vuoksi palautumissuunnitelman tarkastuslistaan piti valita sellaisia kohtia, joita ei normaalisti tarkasteta. Tässä työssä asiak-

kaalle tehdyssä palautussuunnitelman testauksessa ei olisi välttämättä ollut tarpeen tarkastaa esimerkiksi BU-aseman resurssiarvoja tai virustorjunnan tilaa, mutta toisaalta kyseiset tarkastukset ovat helppoja ja nopeita tehdä.

Testaukseen saatiin sisällytettyä sopiva määrä tarkastettavia asioita ja esimerkkejä käytännön harjoituksista, joita voitaisiin käyttää testauksessa. Tarkastusten läpikäyntiin menee järjestelmäasiantuntijalta enimmillään pari työpäivää riippuen järjestelmän koosta ja tarkastuksessa ilmenevistä ongelmista ja selvitystä vaativista asioista. Käytännön harjoitukset voivat vaatia enemmän aikaa ja suunnittelua, ja niissä pitää myös huomioida riskit ja harjoituksen sopivuus testattavaan järjestelmään. Sen vuoksi niitä ei kuvailtu testiraportin esimerkkiharjoituksiin kovinkaan tarkasti.

Kokonaisuudessaan palautussuunnitelman testauksen suunnittelu painottui enemmän järjestelmän tekniselle puolelle. Valmetilla on kriisiharjoittelusta ja keskustelupohjaisista harjoitteluista toistaiseksi vähän kokemusta DNA-järjestelmän osalta, joten niiden järjestäminen osana tätä opinnäytetyötä olisi voinut olla liian haastava toimenpide. Voidaan kuitenkin todeta, että työssä saavutettiin sille asetetut tavoitteet. Valmet voi alustavan palautussuunnitelman testauslistan ja tehdyn testauksen koestuksen avulla jatkokehittää palveluaan.

LÄHTEET

Broadcom cyber security. 2021. Broadcom. Verkkosivu. https://www.broadcom.com/products/cyber-security

DNA yleisesittely. 2015. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 4.2.2021.

Forsman, J. 2020. Asiantuntija, koulutuspalvelut. Valmet DNA peruskurssi. Koulutuskurssi. Toukokuu 2020. Valmet Automation Oy. Tampere.

Life Cycle Approach. Valmet Automation Oy. Verkkosivu. Luettu 5.2.2021. https://www.valmet.com/automation/distributed-control-system/life-cycle-approach/

NIST Special Publication 800-184 Guide for Cybersecurity Event Recovery. 2016. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

Stenvik, M. 2020. Collection 2020 Network. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 19.2.2021.

Valmet DNA Automated Process. 2015. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 4.2.2021.

Valmet DNA Backup Concept 1.0. 2021. Valmet Automation Oy, Sisäinen materiaali. Luettu 4.2.2021.

Valmet DNA C2019 Cyber Security. 2019. Valmet Automation Oy. Sisäinen materiaali. Luettu 25.2.2021.

Valmet DNA Cyber Security. 2019. Valmet Automation Oy. Sisäinen materiaali. Luettu 25.2.2021.

Valmet DNA Cyber Security White Paper v3r4. 2020. Valmet Automation Oy. Sisäinen materiaali. Luettu 25.2.2021.

Valmet DNA Network Architecture. 2016. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 4.2.2021.

Valmet DNA Network Architecture DMZ. 2016. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 4.2.2021.

Valmet DNA Recovery Plan. 2020. Valmet Automation Oy. Sisäinen materiaali. Luettu 25.2.2021.

Valmet DNA Security - Malware Protection. Versio 1.2. 2016. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 24.2.2021.

Valmet DNA Suunnittelu- ja ylläpitotyökalut. 2015. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 4.2.2021.

Valmet DNA system architecture. Valmet Automation Oy. Verkkosivu. Luettu 5.2.2021. https://www.valmet.com/automation/distributed-control-system/system-architecture/

Virtualized DNA in VMware. 2016. 2016 versio. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 4.2.2021.

Virtualized DNA in VMware. 2021. 2021 versio. Valmet Automation Oy. Sisäinen koulutusmateriaali. Luettu 4.2.2021.

Wallenius, N. 2021. 5 jatkuvuudenhallinnan termiä, jotka jokaisen pitäisi hallita. Blogikirjoitus. Julkaistu 5.2.2021. Luettu 3.3.2021. https://niklaswallenius.fi/jatkuvuussuunnittelu-termit/

LIITTEET

Liite 1. Valmet DNA -palautumissuunnitelman testausraportti

PRELIMINARY

Valmet DNA Recovery Plan Test Report

Mill
Date

Serviced by

DNA Recovery plan test checklist

Name	Description	OK	Issues	Notes
Documentation				
	Recovery Plan	☐	☐	
	-is available			
	-is up to date (skim through)	☐	☐	
	System layout			
	-is available	☐		
	-is up to date:			
	· Any missing information	☐	☐	
	· Any removed system in layout	☐	☐	
	· All recent updates have been updated to layout	☐	☐	
	Spare part list			
	-is available	☐	☐	
	-is up to date			
	-customer has the critical spare parts in storage	☐	☐	
	Licenses and certificates			
	-are stored/available	☐	☐	
	-certificates are not expiring/expired			
	· vCenter, OPC UA etc	☐	☐	
	-expiration alarm is set (OPC)	☐	☐	
	Periodical backup check reports			
	-are being done	☐	☐	
	-are available			
	-all important backup targets are checked	☐	☐	

1 (4)

DNA Recovery plan test checklist

Name	Description	OK	Issues	Notes
Antivirus	**SEP manager**			
	-all windows nodes are connected to av-server	☐	☐	
	-all clients have latest virus definitions	☐	☐	
Backups	**DNA backups**			
	-eaBackup is valid and on time	☐	☐	
	-all db packets are backed up	☐	☐	
	-EAS's BuBackup cpio file condition (Open with BSGUI)	☐	☐	
	-Network switch and router configuration files stored	☐	☐	
	NAS / Disk array			
	-is up and running	☐	☐	
	-disk space	☐	☐	
	-Backup files are on time and valid	☐	☐	
	Avamar / vRanger			
	-backups are scheduled	☐	☐	
	-all important VM/files are backed	☐	☐	
	-Backup files are on time and valid	☐	☐	
	Veritas System Recovery			
	-backups are scheduled	☐	☐	
	-all important files or nodes are being backed up (EAS, BU etc)	☐	☐	
	-any errors in scheduled backups	☐	☐	
	-verify a backup file to make sure	☐	☐	

DNA Recovery plan technical exercises

Name	Description	OK	Issues	Notes
Examples that can be applied system-specifically or customized to suit a certain system.				
Backup restore test	Recover a machine (physical or virtual) to a safe environment to verify that a machine can be actually recovered with a backup file. Report the RTO result time to the RP section 5.20.	☐	☐	
Spare part swap test	During a maintenance downtime of the plant, swap a spare part (PCS, network switch, etc) to the system to confirm that the spare part is pre-configured correctly and to train the swap process.	☐	☐	
High Availability test	Test vCenter high availability function by shutting down one ESXi platform and then starting the VMs from another ESXi.	☐	☐	
Firewall/router redundancy test	During a maintenance downtime and otherwise safe time, test the firewall/router redundancy. This can be done by disconnecting some cables and monitoring if the redundant switch takes over.	☐	☐	

DNA Recovery plan tabletop exercises

Name	Description	OK	Issues	Notes
System breakdown scenario	Go through a scenario with the customer's system responsible where a network or process controller device breaks down. In co-operation figure out the roles and steps how the system can be recovered in real situation.	☐	☐	
Malware scenario	Go through a scenario with the customer's system responsible where a malware has been detected in the system. In co-operation figure out the roles and steps how the system can be recovered in real situation.	☐	☐	

Comments	- In this section we list up all the comments and recommendations - to the "Notes" coloumn name also the attachment where the appropriate information can be found. - new line in this cell: ALT+Enter

Liite 2. Valmet DNA -palautumissuunnitelman sisällysluettelo (Valmet DNA Recovery Plan 2020)

Table of Contents