

Palautumissuunnitelma palvelun- tarjoajan GPON-verkkolaitteistolle

Joonas Viinikainen

Opinnäytetyö
Marraskuu 2016
Tekniikan ja liikenteen ala
Insinööri (AMK), tietotekniikan koulutusohjelma

Tekijä(t) Viinikainen Joonas	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä Marraskuu 2016
	Sivumäärä 62	Julkaisun kieli Suomi
		Verkojulkaisulupa myönnetty: x
Työn nimi Palautumissuunnitelma palveluntarjoajan GPON-verkkolaitteistolle		
Tutkinto-ohjelma Tietotekniikan koulutusohjelma		
Työn ohjaaja(t) Rantonen Mika Kotikoski Sampo		
Toimeksiantaja(t) Keski-Suomen Valokuituverkot Oy		
Tiivistelmä <p>Opinnäytetyön toimeksiantajana toimi Keski-Suomen Valokuituverkot Oy. Keski-Suomen Valokuituverkot Oy rakentaa laajakaistaverkkoa sekä tarjoaa Internetpalveluita Keski-Suomessa.</p> <p>Työn tarkoituksena oli hankkia tietoa palautumissuunnittelusta ja kartoittaa yrityksen GPON-verkkolaitteiston toimintaan vaikuttavat riskit. Työssä myös suunniteltiin ja testattiin yrityksen GPON-verkkolaitteiston toiminnan palauttamiseen kuuluvat toimenpiteet. Verkkolaitteistoon kuului GPON -kytkinten keskitetty hallintapalvelin (CMS) sekä eri kunnissa sijaitsevat Calix E7-2 GPON -kytkimet. Palauttamisessa käytiin läpi toimenpiteet, joita vaadittiin laitteiden palauttamiseen.</p> <p>Laiterikon jälkeisen palauttamisen testaus toteutettiin yrityksen testiympäristössä Jyväskylässä. GPON -kytkimen palauttaminen toteutettiin korvaamalla laite uudella ja palauttamalla vioittuneen laitteen konfiguraatio korvaavaan laitteeseen. CMS-palvelimen palauttamista testattiin palauttamalla demovirtuaalikoneen varmuuskopio Veeam Backup & Replication -palvelimelta tuotantoympäristöön.</p> <p>Työn tuloksena saatiin selvitettyä eri sijainneissa olevien laitteiden likimääräiset palautusajat sekä testattua palvelimen ja kytkinten palauttaminen. Dokumentaatiota voidaan käyttää työohjeena laitteiston palauttamisessa.</p>		
Avainsanat (asiasanat) Palautumissuunnitelma, GPON, PON, CMS, Calix E7-2		
Muut tiedot		

Author(s) Viinikainen Joonas	Type of publication Bachelor's thesis	Date November 2016 Language of publication: Finnish
	Number of pages 62	Permission for web publication: x
Title of publication Recovery planning for service provider's GPON-network devices		
Degree programme Information Technology		
Supervisor(s) Rantonen Mika Kotikoski Sampo		
Assigned by Keski-Suomen Valokuituverkot Oy		
Abstract <p>This bachelor's thesis was assigned by Keski-Suomen Valokuituverkot Oy. Keski-Suomen Valokuituverkot Oy builds a broadband network and provides internet services in the territory of Central Finland.</p> <p>The purpose of this thesis was to gather information about recovery planning and to identify the risks affecting the company's GPON-network device operations. The thesis includes planning and testing the required operations to recover the company's GPON-network devices. The Network devices included the GPON switches management server (CMS) and the Calix E7-2 GPON switches located in different municipalities. The recovery included the operations needed to recover the devices.</p> <p>The recovery after a hardware failure was implemented in a test environment in Jyväskylä. A recovery of a GPON-switch was carried out by replacing the device with a new one and restoring the configuration to the replacement device. The recovery of a CMS-server was tested by restoring a backup of demo virtual machine to the production environment from a Veeam Backup & Replication server.</p> <p>As a result of the thesis, the approximate recovery time of the devices in different locations was determined, and the recovery of the server and switches was tested. The documentation can be used as a working instruction when recovering the devices.</p>		
Keywords/tags (subjects) Recovery Planning, Disaster Recovery, GPON, PON, CMS, Calix E7-2		
Miscellaneous		

Sisältö

1	Työn lähtökohdat	7
1.1	Tutkimusongelma	7
1.2	Tutkimusmenetelmät	8
1.3	Opinnäytetyön tavoitteet.....	9
1.4	Ajankohtaisuus	9
1.5	Toimeksiantaja	10
2	Suunnittelua tukeva teoria	11
2.1	Yleistä	11
2.1.1	Optinen tiedonsiirto	11
2.1.2	APC.....	12
2.1.3	Jaotin.....	13
2.1.4	PON.....	14
2.2	Palautumissuunnittelun hyödyt	16
2.3	MTD	16
2.4	RTO	16
2.5	RPO	17
2.6	Palautumisaika	17
2.7	Palvelutasot.....	17
2.8	Veeam Backup & Replication v9.0	18
2.8.1	Komponentit.....	18
2.8.2	Data Compression & Deduplication	19
2.8.3	Varmuskopiointimenetelmät	20
2.8.4	Tuetut ympäristöt.....	22
2.9	Palautumissuunnittelua koskeva laitteisto	23
2.9.1	CMS.....	23
2.9.2	Calix E7-2:n runko.....	23

	2
2.9.3 GPON-4R2 linjakortti	24
3 Palautumissuunnittelu.....	24
3.1 Riskianalyysi.....	24
3.2 Tiimin henkilöstö	26
3.3 Kommunikointi vian sattuessa	26
3.4 Varalaitteisto	27
3.5 Sähkönsyöttö.....	27
3.6 Verkon redundanttisuus.....	28
3.7 Vasteajat.....	30
3.8 Calix E7-2:n palautus	33
3.9 CMS-palvelimen palautus.....	33
4 Toteutus.....	34
4.1 Testausympäristö	34
4.2 Calix E7-2:n ajastettu varmuuskopiointi	35
4.3 Calix E7-2:n palautus	38
4.4 CMS-palvelimen ajastettu varmuuskopiointi.....	45
4.5 CMS-palvelimen palautuksen testaus	54
5 Yhteenveto.....	61
5.1 Pohdinta	61
5.2 Jatkokehitysideat.....	62
Lähteet	63
Liitteet.....	65
Liite 1. Riskianalyysi	65

Kuviot

Kuvio 1. Verkkoalue.....	10
Kuvio 2. Optinen tiedonsiirto	12
Kuvio 3. 19" 1:32 SC APC-jaotin	13
Kuvio 4. Jaottimen periaate	14
Kuvio 5. PON.....	15
Kuvio 6. Forever forward incremental	21
Kuvio 7. Forward incremental	21
Kuvio 8. Reverse incremental.....	22
Kuvio 9. Riskin määritteitä	25
Kuvio 10. Sähkönsyöttö.....	28
Kuvio 11. Rinkiverkon toiminta 1	29
Kuvio 12. Rinkiverkon toiminta 2	30
Kuvio 13. Palautusajat	32
Kuvio 14. Varmuuskopioinnin arkkitehtuuri	33
Kuvio 15. Testauslaitteisto	35
Kuvio 16. E7 backup-vaihe 1	36
Kuvio 17. E7 backup-vaihe 2	36
Kuvio 18. E7 backup-vaihe 3	37
Kuvio 19. E7 backup-vaihe 4	37
Kuvio 20. E7 backup-vaihe 5	38
Kuvio 21. Testausympäristö	38
Kuvio 22. Varalaitte	38
Kuvio 23. Turnup	39
Kuvio 24. kirjautuminen	40
Kuvio 25. Interface enable	40
Kuvio 26. Role trunk	41
Kuvio 27. VLAN Create	41
Kuvio 28. VLAN Create	42
Kuvio 29. VLAN member	42
Kuvio 30. VLAN member	43
Kuvio 31. Backup load	43

Kuvio 32. FTP information	44
Kuvio 33. Backup switch	44
Kuvio 34. Backub job	45
Kuvio 35. Job name	46
Kuvio 36. Työn kohteet	47
Kuvio 37. Storage.....	48
Kuvio 38. AS backup	49
Kuvio 39. AS Notifications	50
Kuvio 40. AS Storage	51
Kuvio 41. Guest processing	52
Kuvio 42. Schedule	53
Kuvio 43. Summary.....	54
Kuvio 44. Restore entire VM	55
Kuvio 45. Restore Point	56
Kuvio 46. Restore Mode	57
Kuvio 47. Restore reason	58
Kuvio 48. Summary.....	59
Kuvio 49. Upload nopeus	59
Kuvio 50. Restore logs	60
Kuvio 51. VM:n tilan tarkistus	60
Kuvio 52. VM:n toiminta	61

Taulukot

Taulukko 1. Jakovaimennukset	14
Taulukko 2. PON standardeja	15
Taulukko 3. Matkustusajat laiteloittain	31
Taulukko 4. Palautusajat laiteloittain	32

Lyhenteet

APC	Angled Physical Contact
CLI	Command Line Interface
CMS	Calix Management System
CPU	Central Processing Unit
DR	Disaster Recovery
EPON	Ethernet PON
FTP	File Transfer Protocol
Gbps	Gigabits per second
GE	Gigabit Ethernet
GPON	Gigabit-capable Passive Optical Networks
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IM	Instant Messaging
IP	Internet Protocol
IT	Informaatioteknologia
Mbps	Megabits per second
MPLS	Multiprotocol Label Switching
MTD	Maximum Tolerable Downtime
NTP	Network Time Protocol
OAM	Orbital Angular Momentum
OLT	Optical Line Terminal

ONT	Optical Network Terminal
ONU	Optical Network Unit
OS	Operating System
P2MP	Point-to-Multipoint
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RU	Rack Unit
SC	Subscriber Connector
SFP	Small Form-Factor Pluggable
SFP+	Enhanced Small Form-Factor Pluggable
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
UPC	Ultra Physical Contact
VBK	Veeam Backup Virtual Machine Backup File
VDC	Volts of Direct Current
VDSL2	Very-high-bit-rate digital subscriber line 2
VIB	vSphere Installation Bundle
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtual Private Network
VRB	Veeam Reverse-incremental Backup
XFP	10 Gigabit Small Form-Factor Pluggable
XG-PON	10 Gigabit-Capable PON

1 Työn lähtökohdat

1.1 Tutkimusongelma

Minkä takia yrityksellä tulisi olla palautumissuunnitelma?

Yritys, joka tarjoaa asiakkailleen internetpalveluita, on vastuussa asiakkaidensa palveluiden toimivuudesta palvelusopimusten mukaisesti. Verkko tulisi aina rakentaa siten, että vikatilanteessa verkon toiminta jatkuu varayhteydellä, jotta ensisijainen yhteys voidaan korjata ja asiakkaan palvelut toimivat katkotta. Vikatilanteita varten internetpalveluita tarjoavalla yrityksellä tulisi olla selvillä, miten tällaisista tilanteista toivutaan mahdollisimman nopeasti, sillä pitkittyneet palvelukatkokset aiheuttavat yritykselle taloudellisia menetyksiä.

Katastrofin tapahtuessa sellaiselle yritykselle, joka ei ole tehnyt palautumissuunnitelmaa on palautuminen tilanteesta haastavaa. Mikäli katastrofi vaikuttaa olennaisesti liiketoimintaan jolle ei ole suunniteltu palautumista, mahdollisuudet palautumiseen ovat pienet. (Gregory 2007, 12.)

Vikatilanteita varten on palveluiden toiminnan kannalta käytävä läpi sellaiset riskit, jotka toteutuessaan aiheuttavat palvelukatkoksen. Riskianalyysin perusteella on laadittava palautumissuunnitelma erilaisia ongelmatilanteita varten.

Kun palautumissuunnitelma on tehty, on sitä testattava, sillä ilman suunnitelman testausta ei voida olla täysin varmoja suunnitelman toimivuudesta todellisen vikatilanteen tapahtuessa. Mikäli testausvaiheessa havaitaan puutteita suunnittelussa, täytyy havaittujen puutteiden perusteella muokata palautumissuunnitelmaa siten, että testaus sujuu ongelmitta ja palveluiden palautuminen onnistuu.

Palautumissuunnitelma ei itsessään takaa, etteikö katastrofin osuessa kohdalle tulisi ongelmia. Jos palautumissuunnitelma on luotuna, on katastrofista selviäminen paljon helpompaa. (Gregory 2007, 12.)

1.2 Tutkimusmenetelmät

Opinnäytetyöhön kerätään aineistoa eri lähteistä, joita käytetään työn teon aikana apuna käsittelyssä ja kerätyn aineiston analysoimisessa. Analysointiin on mahdollista käyttää monia erilaisia tutkimusmenetelmiä. Tutkimusmenetelmät voidaan karkeasti erottelamalla jakaa kahteen eri ryhmään, jotka ovat kvantitatiivinen ja kvalitatiivinen tutkimusote. (Kananen 2007, 18.)

Tässä opinnäytetyössä oli tavoitteena kerätä eri lähteistä materiaalia, joita käytetään hyödyksi palautumissuunnitelman laatimisessa. Työssä itse testauksen ja muun käytännön lähestymisen kautta tutkittiin, millaisiin asioihin tulee kiinnittää huomiota riskien kartoituksessa ja laitteiden toiminnan palauttamisessa.

Toimintatutkimus

Toimintatutkimus tarkoittaa tutkimisen lisäksi, että käytäntöjä pyritään muuttamaan ja aktiivisella tekemisellä pyritään saavuttamaan haluttu päämäärä. (Saaranen-Kauppinen & Puusniekka 2006.)

Kvalitatiivinen tutkimus

Kuten kaiken tutkimustyön, myös opinnäytetyön tulee olla tieteellistä käytettäessä kvalitatiivista tutkimusmenetelmää. Kvalitatiivinen tieto on laadullista. Tieto on asiasyhteyteen liittyvää ja yksityiskohtaista sekä tutkijalle mieluista, jolloin tutkija pystyy antamaan itselle mielekkään tulkinnan asian kuvaamiseksi. Kvalitatiivisessa tutkimuksessa tutkija on yleensä kiinnostunut tutkimusprosessista ja ilmiön ymmärtämisestä kuvien, sanojen ja tekstien avulla. (Kananen 2007, 17, 24-25.)

Kvantitatiivinen tutkimus

Parametrien, muuttujien ja ilmiön tekijöiden tuntemusta edellyttävä tutkimus on kvantitatiivista. Tällaista tutkimusta on vaikeaa tehdä ennen kuin tutkittava ilmiö on riittävän täsmentynyt tutkimuksen tekijälle. Määrien laskeminen määrällisen tiedon perusteella kuten lukujen on kvantitatiivista, kun taas kvalitatiivisessa tutkimuksessa havainnointi, tekstianalyysi ja haastattelut ovat olennaisia. (Kananen 2011, 17-18.)

1.3 Opinnäytetyön tavoitteet

Opinnäytetyön tavoitteena oli kartoittaa yrityksen Calix E7 GPON (Gigabit-capable Passive Optical Networks) Access -kytkinten hallintapalvelimen, sekä kytkinten toimintaan vaikuttavat riskit. Riskikartoituksen perusteella, luotiin edellä mainitulle laitteistolle palautumissuunnitelma. Kun palautumissuunnitelma oli luotu, testattiin sen toiminta. Mikäli testausvaiheessa huomattiin puutteita, täydennettiin palautumissuunnitelma puutteiden mukaisesti. Palautumissuunnitelman ja testauksessa luotujen dokumentaatioiden oli oltava sellaiset, että koulutettu henkilöstö pystyy tarpeen tullen niitä hyödyntämään toiminnan palauttamisessa. Tarkoituksena oli myös tutkia, millaisella ajalla kytkimen laiterikossa saadaan uusi laite rikkoutuneen tilalle sekä toiminta palautettua.

Tavoitteena oli oppia tunnistamaan verkon ja verkkolaitteiston toimintaan vaikuttavia riskejä sekä suunnittelemaan palautumista vikatilanteista. Tavoitteena oli kehittää omaa ammattitaitoa työskentelemällä internetpalveluita tarjoavassa yrityksessä sekä työajan ulkopuolella itsenäisesti opiskellen palautumissuunnitteluun liittyvää kirjallisuutta sekä tutustumalla eri verkkolähteisiin.

1.4 Ajankohtaisuus

IT (informaatioteknologia) -infrastruktuurin ongelmatilanteisiin varautuminen on aina ajankohtaista. Yritysten verkkojärjestelmät muuttuvat ja kehittyvät jatkuvasti. Liiketoiminnan kannalta kriittisten prosessien katastrofaalinen seisahtuminen ilman mietittyä palautumissuunnitelmaa voi olla kohtalokasta. Ihmisten riippuvuus toimivasta ja nopeasta internetyhteydestä kasvaa jatkuvasti. Nykyään suuri osa ihmisten välisestä kanssakäymisestä tapahtuu verkon välityksellä. Kotoa käsin tehtyjen töiden yleistyessä internetyhteys on välttämätön, jotta päästään yrityksen sisäisiin resursseihin VPN-yhteyttä hyödyntäen.

1.5 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Keski-Suomen Valokuituverkot Oy. Yritys on melko uusi, sillä liiketoiminta aloitettiin vuonna 2014. Yrityksen toimialana on langallisen verkon hallinta ja palvelut. Yrityksen omistus koostuu siten, että Keski-Suomen Verkkoholding Oy omistaa Keski-Suomen Valokuituverkot Oy:n, ja Keski-Suomen Verkkoholding Oy:n omistavat Keski-Suomalaiset kunnat joihin kuuluvat: Konnevesi, Kannonkoski, Toivakka, Multia, Karstula, Kyyjärvi, Luhanka, Pihtipudas, Kivijärvi ja Petäjävesi. (Keski-Suomen Valokuituverkot Oy.)

Kuvio 1 havainnollistaa alueet, joissa Keski-Suomen Valokuituverkot tarjoaa internet-palveluita ja rakentaa valokuituverkkoa.



Kuvio 1. Verkkoalue (Keski-Suomen Valokuituverkot Oy.)

Yrityksen toimenkuvaan kuuluu valokuituverkon rakennus omistajakuntiensa alueella Nopea laajakaista -hankkeen mukaisella julkisella tuella, sekä internetpalveluiden tarjoaminen.

Nopea laajakaista -hankkeen tavoitteena on saavuttaa verkon asiakkaille 100Mbps (Megabits per second) internetyhteys, kahden kilometrin etäisyydelle vakituisesta asuinpaikasta tai yrityksen toimipisteestä. Hankkeessa käyttäjiksi määritellään julkishallinnon organisaatiot, asiakkaiden vakituiset asunnot, sekä muiden yritysten vakinaiset toimipaikat. Laajakaistahankkeen 130 miljoonan euron rahoitus koostuu siten, että kunnat osallistuvat hankkeeseen 40 miljoonalla eurolla, valtio 66 miljoonalla eurolla ja 25 miljoonaa euroa tulee EU:n Manner-Suomen maaseutuohjelmasta. Hanke käynnistettiin vuonna 2008, sellaisia alueita varten, jonne kaupallinen tarjonta ei oletettavasti toteudu. (Nopea laajakaista -hanke tuo huippunopeat internetyhteydet haja-asutusalueille, 2016.)

Keski-Suomen Valokuituverkot Oy:n verkko on ns. Open Access verkko. Tämä tarkoittaa, että muilla palveluntarjoajilla on mahdollisuus solmia operaattorisopimuksen hinnaston mukaisesti sopimus Keski-Suomen Valokuituverkot Oy:n kanssa ja tarjota omia palveluitaan verkon alueella. Yrityksen arvot koostuvat nopeasta ja asiantuntevasta asiakaspalvelusta, sekä yrityksen työntekijöille asiakkaan palvelun toiminta on aina etusijalla.

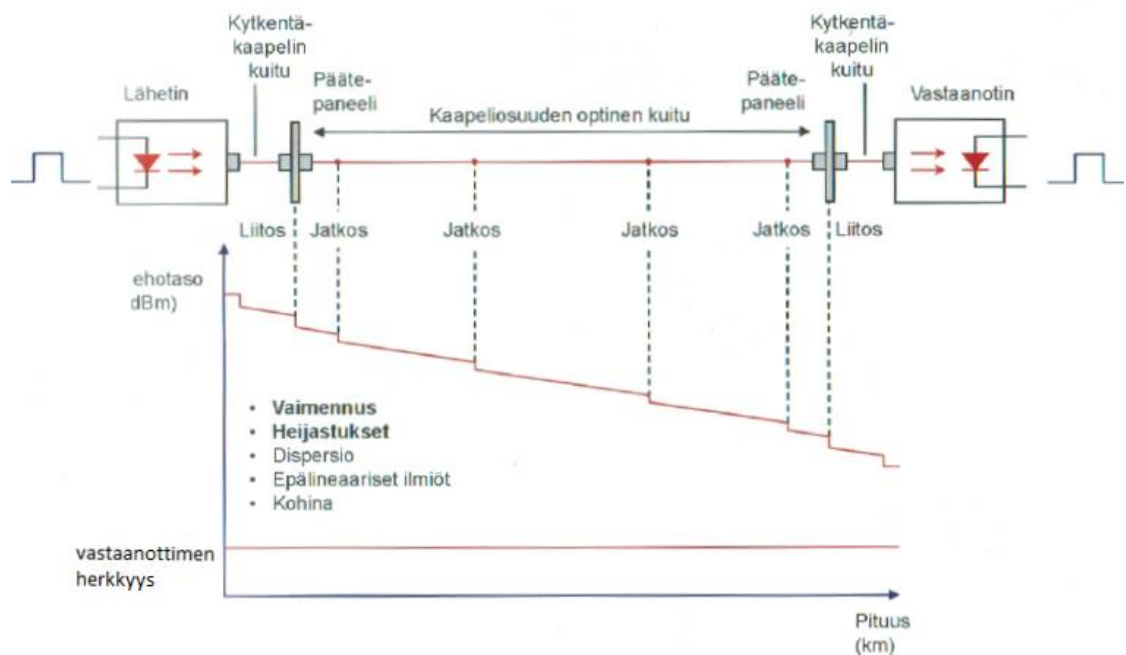
2 Suunnittelua tukeva teoria

2.1 Yleistä

2.1.1 Optinen tiedonsiirto

Optinen tiedonsiirto tarkoittaa signaalin siirtämistä valon muodossa optista kuitua pitkin lähettimeltä vastaanottimelle. Lähettimen tehtävä on muuntaa siirrettävä sähköinen signaali valoksi ja sovittaa signaali kuituun. Vastaanotin ottaa valon vastaan ja muuntaa sen sopivaan sähköiseen muotoon signaalin jatkokäsittelyä varten. Kun valosignaali siirtyy optista kuitua pitkin, se menettää osan tehostaan ja vaimenee. Kuituyhteysvälillä on myös jatkoksia, joiden takia syntyy lisävaimennusta. Valokaapelin

sisällä on yksittäisiä kuituja, jotka on päätetty molemmissa päissä kuitupaneelin liittimiin. Nämä liittimet toimivat liitinrajapintoina, joihin lähetin ja vastaanotin kytketään kytkentäkaapeleita käyttäen. Myös näistä liitoksista aiheutuu vaimennusta. Yhteysvä-
lillä olevista jatkoksista ja liitoksista syntyy etenevän valon heijastuksia paluusuun-
taan päin. Kuvio 2 havainnollistaa optisen tiedonsiirron periaatteen. (FTTX Optiset lii-
tyntäverkot 2015, 10.)



Kuvio 2. Optinen tiedonsiirto (FTTX Optiset liityntäverkot 2015, 11.)

Kokonaisvaimennus tiedonsiirtoyhteydellä koostuu kuidun vaimennuksesta, sekä liitoksista ja jatkoksista syntyvistä vaimennuksista. Lähettimen lähettämä optinen tehotaso pienenee yhteysvä-
lillä kokonaisvaimennuksen verran. Vastaanotetun tehota-
son on oltava sellainen, että kokonaisvaimennuksen jälkeen vastaanotin tunnistaa ja ilmaisee signaalin. Olennaiset asiat yhteyden toiminnan kannalta ovat siis lähettimen tehotaso, yhteyden kokonaisvaimennus ja vastaanottimen herkkyys. (FTTX Optiset liityntäverkot 2015, 10.)

2.1.2 APC

APC-liittämissä (Angled Physical Contact) liittimen eli ferrulen pää on hiottu vinoon. Yleisimmin pää on hiottu kahdeksaan asteeseen. Vinohionnalla, saavutetaan suu-
rempi heijastusvaimennus, joka on tärkeä ominaisuus esimerkiksi kaapeli-tv ja PON-
verkoissa. Saavutettu heijastusvaimennus liitettynä on yli 60 dB ja liittämättömänä

yli 55 dB. Vertauksena UPC (Ultra Physical Contact) hiottun liittimen heijastusvaimennus on liittämättömän noin 14 dB. (FTTX Optiset liityntäverkot 2015, 50.)

Kuidun liittimen pään tyypillä, hionnalla sekä mittatarkkuuksilla saadaan aikaa suurin osa liittimen optisista ominaisuuksista. Heijastusvaimennukseen vaikuttaa eniten, miten liitin on hiottu. Liitinpään tyyppi on valittava APC, jotta heijastusvaimennus saataisiin pysymään mahdollisimman suurena. (Reinikainen & Arvinen, 2013.)

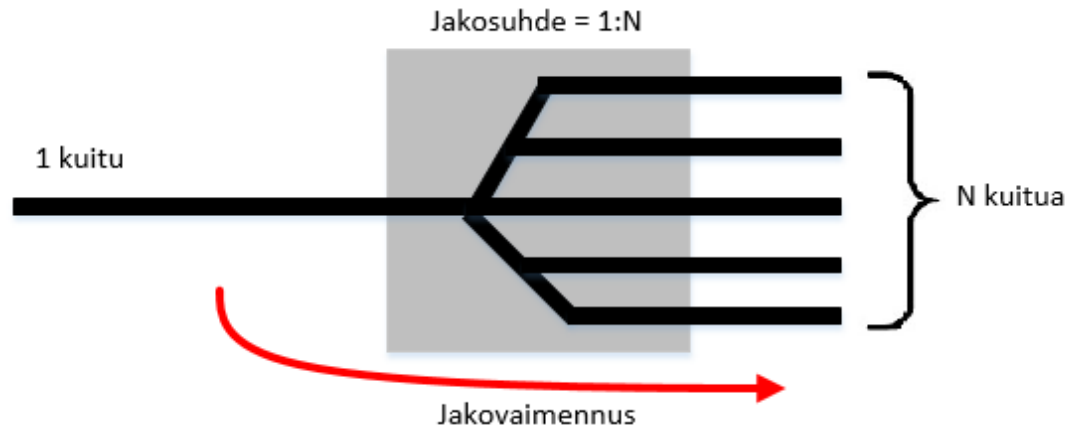
2.1.3 Jaotin

Kuviossa 3 on 19 tuuman 1:32 SC (Subscriber Connector) APC-jaotin. Adapteri vasemmassa reunassa toimii PON sisääntulona. Muut adapterit ovat asiakaslähtöjä, jotka kytketään kytkentäkuidulla ristikytkentään, joista lähtevät liityntäverkon kuidut aina asiakkaan kiinteistöön asti.



Kuvio 3. 19" 1:32 SC APC-jaotin

Jaotin toimii PON (Passive Optical Network) verkon komponenttina, jonka tehtävänä on jakaa siihen syötetty valoteho asiakkaille. Asiakkaalta eli kuitupäätelaitteelta keskittimelle päin tuleva valosignaali yhdistetään useasta kuidusta yhteen kuituun. Jaottimen jakosuhte ilmoitetaan muodossa 1:N. Jaotin siis jakaa tehoa ja näinollen valon siirtyessä jaottimen läpi, syntyy myös vaimennusta. Jaottimen läpi syötetyn valotehon vaimenemista kutsutaan jakovaimennukseksi. Kuviossa 4 on havainnollistettu jaottimen periaate. (FTTX Optiset liityntäverkot, 58.)



Kuvio 4. Jaottimen periaate (FTTX Optiset liityntäverkot, 59.)

Taulukko 1 esittää jaottimen yleisimmät jakosuhteet ja niitä vastaavat tyypilliset jakovaimennukset.

Taulukko 1. Jakovaimennukset (FTTX Optiset liityntäverkot, 59.)

Jakosuhte	Vaimennus, dB
1:2	3,5
1:4	7,0
1:8	10,5
1:16	14,0
1:32	17,5
1:64	21,0
1:128	24,5

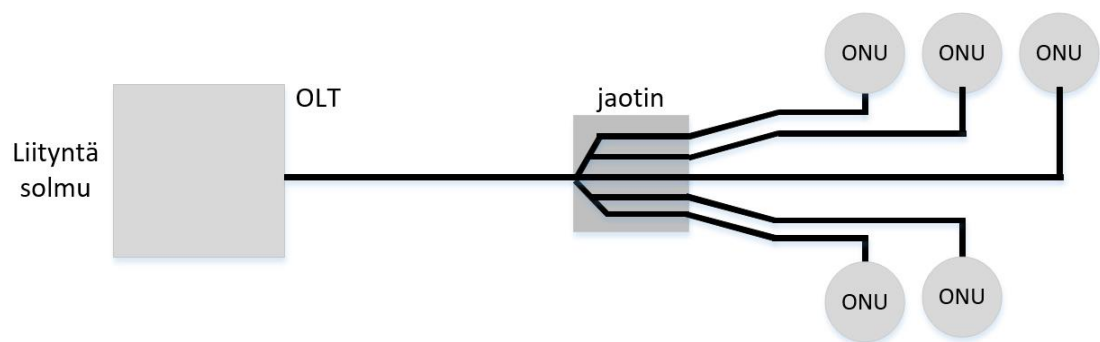
2.1.4 PON

PON verkossa OLT (Optical Line Terminal) on keskuksen päässä sijaitseva laite, jonka kautta asiakkaat liittyvät verkkoon. Asiakkaan pään laitteesta käytetään nimitystä ONT (Optical Network Unit). (FTTX Optiset liityntäverkot 2015, 81.)

ONU ja ONT tarkoittaa PON verkoissa samaa asiaa. ONT on ITU-T:n määrittelemä termi ja ONU on IEEE:n määrittelemä.

Jokainen yksittäinen asiakas liittyy omalla kuituyhteydellä jaottimeen ja jaotin on kytketty useimmiten yhdellä kuituyhteydellä keskittimeen. Keskittimen ja jaottimen välinen kapasiteetti jaetaan siis yhden GPON syötön perässä olevien asiakkaiden kesken. PON tekniikassa siis jaottimen jakosuhteen mukaisesti päätetään monta asiakasliittymää yhteen pisteeseen. Tällaisesta topologiasta käytetään termiä P2MP (Point-to-Multipoint) (FTTX Optiset liityntäverkot 2015, 76.)

Kuvio 5 havainnollistaa passiivisen optisen verkon topologian.



Kuvio 5. PON

ONU:n aktivoituessa PON:ssa, se aloittaa neuvottelun OLT:n kanssa synkronisoinnista, sekä fyysisen kerroksen OAM (Orbital Angular Momentum) kanavasta ja etäisyydestä. Koska PON verkko on P2MP järjestelmä, on erityisen tärkeää, että jokainen ONU identifioidaan ja rekisteröidään tietylle asiakkaalle. (ITU-T.984.3 2014, 19.)

Taulukko 2 esittää yleisimmät PON-standardit nopeuksineen.

Taulukko 2. PON standardeja (FTTX Optiset liityntäverkot 2015, 81.)

PON	Nopeus alavirtaan	Nopeus ylävirtaan	Standardi
GPON	2,5 Gbit/s	1,2 Gbit/s	ITU-T G984-sarja
XG-PON	10 Gbit/s	2,5 Gbit/s	ITU-T G.984-sarja
EPON	1 Gbit/s	1 Gbit/s	IEEE 802.3ah
10G-EPON	10 Gbit/s	1 Gbit/s	IEEE 802.3av
	10 Gbit/s	10 Gbit/s	

2.2 Palautumissuunnittelun hyödyt

Palautumissuunnittelun avulla kyetään selviytymään vikatilanteista, mutta palautumissuunnittelusta on muitakin hyötyjä. Esimerkiksi teknologia kehittyy, koska palautumissuunnittelun aikana IT järjestelmiä kehitetään, jotta elpymistavoite saavutetaan vikatilanteiden sattuessa. Myös verkon häiriömäärät laskevat. Teknologian kehittymisen myötä järjestelmät toimivat paremmin ja ovat muutenkin vakaampia. Palveluiden laatu paranee suunnittelun aikana, prosessien ja teknologian kehittymisen seurauksena. Myös liiketoimintaprosessit paranevat palautumissuunnitelmaa laadittaessa. Koska verkkoa ja laitteistoa tarkkaillaan erityisesti suunnittelun aika, löytyy verkon infrastruktuurista lähes varmasti parannettavaa. (Gregory 2007, 13.)

Kun palautumissuunnitteluun sisältyy testaus, jossa demonstroidaan vikatilanne ja sen jälkeinen palautuminen, saadaan varmuus suunnitelman toimivuudesta. Testausvaiheessa saadaan suunnitelman puutteet esille, mikäli palauttamisessa huomataan ongelmia.

2.3 MTD

Maximum Tolerable Downtime (MTD) on määritelty aika, jonka jälkeen yrityksen liiketoiminnan kannattavuudelle aiheutuu suurta haittaa ja seuraukset ovat kohtalokkaita. MTD voi vaihdella eri prosesseissa. MTD vaihtelee yleensä tunneista päiviin tai pidempiin aikoihin. (Gregory 2007, 64.)

2.4 RTO

Recovery Time Objective (RTO) on aikaväli, jonka aikana keskeytynyt liikeprosessi pyritään saamaan jälleen toimintaan. RTO on aina pienempi kuin MTD, jokaista liiketoimintaprosessia suunniteltaessa. Mikäli tavoitteena on pieni RTO, vaatii se myös enemmän ennakkoon varautumista. Jos esimerkiksi RTO olisi 50 minuuttia, tulisi fyysisesti hajonneen palvelimen tilalle olla valmiina reaaliajassa replikoitu palvelin valmiina käynnissä, joka hajoamisen jälkeen voidaan ottaa käyttöön. (Gregory 2007, 65.)

2.5 RPO

Recovery Point Objective (RPO) on kadotetun datan maksimimäärä, joka voidaan menettää prosessin keskeytymisen ja palauttamisen välillä. Mikäli halutaan alhaisempi RTO, on myös datan replikointiin ja varmuuskopiointitekniikkaan sijoitettava enemmän. (Gregory 2007, 65-66.)

2.6 Palautumisaika

Palautumisaika on aikaväli verkon vikaantumisesta siihen hetkeen, kun verkko on taas toiminnassa tai liikenne siirtyy kulkemaan varayhteyttä pitkin. Yksi tärkeistä kriteereistä palautumiselle on pieni palautumisaika, jolloin verkon palvelut kärsivät vähemmän verkon vikaantumisesta. (Vasseur, Pickavet & Demeester 2004, 26.)

2.7 Palvelutasot

Palautumissuunnittelussa ja testauksessa tulisi elpymisaikoja pohtia palvelutasojen perusteella. Yrityksen ja asiakkaiden sopimuksissa on yleensä määritelty häiriöiden ja katkosten korjausajat. Jos esimerkiksi on määritelty, että palvelun palauttaminen vikatilanteesta saa kestää maksimissaan vuorokauden, on tämän ajan ylittyessä yritykselle liiketoiminnallisia seurauksia.

Yritykset ovat yhä enemmän riippuvaisia tietoteknisistä palveluista ja ratkaisuista peilaten liiketoimintaan. Tavoitteet palvelutasolle vaihtelevat sen perusteella, mikä on palvelun kohteena ja millaiset ovat aikamääreet. Palvelutasosopimus solmitaan palvelun tarjoajan ja asiakkaan välille ja siinä on kuvattuna palvelun sisältö ja tasot. Palvelutasosopimuksesta käytetään termiä SLA (Service Level Agreement). Palvelutasosopimus pitää sisällään palvelutasotavoitteet, sopimuksen vastakohtien vastuut, sekä palvelukuvauksen. Palvelutaso sisältyy osana laajempaan prosessikokonaisuuteen, palvelutasonhallintaan, josta käytetään termiä SLM (Service Level Management). (JHS-XXX IT-palveluiden palvelutasoluokitus. n.d.)

2.8 Veeam Backup & Replication v9.0

Veeam Backup & Replication palvelinta hyödyntäen, pystytään luomaan mukautuva varmuuskopiointi -infrastrukturi. Sen ominaisuuksina on erilaiset tehtävät liittyen datan suojaamiseen. Datan suojaukseen kuuluvat katastrofin jälkeiseen palautukseen liittyvät tehtävät, virtuaalikoneiden varmuuskopiointi sekä replikointi. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 11.)

2.8.1 Komponentit

Backup Server

Varmuuskopiointipalvelimena voi toimia virtuaalinen tai fyysinen Windows-palvelin, johon Veeam Backup & Replication asennetaan. Palvelimen tarkoituksena on huolehtia virtuaalikoneiden varmuuskopioinnista ja replikoinnista. Sen tehtäviin kuuluu myös palautuksen varmistamisen ja tehtävien koordinoinnin tehtävät. Myös töiden ajastus ja resurssien allokointi sekä varmuuskopiointin infrastruktuurin komponenttien hallinta kuuluvat palvelimen tehtäviin. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 12.)

Varmuuskopiointipalvelin pystyy myös itse toimimaan varmuuskopiointi proxyä ja repositioriona, jolloin se hallinnoi myös datan käsittelyyn ja tallennukseen kuuluvia tehtäviä. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 12.)

Backup & Replication Console

Varmuuskopiointipalvelimelle pääsy tapahtuu Backup & Replication Consolen kautta. Oletuksena Veeam Backup & Replication palvelimen asennuksen yhteydessä, asennetaan palvelimelle myös Console. Consolen avulla kirjaututaan varmuuskopiointipalvelimelle, kun tarkoituksena on tehdä datan suojaukseen ja katastrofin jälkeiseen palautumiseen liittyviä operaatioita. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 13.)

Palvelimelle pääsyn edellytyksenä on, että kirjautuva käyttäjä on palvelimen Local Users ryhmässä tai Domain Users ryhmässä. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 13.)

Backup Proxy

Kun Veeam Backup & Replication palvelin on asennettu, se koordinoi tehtäviä. Tehtäviin kuuluu VM (Virtual Machine) kopiointi, varmuuskopiointi, VM migraatiot, replikointityöt sekä palauttamiseen liittyvät työt. Palvelin toimii itsenäisesti käsitellessään dataliikennettä. Kun virtuaalikoneen dataa siirretään, se siirtyy lähteestä kohteelle varmuuskopiointipalvelimen kautta. Pienissä, vain muutaman virtuaalikoneen ympäristöissä palvelin voi toimia itsenäisesti dataliikenteen käsittelijänä. Työkuorman jakamiseen on kuitenkin keksitty menetelmä. Työkuormaa saadaan jaettua käyttämällä Backup Proxy palvelimia. Proxy sijoitetaan ympäristöön datan lähteen ja kohteen väliin ja sen tehtävänä on vähentää varmuuskopiointipalvelimen työkuormaa suorittamalla varmuuskopiointi- ja replikointitöitä. Backup Proxy välittää tuotanto storagelta haetun virtuaalikoneen datan, varmuuskopio repositorioon. Backup Proxy pakkaa datan ennen siirtoa, jonka ansiosta siirretty datamäärä on pienempi ja kaistaa saadaan säästettyä. Kun dataa replikoidaan, Backup Proxy välittää dataa toiselle Backup Proxylle. Backup Proxy -roolissa voi toimia fyysinen tai virtuaalinen Windows palvelin. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 15.)

Backup Repository

Backup Repositoriossa säilytetään VM kopioita ja niiden metadataa, sekä varmuuskopiotiedostoja. Infrastruktuuriin on mahdollista käyttää kolmea erilaista repositoriotyyppiä: Simple backup repositoriota, Scale-out backup repositoriota tai Backup repositoriota käännettyillä levyillä. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 20.)

2.8.2 Data Compression & Deduplication

Varmuuskopion koon pienentämiseksi, dataa voidaan pakata. Pakkaamisella säästetään levytilaa ja nopeutetaan varmuuskopiontiprosessia. Myös verkon liikenne pysyy pienempänä, kun siirretyn varmuuskopion koko on pienempi. Datan pakkaamiseen Veeam Backup & Replication tarjoaa viisi erilaista tasoa, jotka ovat None, Dedupe-friendly, Optimal, High ja Extreme. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 99.)

Laitteistotason pakkauksessa ja deduplikoinnissa suositellaan käytettäväksi Nonea. Jos tarkoituksena on vähentää Backup Proxyn prosessorikuormaa, suositellaan käytettäväksi Dedupe-friendly tasoa. Optimal taso tuo parhaan suhteen varmuuskopioon ja ajan välille. High vaihtoehdolla saadaan aikaiseksi jopa 10% parempi pakkaus kuin Optimal tasoa käytettäessä, mutta CPU (Central Processing Unit) kuorma on kymmenen kertainen. Kaikista vähiten levytilaa vie Extreme taso, mutta tasoa käytettäessä myös suorituskyky on huonoin. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 99.)

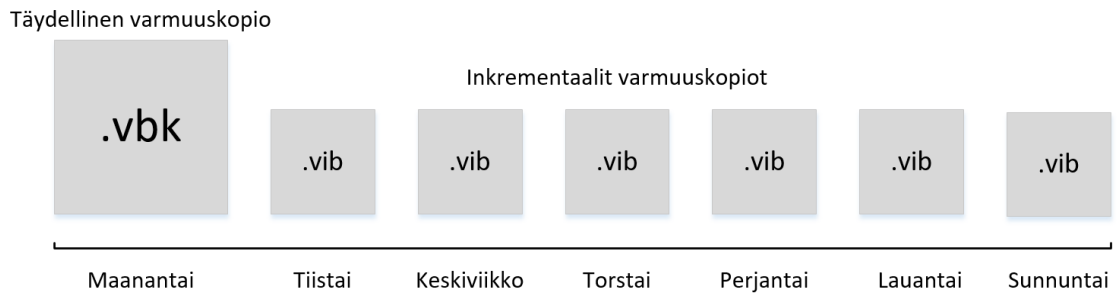
Datan deduplikoinnilla saadaan säästettyä levytilaa. Kun deduplikointia käytetään, ei identtisiä datablokkeja kirjoiteta useaan kertaan, esimerkiksi jos samassa varmuuskopioityössä on useita samalla alustalla luotuja virtuaalikoneita. Datablokkeja joiden koko on 0 tavua ei myöskään prosessoida, joten deduplikoinnista on hyötyä, jos virtuaalikoneen loogisella levyllä on paljon tyhjää tilaa. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 99.)

2.8.3 Varmuuskopiointimenetelmät

Veeam Backup & Replication luo varmuuskopioketjuja muodostaessaan varmuuskopioita. Ketjut pystytään muodostamaan kolmella eri tavalla jotka ovat: Forever forward incremental backup, forward incremental backup, sekä reverse incremental backup. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 74.)

Forever forward incremental

Varmuuskopioketju koostuu ensimmäisestä täydellisestä varmuuskopiosta ja joulusta eteenpäin kasvavia varmuuskopioita. (ks. Kuvio 6). Kun varmuuskopio luodaan ensimmäisen kerran, tehdään varmuuskopio repositorioon täydellinen VBK (Veeam Backup Virtual Machine Backup File) -tiedosto. Tämän jälkeen kopioidaan vain virtuaalikoneen muuttuneet datablokit verrattuna edelliseen varmuuskopioon, joka voi olla kokonainen tai kasvava ja tallennetaan muuttuneet datablokit inkrementaaleina VIB (vSphere Installation Bundle) -tiedostoina varmuuskopioketjuun. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 74.)

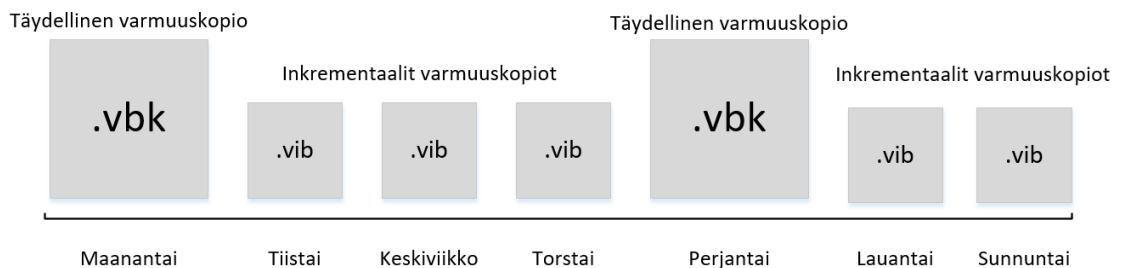


Kuvio 6. Forever forward incremental (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 74.)

Varmuuskopiointityössä on määritelty, montako palautuspistettä työstä säilytetään. Palautuspisteiden määrä tarkastetaan, kun ketjuun lisätään uusi palautuspiste. Kun työn palautuspisteiden määrä on täynnä, palautusketjua muokataan ja uudelle palautuspisteelle tehdään tilaa. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 74.)

Forward incremental

Forward incremental vastaa muilta osin Forever forward incremental -tekniikkaa, mutta virtuaalikoneesta otetaan säännöllisin väliajoin täydellinen varmuuskopio. (ks. Kuvio 7). Näin ketjut pysyvät pienempinä. Ketju koostuu siten, että aina uuden täydellisen varmuuskopion jälkeen otetut inkrementaalit varmuuskopiot käyttävät alkupisteenä edellistä varmuuskopiota. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 76.)

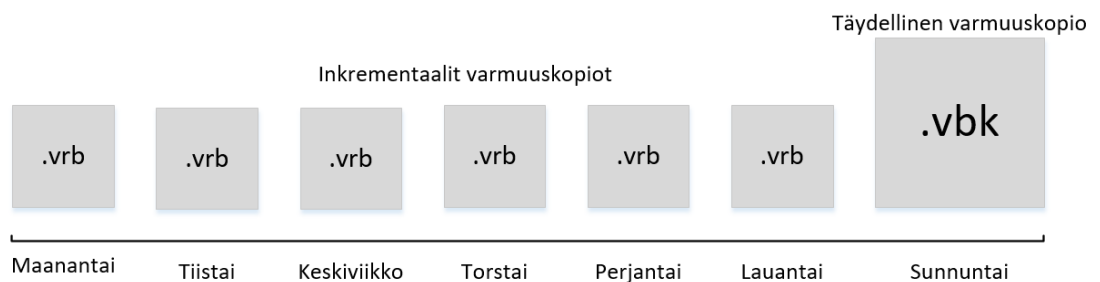


Kuvio 7. Forward incremental (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 76.)

Reverse incremental

Reverse incremental tapaa käytettäessä, ketju koostuu viimeisimmästä täydellisestä varmuuskopiosta ja joukosta edeltäviä inkrementaaleja varmuuskopioita. (ks. Kuvio

8.) Työn ensimmäisellä ajolla luodaan täydellinen varmuuskopio virtuaalikoneesta. Tämän jälkeen suoritetuilla töillä, tallennetaan vain virtuaalikoneen muuttunut data, kuten aikaisemmissa varmuuskopiointimenetelmissä. Luodut varmuuskopiot ovat VRB (Veeam Reverse-incremental Backup) -tiedostoja, joita Veeam Backup & Replication käyttää viimeisimpään täydelliseen varmuuskopioon, rakentaakseen täydellisen varmuuskopion virtuaalikoneen viimeisimmästä tilasta. (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 78.)



Kuvio 8. Reverse incremental (Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere 2016, 78.)

2.8.4 Tuetut ympäristöt

Veeam Backup & Replication tukee sekä VMwaren, että Microsoftin virtualisointi -infrastruktuuria.

Tuettuihin VMware tuotteisiin kuuluvat vSphere 4.1, vSphere 5.x ja vSphere 6.0 alustat, ESX(i) 4.1, ESXi 5.X ja ESXi 6.0 hostit, sekä vCenter Server 4.1, vCenter Server 5.X, vCenter Server 6.0, vCloud Director 5.1, 5.5, 5.6 ja 8.0 ohjelmistot. (Veeam Backup & Replication What's New in v9? 2016, 2.)

Tuettuihin Microsoft tuotteisiin kuuluvat Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2 alustat, Microsoft Hyper-V Server 2008 R2 SP1, Windows Server Hyper-V 2008 R2 SP1, Microsoft Hyper-V Server 2012, Windows Server Hyper-V 2012, Microsoft Hyper-V Server 2012 R2 ja Windows Server Hyper-V 2012 R2 hostit, sekä Microsoft System Center Virtual Machine Manager 2008 R2 SP1, Microsoft System Center Virtual Machine Manager 2012 SP ja Microsoft System Center Virtual Machine Manager 2012 R2 ohjelmistot. (Veeam Backup & Replication What's New in v9? 2016, 2.)

2.9 Palautumissuunnittelua koskeva laitteisto

2.9.1 CMS

CMS (Calix Management System) tarjoaa työkalun, sekä monia ominaisuuksia kupari- ja kuituverkkojen asennukseen ja ylläpitoon. Verkkoa kyetään hallinnoimaan ja ope- roimaan, sekä palvelua pystytään tarjoamaan sadan asiakkaan kokoisista toteutuk- sista, jopa miljoonan laajakaistatilaajan kokoiisiin verkkoihin. (Simplify Network Oper- ations from a Single Element Management System. n.d.)

CMS on palvelin pohjainen hallinta-alusta, joka kykenee usean yksittäisen Calix ver- kon hallintaan. CMS:n avulla voidaan provisoida asiakkaat ja tehdä kunnossapitoon ja vianmääritykseen liittyviä tehtäviä. Se mahdollistaa verkon ylläpitäjien koulutuksen verkon alueiden alustasta riippumatta. CMS:n avulla maantieteellisesti hajautetun verkon hallinta on helppoa, vaikka verkko koostuisi useista tuhansista Calix liityntä- laitteista. CMS järjestelmän oikeuksien rajaus on helppo määrittää siten, että henki- löt pääsevät verkkoinfrastruktuurin tiettyjen alueiden resursseihin tietyin oikeuksin. (Simplify Network Operations from a Single Element Management System n.d.)

CMS-palvelimen tarkoituksena on tarjota työkalu GPON-kytkinten keskitettyyn hallin- taan. CMS mahdollistaa myös asiakkaan palvelun provisioinnin ja yhteyden vianselvi- tyksen.

2.9.2 Calix E7-2:n runko

Calix E7-2:n avulla saadaan tarvittu kaistanleveys toteutettua ja tarpeen tullen kais- tanleveyttä lisättyä. Jokainen E7-2 on modulaarinen kaksi paikkainen, yhden rack yk- sikön (1RU) alusta, 100 Gbps (Gigabits per second) estottomalla taustaväylällä (linja- korttien välillä). Sillä voidaan tarjota tarpeen mukaan millaista yhdistelmää tahansa käyttäen VDSL2 (Very-high-bit-rate digital subscriber line 2), GPON, Active Ethernet / Point-to-point GE (Gigabit Ethernet), 10GE ja GE palveluita.

Rungon mitat ovat 44,5 x 4,3 x 29,1 cm. Käyttölämpötila laitteella on -40c° / +65°. Lai- tetta voidaan hallita käyttäen paikallista hallintarajapintaa CLI:lla (Command Line In-

terface) tai web GUI:lla (Graphical User Interface) tai käyttäen keskitettyä hallintajärjestelmää, CMS (Calix Management System). (Calix E7-2 Ethernet Service Access Platform. n.d.)

2.9.3 GPON-4R2 linjakortti

GPON-4R2 linjakortin ominaisuuksina on neljä kappaletta ITU G.984-yhteensopivia GPON -liitäntää, kahdeksan GE liitäntää, sekä neljä integroitua 10-GE-liitäntää (2 kappaletta SFP+ (Enhanced Small Form-Factor Pluggable) ja 2 kappaletta XFP (10 Gigabit Small Form-Factor Pluggable)). Calix E7-2:n runkoon voidaan asentaa vain toinen tai molemmat Calix E7-2 GPON-4R2 linjakortit.

Yksittäinen PON tukee maksimissaan 64 asiakasta. Jos kokoonpanoon kuuluisi kaksi GPON-4R2 linjakorttia ja käytettäisiin maksimijakosuhdetta (1:64), saataisiin 512 asiakasta syötettyä. Lisäksi kokoonpanolla saataisiin syötettyä 16 kappaletta point-to-point Ethernet tilaajaa. (GPON-4 r2 line card. n.d.)

3 Palautumissuunnittelu

3.1 Riskianalyysi

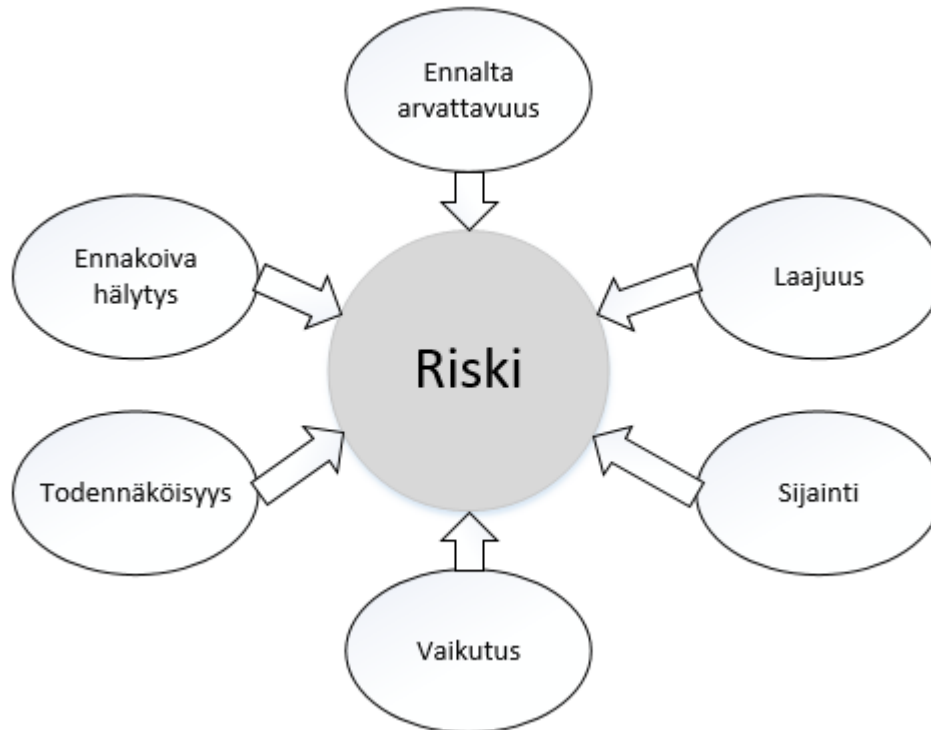
Verkon katkokset voivat lähtökohtaisesti olla suunniteltuja tai suunnittelemattomia. Suunnittelemattomat katkokset johtuvat odottamattomista verkon osien vioista. Tällaisia vikoja ovat aktiivilaitteiden laitteistoviat ja ohjelmistovirheet kuten esimerkiksi linjakortin viat, linkkivälien lähetin-vastaanottimien viat tai virtalähdeviat. Odottamattomiin vikoihin lukeutuvat myös kuitukatkokset, sähköverkon katkokset. Suunniteltuihin verkon katkoksiin kuuluvat esimerkiksi muutos ja asennustöistä aiheutuvat katkokset ilmoitetun huoltoikkunan aikana tai ohjelmistopäivitysten aikana.

Kun palautussuunnitelmaa aletaan tekemään, on aluksi hyvä tunnistaa sellaisia uhkia ja riskejä, jotka voivat aiheuttaa vikoja. Riskien analysoinnissa keskitytään analysoimaan yrityksen verkon ohjausjärjestelmiä, fyysistä ja ympäristöllistä turvallisuutta ja näiden riittävyttä kun peilataan uhkiin. (Disaster Recovery: Best Practices, 5.)

Analyysiprosessissa tulisi tekeminen peilata verkon toimintaan vaikuttaviin funktioihin. Näin tekemällä saadaan olennaiset asiat riskianalyysiin. Näihin funktioihin kuuluu

verkon operaatioihin vaikuttavat ja taloudellisiin menetyksiin johtavat funktiot. (Disaster Recovery: Best Practices 2008, 5.)

Riskiarvioinnissa on hyvä pohtia riskin eri määritteitä (ks. Kuvio 9)



Kuvio 9. Riskin määritteitä (Disaster Recovery: Best Practices, 5.)

Tarkastellaan kuviota ja peilataan sitä yritykseen, jolle palautumissuunnittelu tässä opinnäytetyössä luotiin.

Tarkastellaan esimerkiksi riskin ennalta arvattavuutta. Kovan ukonilman tai myrskyn aikana on todennäköistä, että yrityksen verkon alueella ilmenee katkoksia sähkönjakelussa. Menneen kesän (2016) aikana ilmastosta johtuneita sähköverkon katkoksia yrityksen verkon alueella ilmeni muutamia. Kun tiedetään, että luvassa on myrskyisää säätä, monitoroidaan verkkoa tehostetusti sekä tarkkaillaan akuston riittävyyttä sähkökatkoksien aikana.

Kesän aikana monesti eri yritykset kaivavat sähkö- ja kuitukaapeleitaan maahan.

Myös erilaisilla rakennustyömailla kaivetaan maata, jolloin kuitukatkokset ovat mahdollisia. Tästä syystä on todennäköisempää, että kevään alusta aina myöhäiseen syksyyn tapahtuu odottamattomia kuitukatkoksia yhteysväleillä.

Riskianalyysissä pohdittiin olennaisia ongelmia, joista voi aiheutua häiriöitä tai katkoksia verkon palveluiden toimintaan. Tällaisia riskejä olivat kuitukatkokset, konfigurointivirheet, sähkökatkokset, laiteviat ja häiriöt, Ilkivalta, lämmityksen toimimattomuus, jäädytyksen toimimattomuus, tietoturvaloukkaukset, asennustöistä johtuvat katkokset sekä päivityksistä aiheutuvat ongelmat. Laitteiston toimintaan vaikuttavia riskejä pohdittiin ja olennaisimmat riskit saatiin listattua. Liite 1 esittää Calix E7-2:n ja CMS-palvelimen toimintaan vaikuttavat riskit selvennyksineen.

3.2 Tiimin henkilöstö

Katastrofin sattuessa tiimin tehtävänä on alkaa suunnitelman mukaisesti suorittamaan erinäisiä tehtäviä liittyen liiketoimintaa tukevien IT järjestelmien arviointiin, uudelleenkäynnistykseen, ja palauttamiseen. (Gregory 2007, 33).

Vikatilanteessa, palautumissuunnittelussa on oltava selvillä henkilöt jotka vastaavat laitteiden palauttamisesta. Runkokytöntien palauttamiseen on normaalina työaikana käytössä päivystystiimiin kuuluvat henkilöt, joista yksi henkilö on vuorollaan päivystäjänä. Päivystäjän tulee reagoida 2 tunnin sisällä laitteen viasta. Normaalin päivittäisen työajan sisällä, on useampi henkilö puhelimitse tavoitettavissa, sekä valmiudessa palauttamaan laitteiston toiminta, palautumissuunnitelman sisältävien työohjeiden mukaisesti. Mikäli ongelmia ilmenee palauttamisen yhteydessä, on henkilöstö tavoitettavissa puhelimitse.

3.3 Kommunikointi vian sattuessa

Henkilöstön kesken, on käytössä useampi IM (Instant Messaging) sovellus. Sovellusta hyödyntämällä kommunikoidaan tiimin kesken tarpeen tullessa. Henkilöstö on hajajoitettu eri kuntien alueilla ja tiimin kesken kommunikoidaan tarpeen tullen etättyövälineillä.

Tarpeen tullen vian korjaamiseksi otetaan yhteyttä kumppaniyritysten henkilöihin. Jos vian korjaus vaatii esimerkiksi vaurioituneen kuidun hitsausta, tilataan korjaus yritykseltä, joka pystyy vian korjaamaan.

Tarvittaessa saadaan korkeamman tason teknistä osaamista puhelimitse tai hätätapauksessa paikan päällä. Tällaisessa tilanteessa otetaan yhteys laitteiston maahantuojaan. Ensisijaisesti yritetään selvittää ongelma puhelimesta. Mikäli ongelman selvittäminen tarvitsee vieläkin syvällisempää asiantuntemusta, saadaan tarvittaessa tukea vieläkin korkeammalta tasolta, aina laitevalmistajalta asti.

3.4 Varalaitteisto

Palautumissuunnitelmaan kuuluu myös varmistaa, että varalaitteisto on saatavilla sellaisessa tilanteessa, jossa verkkolaite tai verkon komponentti hajoaa fyysisesti, eikä sillä voida toteuttaa enää palveluita. Palautumissuunnitelmasta vastaavan henkilön tulee siis pitää huoli, että varastossa on aina vähintään yksi kappale jokaista laitetta ja komponenttia saatavana. Mikäli varalaitetta ei vian sattuessa ole heti saatavilla, voi sen toimituksessa kestää useita päiviä, viikkoja tai jopa kuukausia.

Verkon toiminnan palauttamista varten varalla täytyy olla tarvittavat SFP (Small Form-Factor Pluggable) moduulit, linjakortit, laiterungot, kytketä kuidut, invertterit, tasasuuntaajat, sekä muut laitteistot, jotka vikaantuessaan täytyy vaihtaa uusiin toiminnan palauttamiseksi.

Jokaisen Calix E7-2:n laitteistosta luotiin dokumentti, jossa on tarkat tiedot rungosta, linjakorteista, SPF, SFP+ ja XFP moduuleista, sekä kytkentäkuiduista joita moduuleihin on kytketty. Luoduista dokumentaatioista pystytään nopeasti selvittämään tarvittava varalaitteisto, kun vikaa lähdetään korjaamaan.

3.5 Sähkönsyöttö

Kuvio 10 havainnollistaa Calix E7-2:n sähkönsyötön. Calix E7-2 rungossa on redundanttinen -48/60 VDC (Volts of Direct Current) sähkönsyöttö (A ja B).

Syötettävä jännite tulee olla -42,5 VDC ja -72 VDC välillä. Koska Calix E7-2 rungossa on redundanttiset virtalähteet, ei yhden virtalähteen hajoaminen aiheuta katkosta asiakkaiden palveluissa.

Mikäli sähköverkossa ilmenee katkos ja laitetilän sähkönsaanti estyy, on laitetoiloissa akustot, joiden avulla laitteet pysyvät käynnissä ja palvelut toiminnassa.



Kuvio 10. Sähkönsyöttö

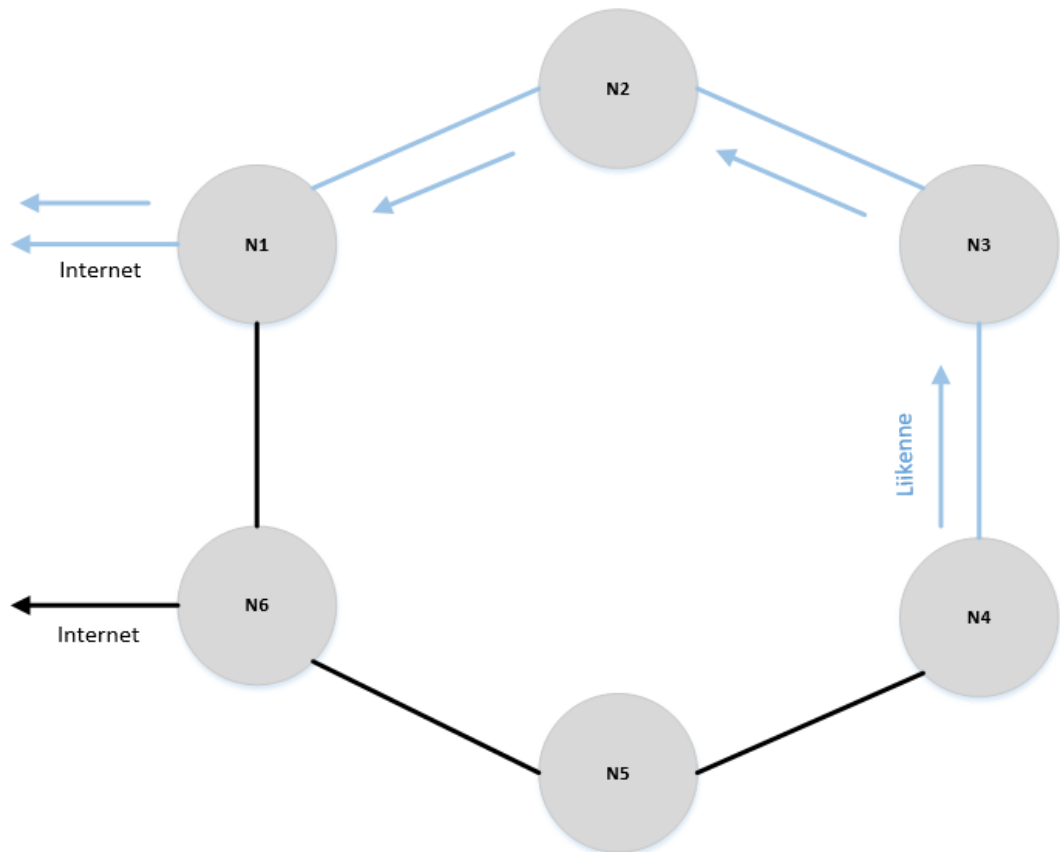
3.6 Verkon redundanttisuus

Runkoverkko on rakennettu ringiksi, joten pääyhteyden katketessa liikenne alkaa kulkea varayhteyttä pitkin. Kuviossa (ks. Kuvio 11) on havainnollistettu ringiverkon toiminta. Kuviossa ympyrän muotoiset kuviot ovat verkon solmupisteitä. Solmut on numeroitu N2-N6, jossa N = node eli solmu. Verkon liikenne kulkee solmujen läpi viimeiselle solmulle asti, josta liikenne reitittyy Internetiin. Normaalitylanteessa liikenne kulkee N4 solmulta internetiin painotettua pääyhteyttä pitkin, solmujen N3, N2 ja N1 kautta.

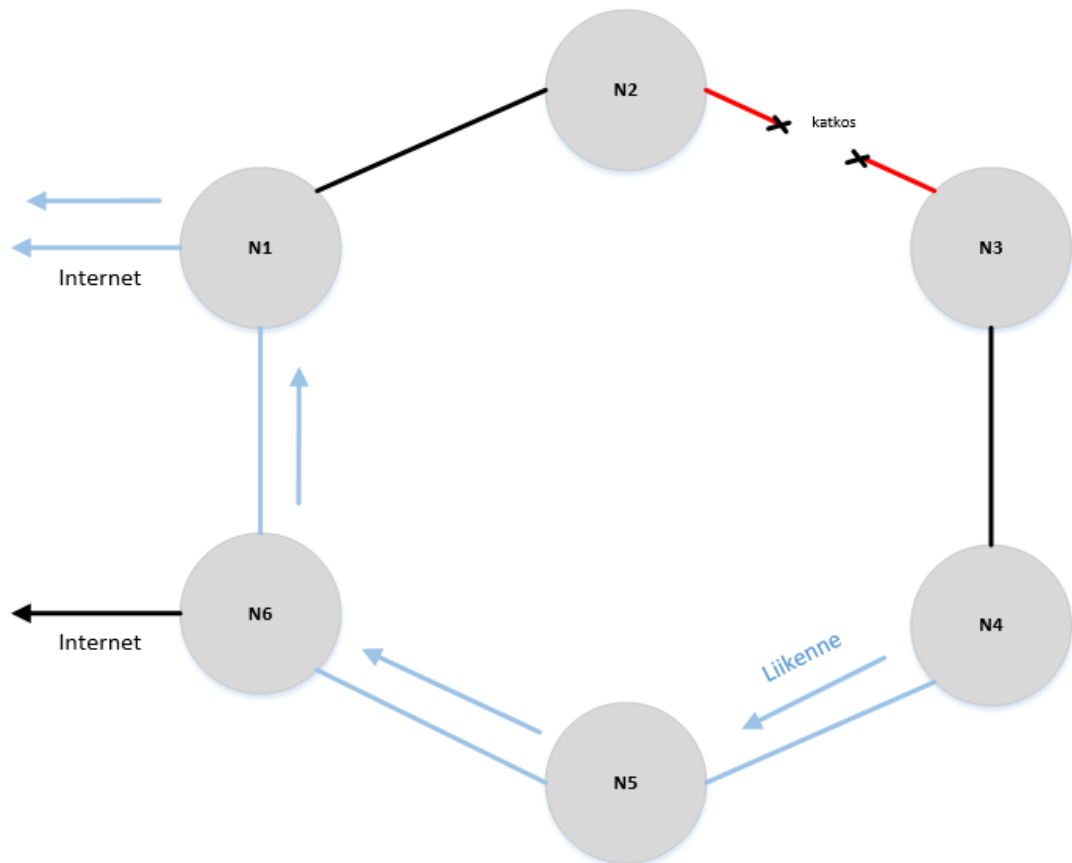
Kun pääyhteys katkeaa, liikenne siirtyy kulkemaan varayhteyttä pitkin (ks. Kuvio 12). Liikenne kulkee solmujen N5, N6 ja N1 kautta. Varareitti on monitoroitu samalla tavalla kuin pääyhteys, jotta tiedetään aina varareitin toimivuus.

Vianselvitys hallintayhteyden katketessa kyetään tekemään mobiilivarayhteyden kautta. Laitetoiloissa on laitteet, joiden avulla päästään VPN (Virtual Private Network) yhteyttä pitkin kiinni laitteisiin. Tämä tarkoittaisi tilannetta, jossa pääyhteys ja varayhteys olisivat molemmat poikki.

Kun tarkastellaan kuvioita 11 ja 12 voidaan todeta, että Internettiin on verkosta kaksi eri reittiä. Mikäli N1 solmuun tulee vikaa, siirtyy verkon liikenne kulkemaan automaattisesti solmun N6 kautta internettiin. Liikenne kulkee N6 solmun kautta internettiin vain siinä tapauksessa, että N1 solmun kautta ei päästä internettiin.



Kuvio 11. Rinkiverkon toiminta 1



Kuvio 12. Rinkiverkon toiminta 2

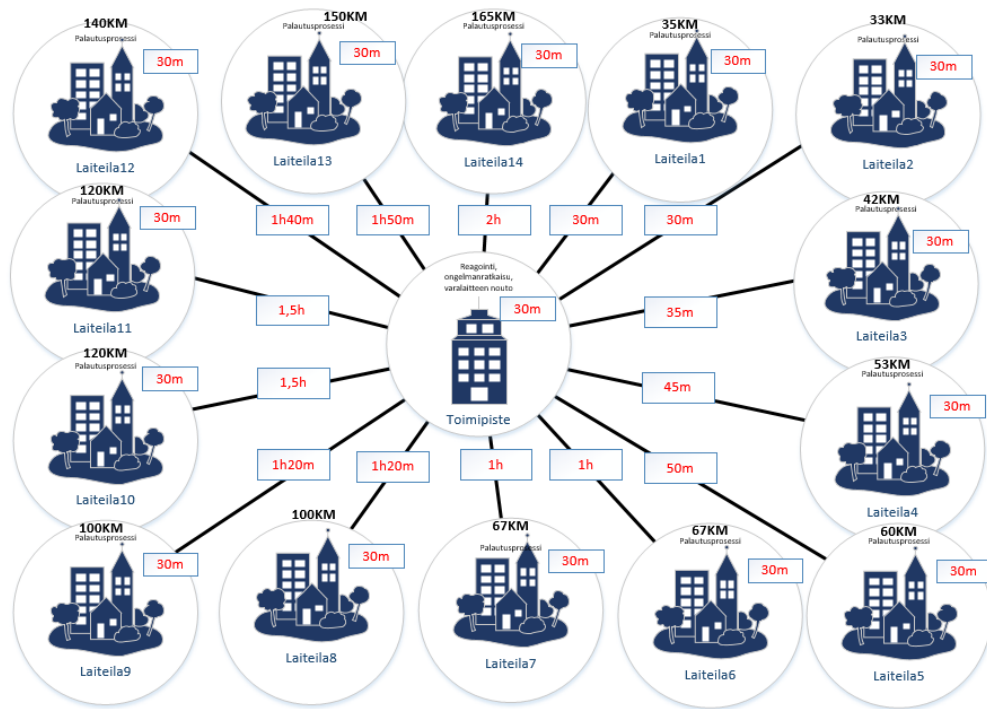
3.7 Vasteajat

Kun aletaan pohtimaan vasteaikoja tulisi huomioida jokaiseen vaiheeseen kuluva aika mahdollisimman tarkasti, jotta todellisessa tilanteessa kyettäisiin antamaan jonkinlainen arvio korjausajoista palveluita palautettaessa. Vasteaikoja tulee peilata palvelutasosopimuksissa määriteltyihin kriteereihin. Aikojä pohtiessa tulee huomioida myös viikonpäivä ja kellonaika. Mikäli vikatilanne esiintyy arkipäivänä normaalin työajan puitteissa, pystytään siihen reagoimaan nopeasti, lähes saman tien. Päivystysaikoina vian selvitys saattaa kestää kauemmin, koska vian selvittämiseen on vähemmän resursseja käytettävissä. Taulukko 3 esittää etäisyydet, sekä matka-ajat, koskien tässä opinnäytetyössä käsiteltävien GPON-kytkinten palauttamista tilanteessa, jossa paikallinen resurssi tarvitsee varalaitteistoa tai muuta apua yrityksen päätoimipaikalta. Taulukon matka-ajat on laskettu siten, että lähtöpisteenä on yrityksen toimipiste Jyväskylässä.

Taulukko 3. Matkustusajat laitetiloittain

Laitetila	Matka	Aika
1	35km	30m
2	33km	30m
3	42km	35m
4	53km	45m
5	60km	50m
6	67km	1h
7	67km	1h
8	100km	1h 20m
9	100km	1h 20m
10	120km	1,5h
11	120km	1,5h
12	140km	1h 40m
13	150km	1h 50m
14	165km	2h

Pelkkä matkustusaika ei kuitenkaan ole palauttamiseen kuuluva kokonaisuus. Tähän aikaan on lisättävä ajat joihin kuuluvat vikaan reagointi, varalaitteiden nouto ja itse palautusprosessi paikan päällä. Vian ilmetessä ei ole yleensä itsestään selvää, että vika olisi fyysinen ja vaatisi paikan päällä käymistä. Vikaa yritetään yleensä ensisijaisesti korjata etähallintaa hyödyntäen. Tällaisessa tilanteessa takarajana ongelman rajaamiseen on noin puoli tuntia, jonka jälkeen toimenpiteisiin ryhdytään. Normaalina työaikana, tiimin toinen henkilö voi koittaa ratkaista ongelmaa etänä, jos ollaan vielä epävarmoja syystä, samalla kun toinen henkilö on matkalla laitetilaan. Mikäli ongelma ratkeaa matkan aikana, ei laitetilassa tarvitse käydä paikan päällä. Kuvio 13 havainnollistaa palauttamiseen kuluvia kokonaisaikoja eri sijainteihin viitaten.



Kuvio 13. Palautusajat

Taulukko 4 esittää palautukseen kuluvat kokonaisajat laitetiloittain.

Taulukko 4. Palautusajat laitetiloittain

Laitetila	Aika
1	1,5h
2	1,5h
3	1h 35m
4	1h 45m
5	1h 50m
6	2h
7	2h
8	2h 20m
9	2h 20m
10	2,5h
11	2,5h
12	2h 40m
13	2h 50m
14	3h

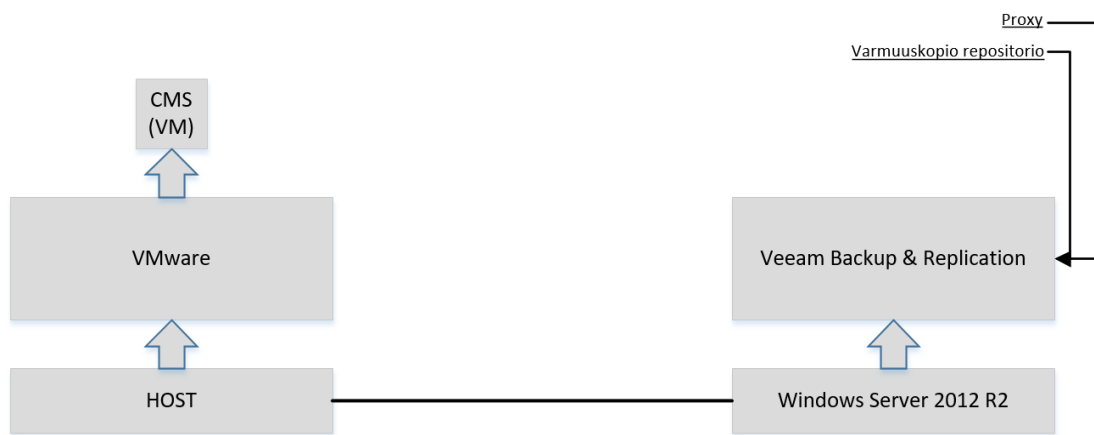
3.8 Calix E7-2:n palautus

Kun Calix E7-2 vikaantuu jossain kappaleessa 3.7 käsitellyistä laitetiloista, lähdetään palautusta toteuttamaan. Ensimmäisenä käytetään hetki tilannearviointiin ja tutkitaan, pystytäänkö ongelma ratkaisemaan etänä. Jos tullaan siihen tulokseen, että vika vaatii paikalla käyntiä, katsotaan dokumentaatiosta laitteen komponenttien tiedot. Tietojen perusteella, otetaan mukaan tarvittavat tavarat.

Kun saavutaan laitetilaan, aloitetaan palautusprosessi vaihtamalla varalaitte rikkoutuneen laitteen tilalle. Tämän jälkeen palautetaan rikkoutuneen laitteen varmuuskopio varalaitteeseen ja vaihdetaan se käyttöön.

3.9 CMS-palvelimen palautus

Varmuuskopiointi on toteutettu Veeam Backup & Replication version 9 palvelimella. Varmuuskopiopalvelin sijaitsee fyysisesti eri sijainnissa, kuin itse virtuaalilaitteisto. Kuvio 14 havainnollistaa varmuuskopiointin arkkitehtuurin.



Kuvio 14. Varmuuskopiointin arkkitehtuuri

Mikäli CMS-palvelimeen tulee vikaa, on sen palauttamiseen olemassa kaksi vaihtoehtoa. Palvelin voidaan palauttaa käyttäen Instant VM Recovery toimintoa, joka käynnistää virtuaalikoneen suoraan pakatusta ja deduplikoidusta varmuuskopiotiedostosta. Instant VM Recovery luo väliaikaisen kopion alkuperäisestä virtuaalikoneesta ja näin ollen mahdollistaa palauttamisen sekunneissa tai muutamassa minuutissa.

Toinen tapa jolla palvelimen toiminta saadaan palautettua, on Full VM Recovery. Full VM Recovery palauttaa täydellisen virtuaalikoneen varmuuskopiotiedostosta ja rekisteröi sen kohdehostille. Full VM Recovery toiminto vie enemmän aikaa, koska VM image täytyy purkaa tuotantolevylle.

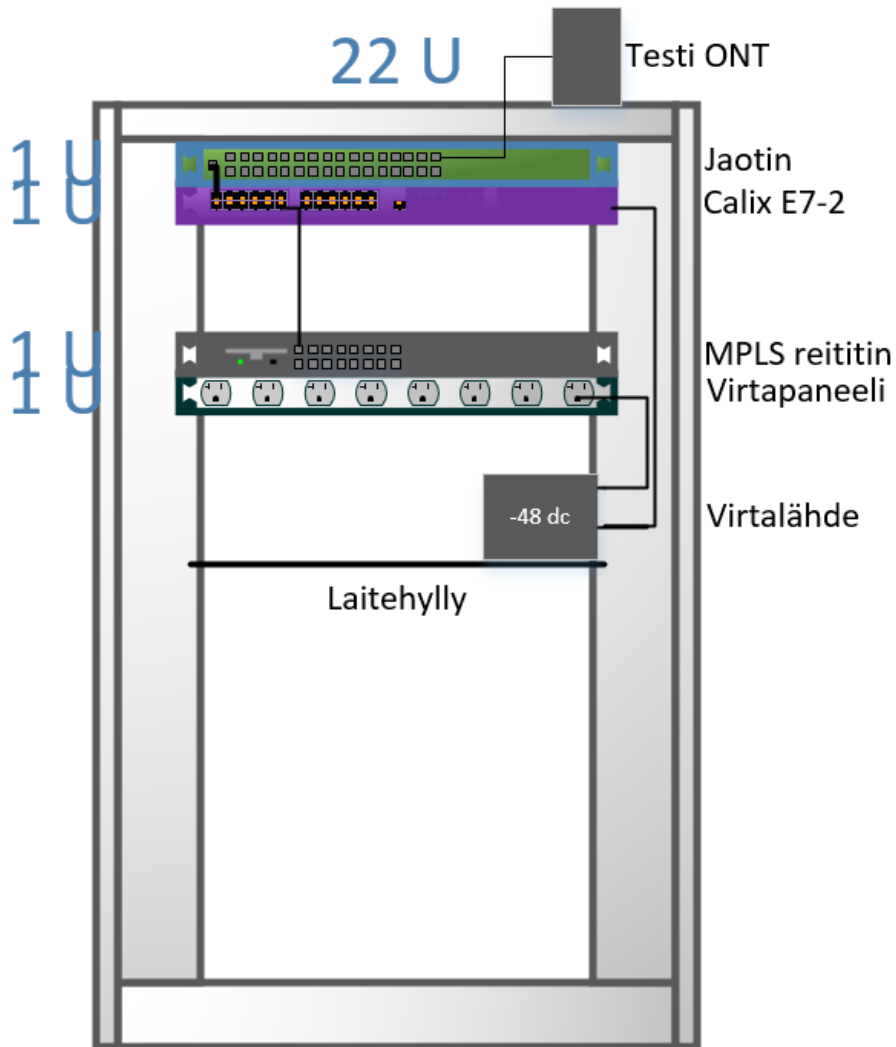
Virtuaalikone voidaan palauttaa viimeisimpään pisteeseen tai mihin tahansa muuhun palautuspisteeseen, alkuperäiseen sijaintiin tai uuteen sijaintiin. (Veeam Backup & Replication for VMware vSphere 2016, 53.)

Tämän työn toteutusvaiheessa CMS-palvelimen ajastettu varmuuskopiointi, sekä palvelimen toiminnan palauttaminen toteutettiin demovirtuaalikoneella siten, että se vastasi toteutustavaltaan täysin tuotannon CMS-palvelimen palauttamista. Palautus toteutettiin käyttäen Full VM Recovery toimintoa.

4 Toteutus

4.1 Testausympäristö

Testauslaitteisto oli asennettu 22U:n kokoiseen 19 tuuman kokoiseen laitekaappiin. Laitekaapin etuovi oli lasia, takaovi oli rei'itetty ja sivuseinät olivat irrotettavia. Laitekaapin maksimikuorma oli 500kg. Testilaitteistoon kuului MPLS (Multiprotocol Label Switching) reititin, Calix E7-2 yhdellä GPON-4 linjakortilla, 1:32 SC APC Jaotin, virtapaneeli, laitehylly, testipäätelaite eli ONT, sekä virtalähde Calix E7-2 laitteelle. DR (Disaster Recovery) laitteena oli Calix E7-2 yhdellä GPON 4-R2 linjakortilla. (ks. Kuvio 15).



Kuvio 15. Testauslaitteisto

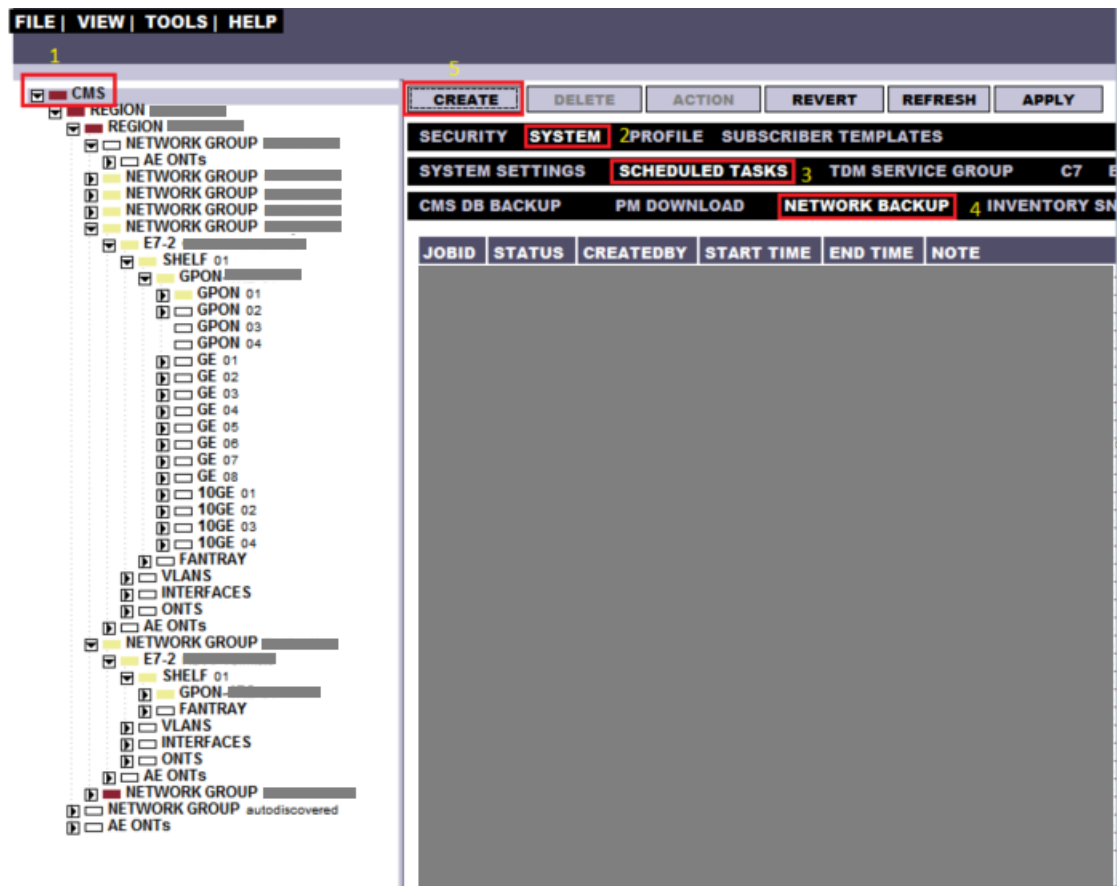
4.2 Calix E7-2:n ajastettu varmuuskopiointi

Calix E7-2:n ajastettu varmuuskopiointi asetettiin tapahtumaan viikon jokaisena päivänä, tiettyyn kellonaikaan. Ajastettu varmuuskopiointi asetettiin CMS-hallintapalvelimelta. Varmuuskopiointi Calix E7-2 laitteelta tiedostopalvelimelle tapahtui FTP (File Transfer Protocol) -protokollaa käyttäen.

Tietokannan varmuuskopiointi koostui kahdesta osasta. Ensiksi tietokannasta ja suorituskäylokeistä luotiin varmuuskopio. Tämän jälkeen varmuuskopiotiedosto siirrettiin tiedostopalvelimelle.

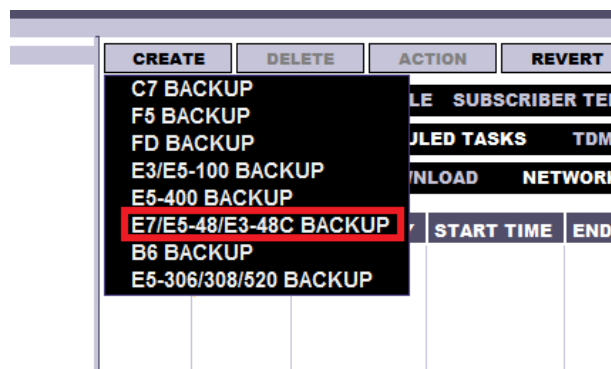
Varmuuskopiointin palautus koostui myös kahdesta vaiheesta. Ensiksi noudettiin viimeisin varmuuskopiotiedosto tiedostopalvelimelta. Tämän jälkeen nykyinen tietokanta korvattiin noudetulla varmuuskopiointitiedostolla.

Ajastetun varmuuskopiointin määrittäminen aloitettiin seuraavasti: Valittiin CMS -> SYSTEM -> SCHEDULED TASKS -> NETWORK BACKUP -> CREATE. (ks. Kuvio 16).



Kuvio 16. E7 backup-vaihe 1

Tämän jälkeen avautuvasta ikkunasta valittiin E7 BACKUP. (ks. Kuvio 17).



Kuvio 17. E7 backup-vaihe 2

Seuraavaksi määriteltiin tehtävä suoritettavaksi myöhemmin valitsemalla schedule for laiter ja asetettiin haluttu kellonaika varmuuskopiointiin ajankohdaksi. Valittiin myös recurring ja asetettiin varmuuskopiointitehtävä suoritettavaksi päivittäin tiettyyn kellonaikaan. Tehtävään syötettiin myös tiedostopalvelimen tiedot sekä haluttu kohdeosoite varmuuskopiointille. Network Selection kohdasta valittiin haluttu Calix E7-2 laite varmuuskopioitavaksi. (ks. Kuvio 18).

Kuvio 18. E7 backup-vaihe 3

Kun tehtävä oli suoritettu, toiminta voitiin varmistaa varmuuskopiointiin ajankohdan jälkeen listauksesta, joka onnistuneen varmuuskopiointin jälkeen näytti tältä. (ks. Kuvio 19).

602 SUCCESSFUL Recurring instance for task 601.1 succeed;0 failed;0 Skippe...

Kuvio 19. E7 backup-vaihe 4

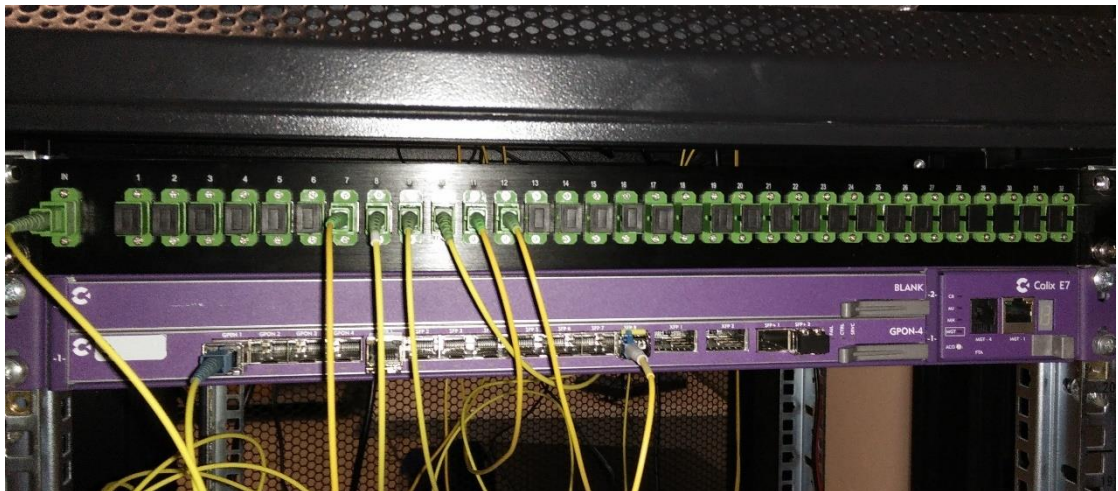
Tämän jälkeen voitiin vielä siirtyä tiedostopalvelimelle ja tarkistaa määritetystä polusta, että varmuuskopiointi oli varmasti onnistunut. (ks. Kuvio 20).

NTWK-CalixE7-██████████-backup-██████████.logs.card-1.1	220 KB	██████████
NTWK-CalixE7-██████████-backup-██████████.logs.card-1.2	220 KB	██████████
NTWK-CalixE7-██████████-backup-██████████.provd.b	20 KB	██████████

Kuvio 20. E7 backup-vaihe 5

4.3 Calix E7-2:n palautus

Testiympäristössä 19 tuuman räkkiin oli kytkettynä Calix E7-2, jonka testaustilanteessa katsottiin vikaantuneen fyysisesti. Kytkimen yläpuolella räkissä oli 19 tuuman 1:32 SC APC-jaotin, jolla syötettiin testi ONT päätelaitetta. Päätelaite oli kytkettynä SC APC kuiduilla jaottimeen. Jaotin oli kytkettynä kytkimen GPON porttiin 1-1-1. Uplinkkinä käytettiin porttia 1-1-GE8 (SFP 8). Kuidut oli kytketty väliaikaisesti suoraan laitteen etupaneelin eteen. Tuotantoympäristössä kuidut asetellaan siististi kulkemaan räkin reunaa pitkin ja niille tehdään mahdollinen vedonpoisto. (ks. Kuvio 21).



Kuvio 21. Testausympäristö

Palautus aloitettiin kytkemällä varalaitteen virtalähde sähkösyöttöön, jolloin laite käynnistyi. Kun laite oli käynnistynyt, kytkettiin Ethernet kaapeli kytkimen front management porttiin (MGT-1). (ks. Kuvio 22).



Kuvio 22. Varalaite

Tämän jälkeen avattiin SSH (Secure Shell) yhteys laitteeseen ja määriteltiin system turnup asetukset. Asetuksissa määriteltiin Calix E7-2:n rooli, aikavyöhyke, järjestelmän ID (Identification), sijainti, määriteltiin hallintaporttien asetukset (etu, taka ja in-band). Etuportti voitiin määrittää jakamaan osoitteet DHCP:lla, jolloin staattista IP-osoitetta (Internet Protocol address) ei tarvitse määrittellä käytettäessä etu-porttia hallintaan. Lisäksi voitiin määrittellä NTP (Network Time Protocol) palvelimen osoite, SNMP (Simple Network Management Protocol) asetukset, sekä määrittellä sallitaanko hallinta myös telnetillä ja HTTP:llä (Hypertext Transfer Protocol) salaamatonta yhteyttä käyttäen. Testausympäristössä voitiin jättää telnet, sekä salaamaton verkkohallinta päälle, mutta tuotantoympäristössä mieluiten ei. (ks. Kuvio 23).

```
login as: e7
Calix E-Series

e7@192.168.1.1's password:
System initial configuration:
(standalone, MC controller, cancel) [s/m/c]: s
Type 'quit' at any prompt to stop.
Timezone (? for a list): Euro
Timezone (? for a list): Europe/Helsinki
System ID: E7-DR
System location: Varasto
Network interface to setup: Front/Rear craft, in-band [f/r/i]: f
IP Address [192.168.1.1]:
Subnet Mask [255.255.255.0]:
Enable DHCP server on this interface? [y/n]: y
Start of DHCP client address range [192.168.1.100]:
End of DHCP client address range [192.168.1.102]:
Network interface to setup: Front/Rear craft, in-band, or done [f/r/i/d]: i
Management VLAN: ██████████
IP Address [0.0.0.0]: ██████████
Subnet Mask [0.0.0.0]: ██████████
Network interface to setup: Front/Rear craft, in-band, or done [f/r/i/d]: d
Management gateway: ██████████
Use NTP for system time? [y/n]: y
NTP server host: ██████████
Set up SNMP (for trap generation)? [y/n]: n
Enable access to the CLI via Telnet [y/n]: y
Enable access to the web GUI via HTTP (not HTTPS) [y/n]: y
```

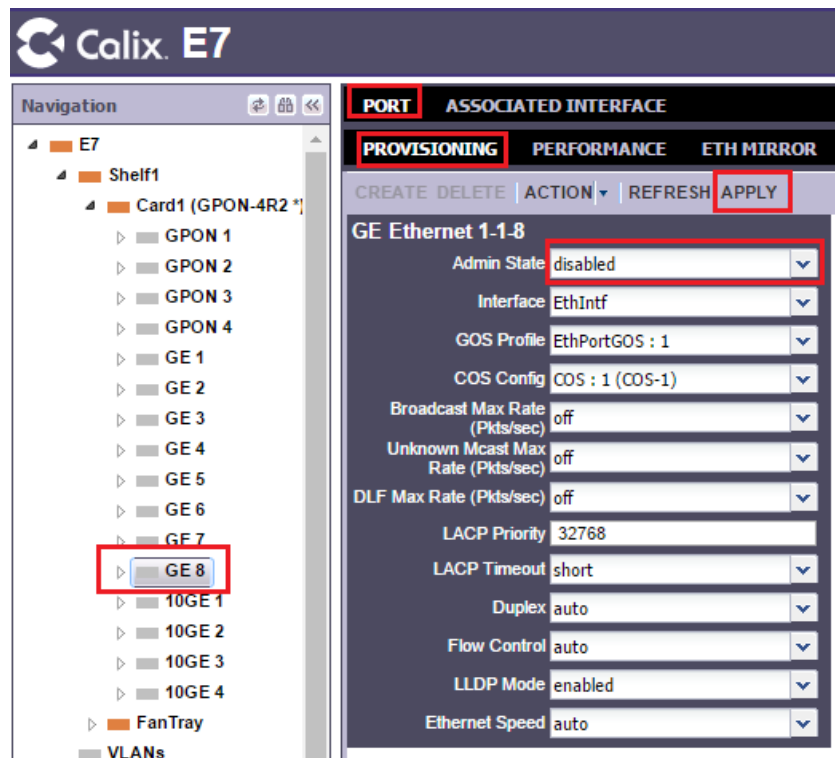
Kuvio 23. Turnup

Kun system startup oli ajettu läpi, siirryttiin laitteen hallintaan selaimella ja kirjaututtiin sisään. (ks. Kuvio 24)



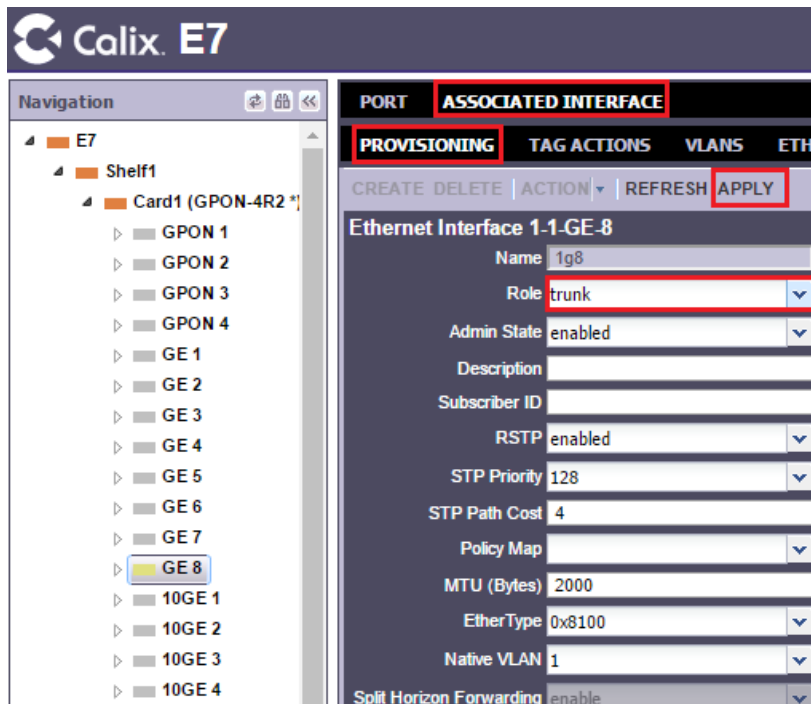
Kuvio 24. kirjautuminen

Tämän jälkeen avattiin vastaava uplink portti (GE 8), kun voittuneessa laitteessa. (ks. Kuvio 25).



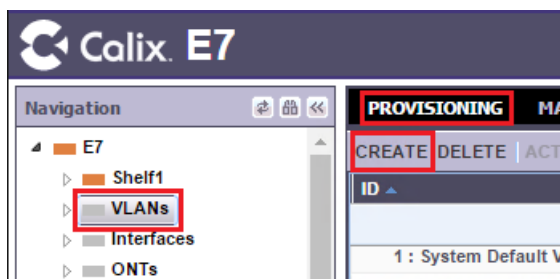
Kuvio 25. Interface enable

Tämän jälkeen asetettiin portin rooli trunkiksi. (ks. Kuvio 26).



Kuvio 26. Role trunk

Tämän jälkeen luotiin hallinta VLAN (Virtual LAN) siirtymällä VLAN asetuksiin ja valitsemalla CREATE. (ks. Kuvio 27).



Kuvio 27. VLAN Create

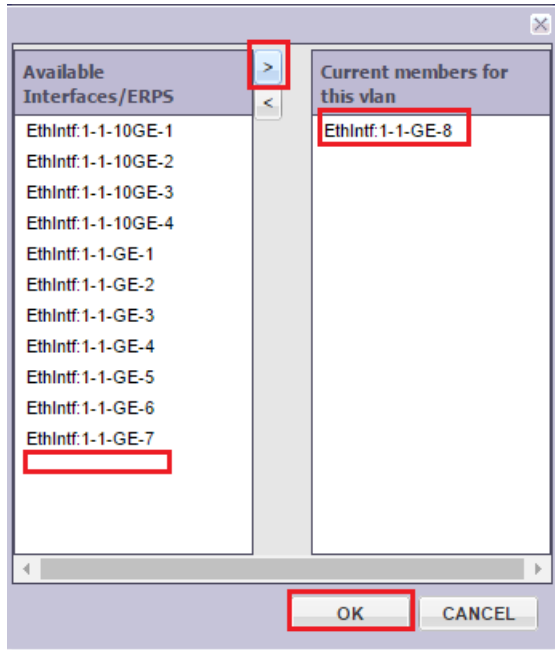
Avautuvaan ikkunaan määriteltiin VLAN ID ja valittiin halutut asetukset. Kun määrittelyt oli tehty, jatkettiin eteenpäin valitsemalla CREATE. (ks. Kuvio 28)

Kuvio 28. VLAN Create

Tämän jälkeen asetettiin luotu hallinta VLAN Uplink porttiin. Siirryttiin kohtaan PROVISIONING -> ACTION -> Add/Remove VLAN Members. (ks. Kuvio 29)

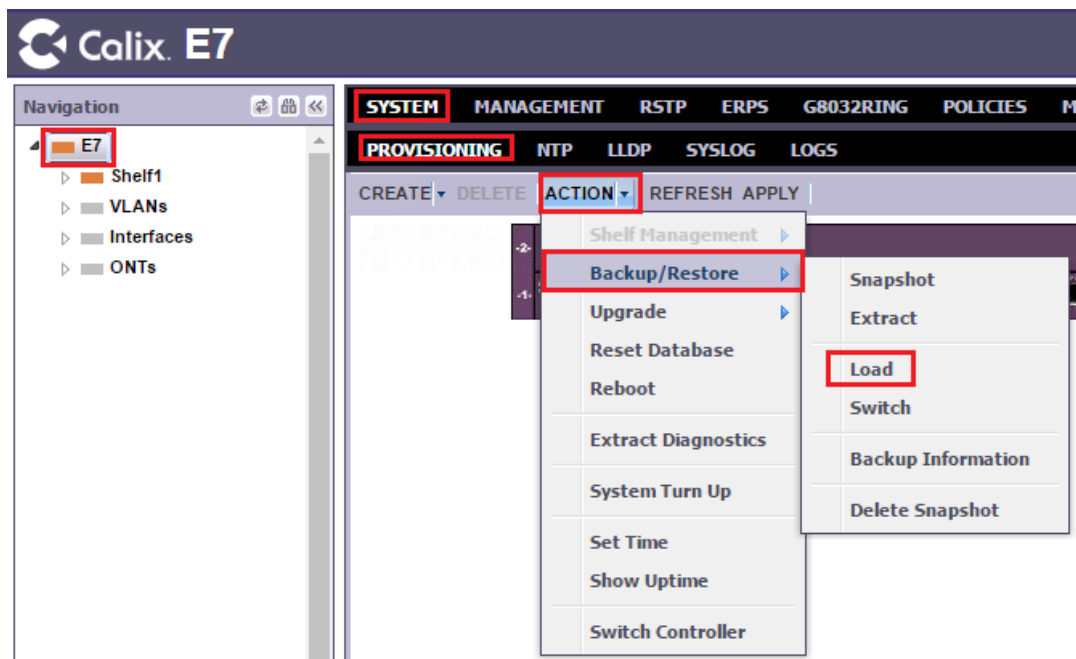
Kuvio 29. VLAN member

Avautuvasta ikkunasta valittiin uplink portti (GE8) ja lisättiin se hallinta VLAN:n jäseneksi (ks. Kuvio 30).



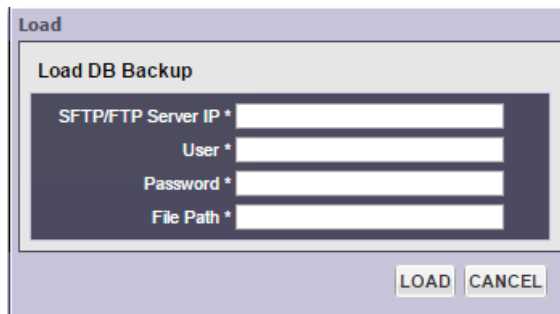
Kuvio 30. VLAN member

Kun hallinta VLAN oli asetettu porttiin, varalaite oli konfiguroitu siten, että sitä pystyttiin hallitsemaan etänä. Hallintaan päästiin siirtymällä aikaisemmassa vaiheessa määritettyyn in-band management osoitteeseen. Tämän jälkeen ladattiin vioittuneen laitteen varmuuskopioitu konfiguraatio, sekä provisiointitietokanta uudelle laitteelle ja vaihdettiin ne käyttöön. Tämä tehtiin siirtymällä E7 -> SYSTEM -> PROVISIONING -> ACTION -> Backup/Restore -> Load. (ks. Kuvio 31)



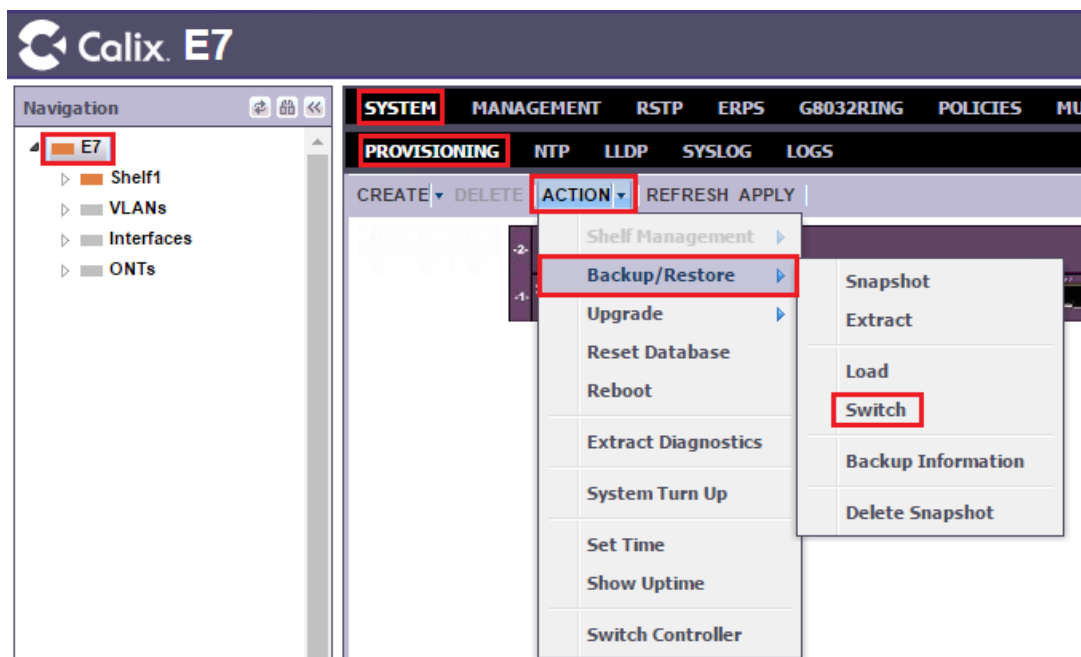
Kuvio 31. Backup load

Avautuvaan ikkunaan syötettiin tiedostopalvelimen tiedot, sekä varmuuskopiointin polku ja valittiin LOAD. (ks. Kuvio 32)



Kuvio 32. FTP information

Kun tiedosto oli ladattu varalaitteelle, vaihdettiin ladattu konfiguraatio käyttöön valitsemalla Switch. Avautuvasta ikkunasta valittiin forced, jolloin kytkin aloitti konfiguraation käyttöönoton. (ks. Kuvio 33)



Kuvio 33. Backup switch

Tämän jälkeen odotettiin noin minuutti, jonka aikana kytkin otti käyttöön konfiguraation ja käynnistyi uudelleen. Noin kahden minuutin kuluttua nähtiin testipäätelaitteen LED-valoista, että service paloi vihreänä, josta voitiin todeta kytkimen palautuminen onnistuneeksi. Internet yhteyden toiminta testattiin kytkemällä kannettava tietokone laitteen Ethernet -porttiin.

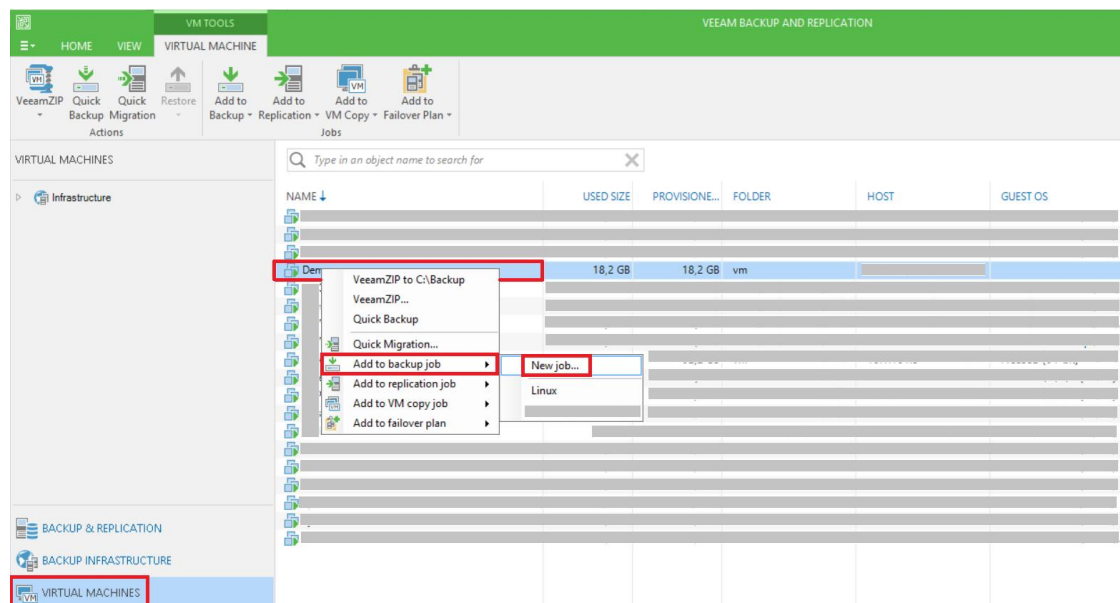
Varmuuskopion palauttamisen jälkeen, varalaite oli vaihtanut käyttöönsä voittuneen laitteen konfiguraation ja provisiointi tietokannan, siten että laitetta kyettiin hallitsemaan etänä.

Todellisessa tilanteessa varmistetaan palveluiden toiminta tarkastelemalla laajemmin kuluttaja-asiakkaiden päätelaitteiden tietoja CMS-palvelimelta. Kun todetaan että palvelun tilaajien laitteet ovat hakeneet IP osoitteen, voidaan varmistua siitä, että palauttaminen on onnistunut.

Palauttamistestauksessa erityishuomiona, että voittuneen laitteen linjakortti oli mallia GPON-4 ja DR laitteen linjakortti mallia GPON-4R2. Palauttaminen suoritettiin onnistuneesti, vaikka DR laitteessa oli uudempi kortti.

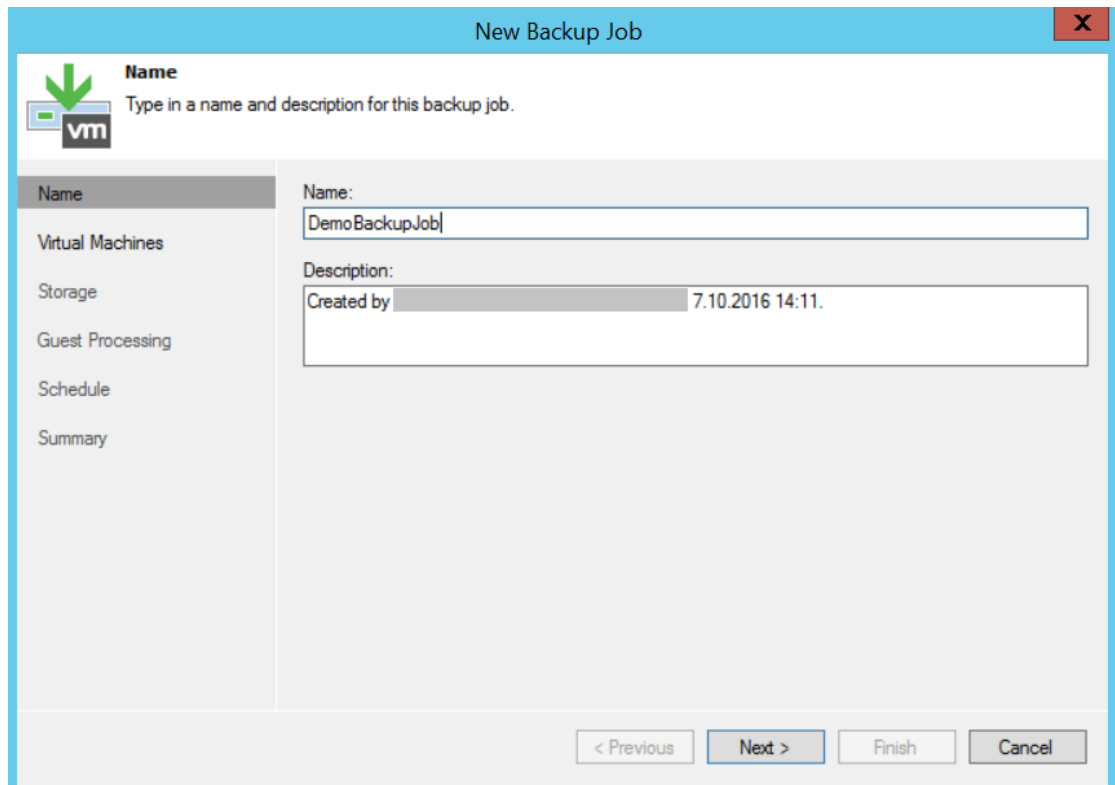
4.4 CMS-palvelimen ajastettu varmuuskopiointi

Palvelimen palauttaminen aloitettiin valitsemalla vasemmalta navigointipuusta Virtual Machines, jonka jälkeen valittiin hiiren oikealla painikkeella näkymästä se virtuaalikone, jolle varmuuskopiointityö haluttiin luoda. Valittiin Add to backup job -> New job. (ks. Kuvio 34)



Kuvio 34. Backub job

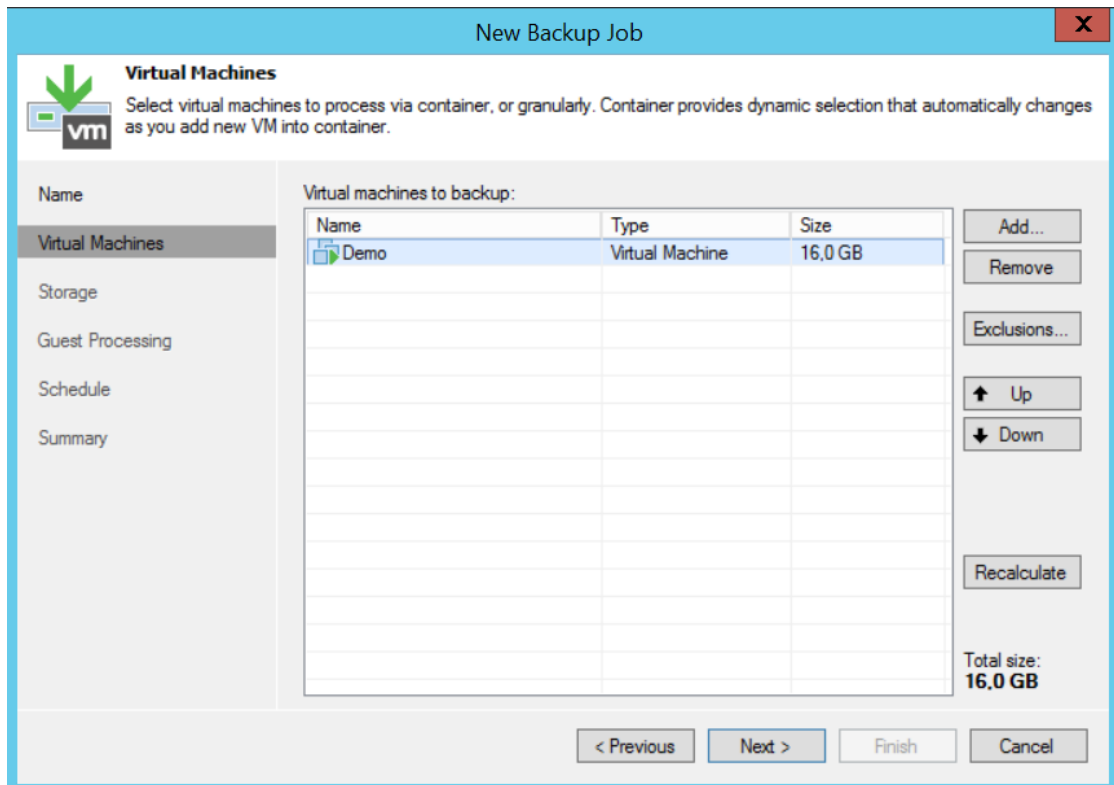
Annettiin työlle nimi ja valittiin Next. (ks. Kuvio 35).



The screenshot shows a window titled "New Backup Job" with a close button (X) in the top right corner. The window has a blue header bar. Below the header, there is a green arrow icon pointing down to a "vm" icon. The text "Name" is displayed in bold, followed by the instruction "Type in a name and description for this backup job." On the left side, there is a vertical navigation pane with the following items: "Name" (selected), "Virtual Machines", "Storage", "Guest Processing", "Schedule", and "Summary". The main area contains two text input fields. The first is labeled "Name:" and contains the text "DemoBackupJob". The second is labeled "Description:" and contains the text "Created by 7.10.2016 14:11.". At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Kuvio 35. Job name

Työ haluttiin tehdä vain kyseiselle virtuaalikoneelle, joten jatkettiin valitsemalla Next. Oikealta valitsemalla Add työhön olisi voinut lisätä virtuaalikoneita tai VM Container: kansioita, resurssipooloja, klustereita, vAppseja tai datastoreja. Jos valittaisiin container ja containeriin lisätään virtuaalikone myöhemmin, sisältyisi uusi virtuaalikone automaattisesti aiemmin luotuun työhön. Mikäli työhön olisi lisätty VM container, olisi kohdasta Exclusions voitu määrittellä virtuaalikoneet, joita ei sisällytetä kyseiseen työhön. (ks. Kuvio 36).



Kuvio 36. Työn kohteet

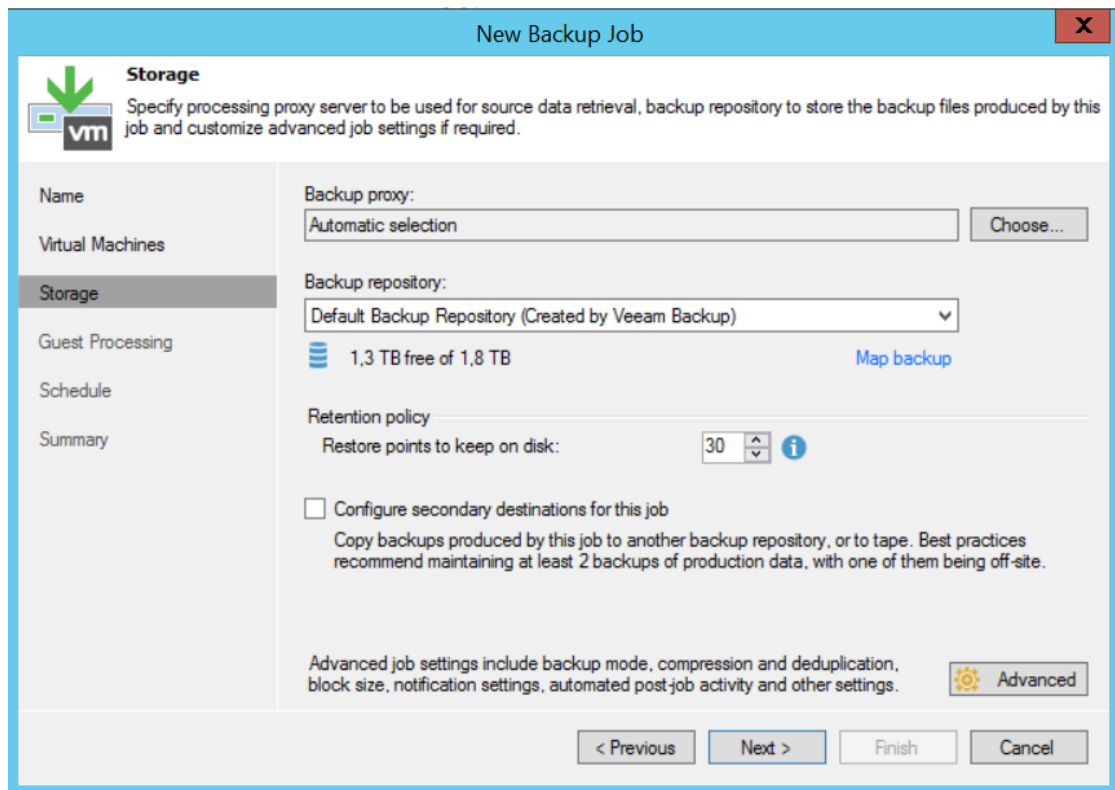
Storagen määrittelyssä ensimmäisenä on kohta Backup proxy (ks. Kuvio 37). Valitsemalla Choose voidaan valita määritetyistä backup proxyista haluttu, mikäli proxyja on määritelty useita. Valittiin Automatic selection, koska näin valittuna Veeam Backup & Replication tarkistaa saatavilla olevien proxy palvelimien asetukset ja käyttää näistä automaattisesti sitä, jolla data saadaan noudettua tehokkaimmin. Tässä tapauksessa palvelin toimi itse proxyana.

Kohdassa Backup repository valitaan konfiguroitu repositorio. Käytettiin automaattisesti valittuna olevaa repositoriota.

Retention policy kohdassa määritellään levyllä säilytettävien palautuspisteiden määrä. Valittiin määräksi 30, jolloin päivittäin suoritettavista varmuuskopiointitöistä on saatavilla palautuspisteet kuukauden ajalta.

Valitsemalla kohta Configure secondary destinations for this job, voidaan valita työn kohteeksi myös toinen repositorio. Noudattamalla hyviä käytänteitä, tuotantoympäristössä tulisi käyttää vähintään kahta repositoriota, joista toinen sijaitsee sivutoimipisteellä eri sijainnissa.

Seuraavaksi siirryttiin Advanced asetuksiin valitsemalla Advanced.

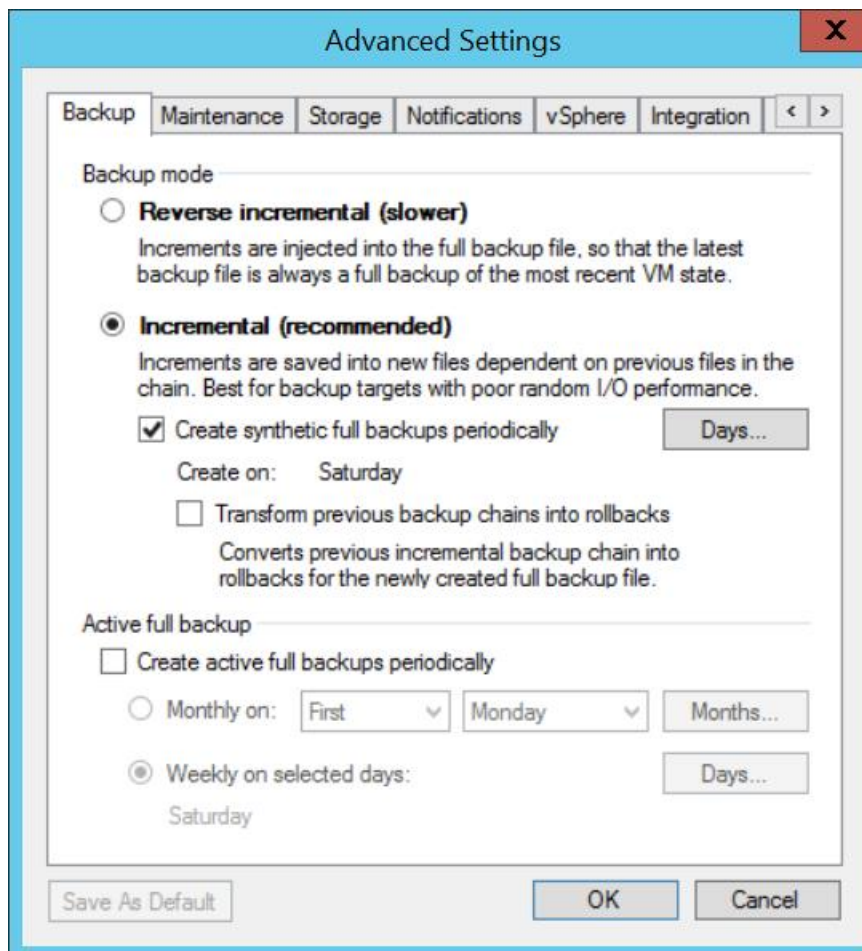


Kuvio 37. Storage

Advanced settings ikkunan välilehdeltä Backup, määritellään backup mode. Määrittäykseen on kolme vaihtoehtoa: forever forward incremental, forward incremental ja reverse incremental. Vaihtoehdot on kuvailtu tarkemmin kappaleessa 2.8.3.

Käytettiin suositeltua ja nopeampaa forward incremental vaihtoehtoa. Valittiin incremental, sekä määriteltiin kerran viikossa otettava täydellinen varmuuskopio. (ks. Kuvio 38).

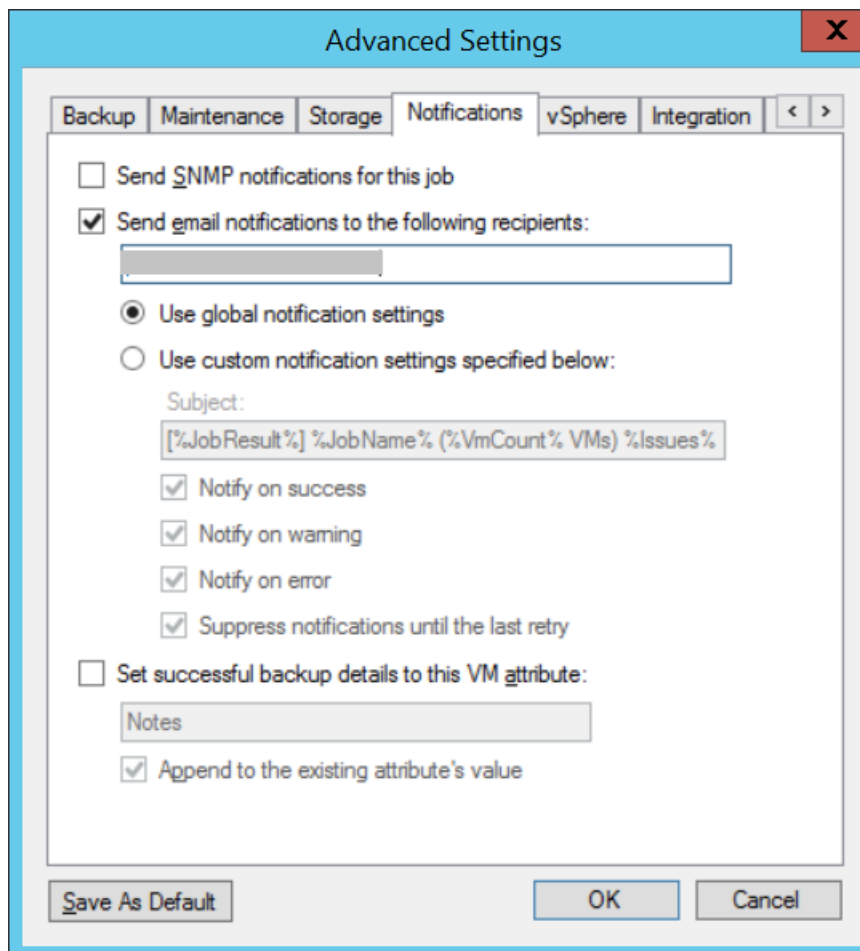
Seuraavaksi siirryttiin välilehdelle Notifications.



Kuvio 38. AS backup

Määriteltiin sähköpostihuomautus suoritetusta työstä (ks. Kuvio 39). Valittiin Send email notifications to the following recipients ja syötettiin kenttään sähköpostiosoite, joihin huomautus haluttiin lähettää. Valittiin Use global notification settings. Mikäli haluttaisiin käyttää kustomoituja huomautuksia, voitaisiin sellaiset määritellä valitsemalla use custom notification settings specified below.

Tämän jälkeen siirryttiin välilehdelle Storage.



Kuvio 39. AS Notifications

Jätettiin suositellut data reduction asetukset valituiksi (ks. Kuvio 40).

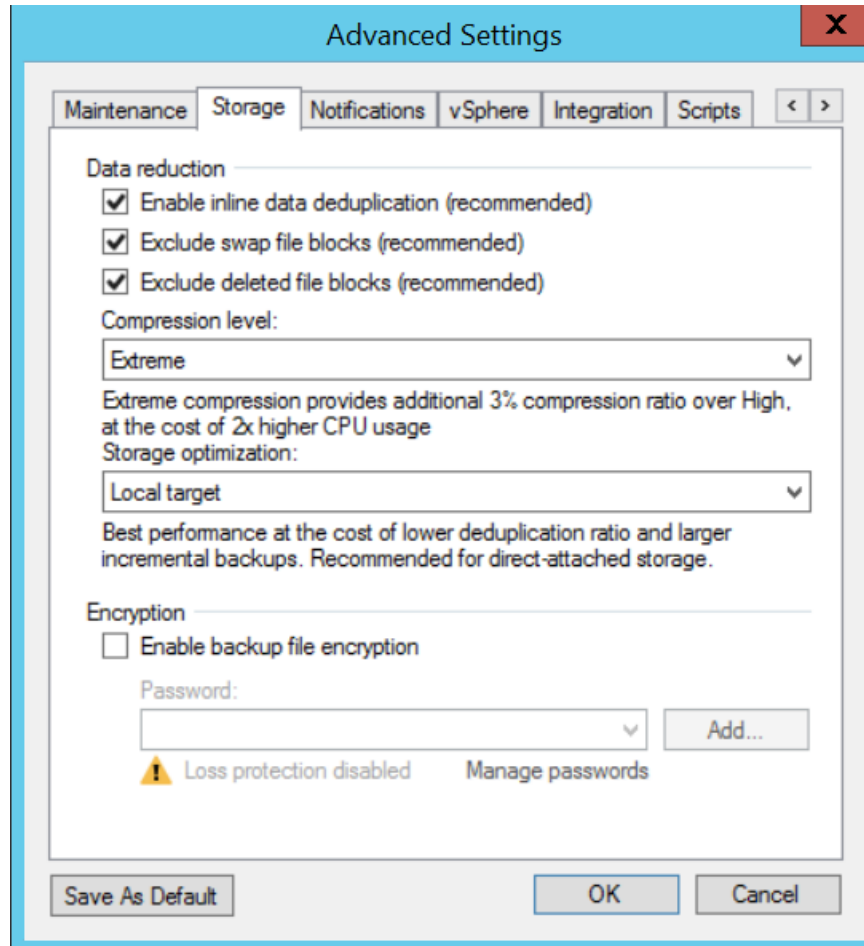
Jos samassa varmuuskopiointityössä olisi useampi virtuaalikone, joiden datablokeissa olisi identtisiä kohtia, tai virtuaalikoneita joiden levyillä on tyhjää tilaa, inline data deduplication deduplikoi identtiset datablokit. Tätä toimintoa käyttämällä saadaan tallennustilaa säästettyä, koska vältetään kirjoittamasta samaa dataa useaan kertaan levyille.

Exclude swap file blocks toiminnossa Veeam Backup & Replication identifioi datablokit virtuaalikoneen guest OS:n (Operating System) windows pagefilessä ja jättää ne pois prosessoinnista, jolloin saadaan kasvatettua suorituskykyä ja pienempiä backup incrementtejä.

Varmuuskopion kokoa saadaan pienennettyä viidellä eri vaihtoehdolla kohdassa Compression level.

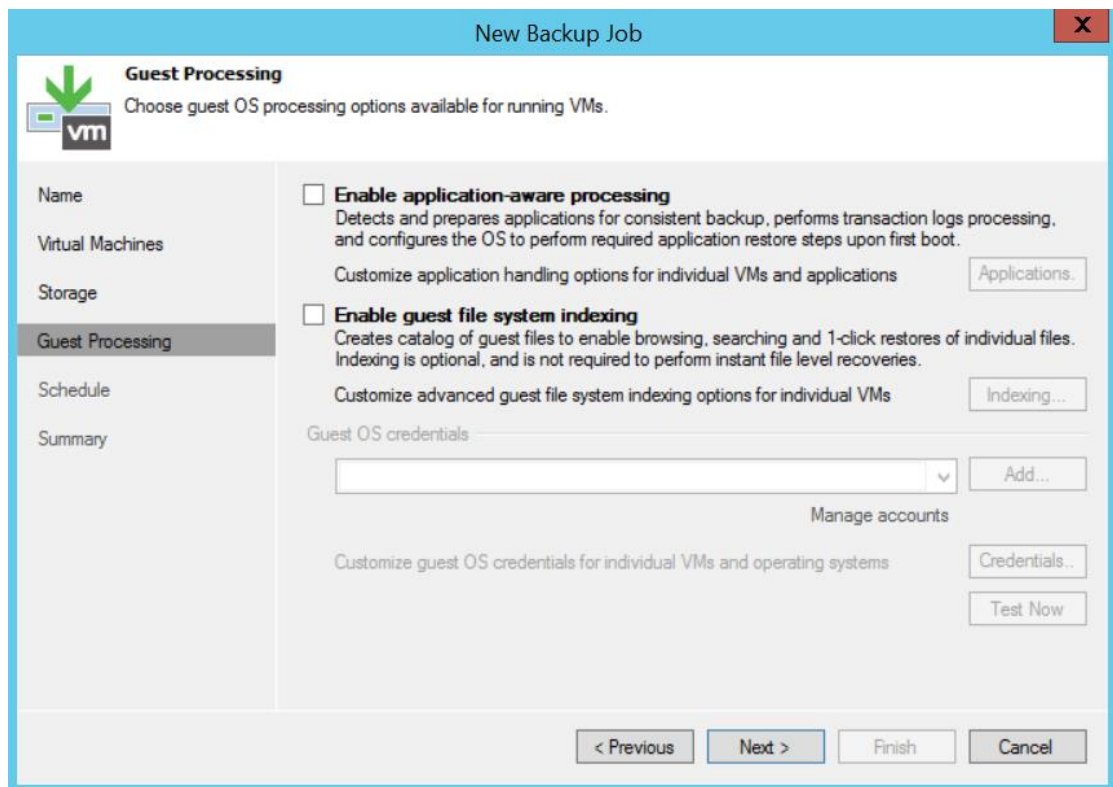
Mikäli varmuuskopiotiedostot haluttaisiin salata, voidaan salaus määritellä kohdassa Encryption.

Valittiin pakkaustasoksi Extreme, valittiin OK ja sen jälkeen siirryttiin vaiheeseen guest processing valitsemalla Next.



Kuvio 40. AS Storage

Guest processing osiossa voidaan määritellä vaihtoehtoiset asetukset virtuaalikoneen guest käyttöjärjestelmän prosessointiin. Vaihtoehtojen selitykset ovat nähtävissä kuviossa (ks. Kuvio 41). Guest käyttöjärjestelmän asetuksiin ei puututtu. Schedule kohtaan siirryttiin valitsemalla Next.



Kuvio 41. Guest processing

Ajastuksen määrittelyssä valittiin Run the job automatically ja asetettiin työ suoritettavaksi päivittäin klo. 16.00 (ks. Kuvio 42).

Automatic retry jätettiin oletusasetuksille, jolloin epäonnistuneet virtuaalikoneen prosessoinnit yritetään suorittaa kolme kertaa uudelleen kymmenen minuutin välein.

Tämän jälkeen valittiin Create, jonka jälkeen siirryttiin kohtaan Summary.

The screenshot shows the 'New Backup Job' wizard in the 'Schedule' step. The window title is 'New Backup Job' with a close button (X) in the top right corner. The 'Schedule' step is highlighted in the left sidebar, which also includes 'Name', 'Virtual Machines', 'Storage', 'Guest Processing', and 'Summary'. The main area contains the following options:

- Run the job automatically:** This section is checked. It includes four radio button options:
 - Daily at this time:** Selected. Time: 16:00, Frequency: Everyday, Days: Days...
 - Monthly at this time:** Time: 22:00, Frequency: Fourth, Day: Saturday, Months: Months...
 - Periodically every:** Frequency: 1, Unit: Hours, Schedule: Schedule...
 - After this job:** Target: Linux (Created by [dropdown])
- Automatic retry:** This section is checked.
 - Retry failed VMs processing:** 3 times
 - Wait before each retry attempt for:** 10 minutes
- Backup window:** This section is unchecked.
 - Terminate job if it exceeds allowed backup window:** Window... button
 - If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

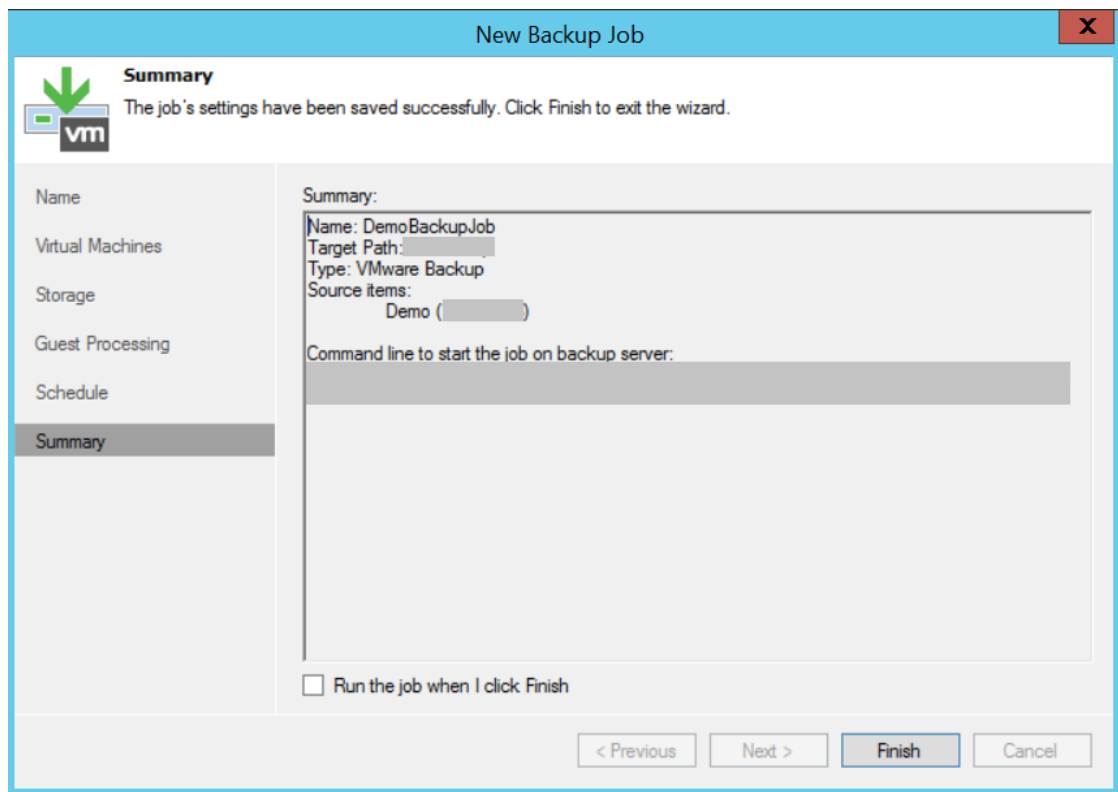
At the bottom of the wizard, there are four buttons: '< Previous', 'Create', 'Finish', and 'Cancel'.

Kuvio 42. Schedule

Summary välilehdeltä nähdään lyhyt tiivistelmä luodusta varmuuskopiointityöstä.

Työ voidaan suorittaa heti valitsemalla Run the job when I click Finish (ks. Kuvio 43).

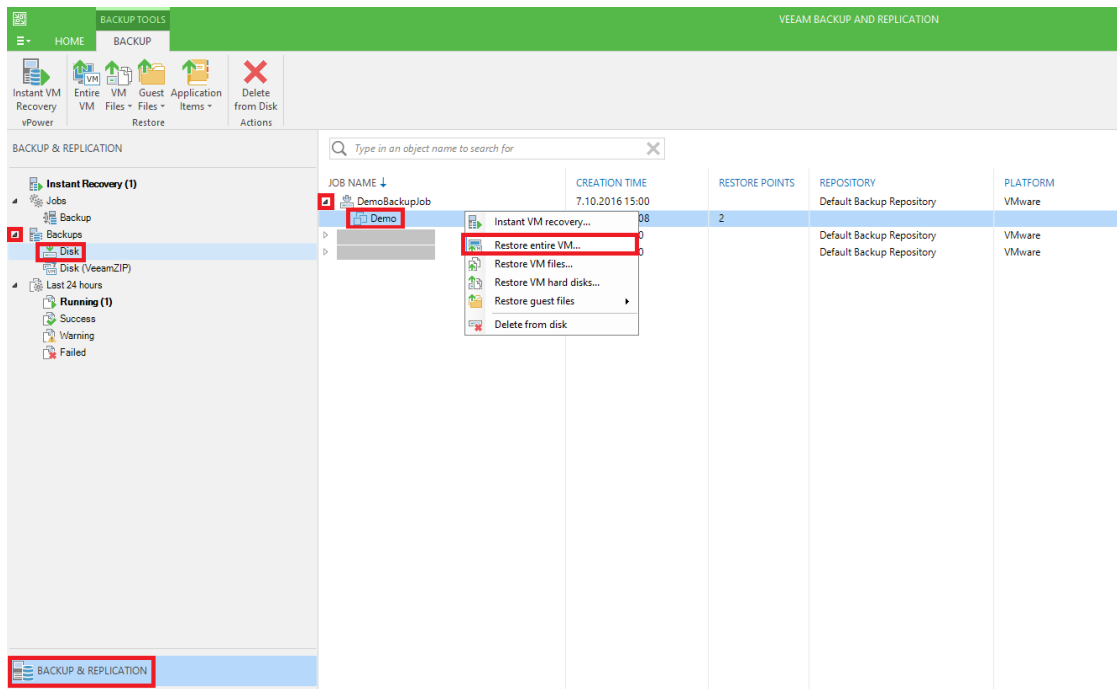
Valittiin Finish ja poistuttiin wizardista.



Kuvio 43. Summary

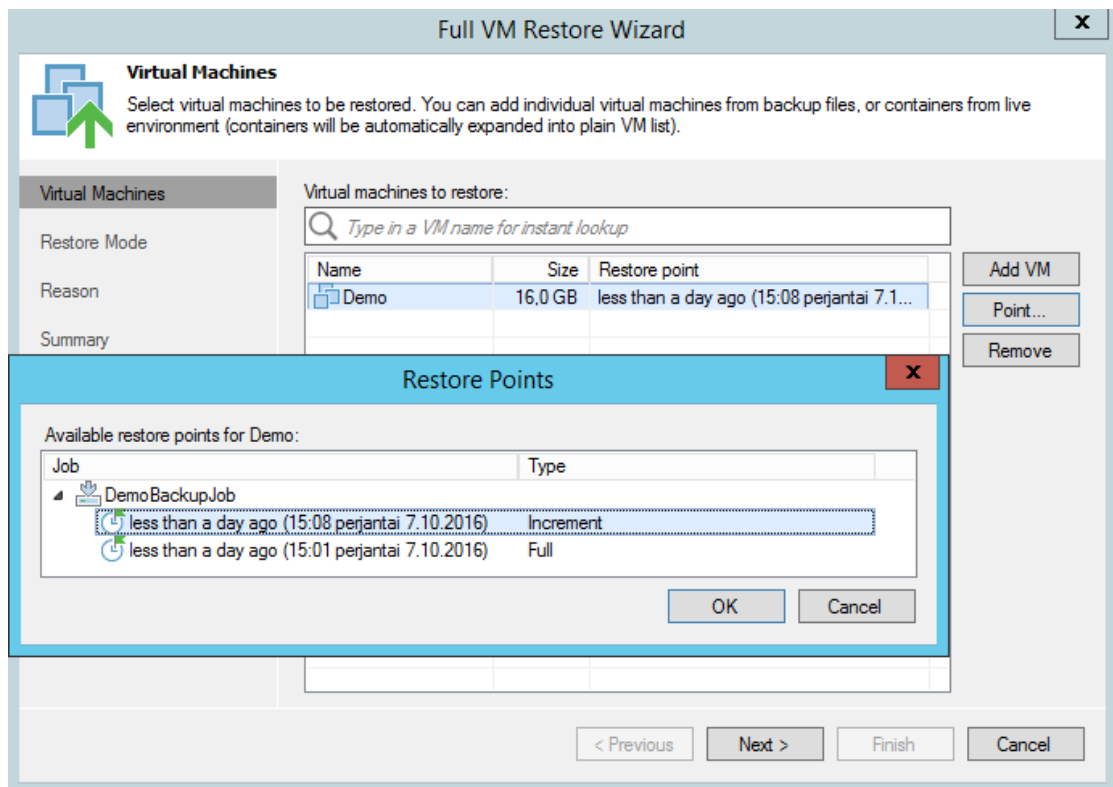
4.5 CMS-palvelimen palautuksen testaus

Palvelimen palautuksen testaus aloitettiin valitsemalla vasemmalta navigointipuusta Backup & Replication -> Backups -> Disk ja tämän jälkeen laajennettiin listauksesta haluttu työ. Valittiin hiiren oikealla virtuaalikone, jolle palautus tehdään ja valittiin Restore entire VM (ks. Kuvio 44).



Kuvio 44. Restore entire VM

Tämän jälkeen valittiin haluttu palautuspiste. Valittiin oikealta Point... ja tämän jälkeen aukeavasta Restore Points ikkunasta haluttu palautuspiste. Kun valitaan Incremental tyyppin palautuspiste, Veeam Backup & Replication palauttaa datablokit full backup tiedostosta ja incremental backup tiedostosta. Valittiin OK ja siirryttiin restore mode vaiheeseen valitsemalla Next (ks. Kuvio 45).

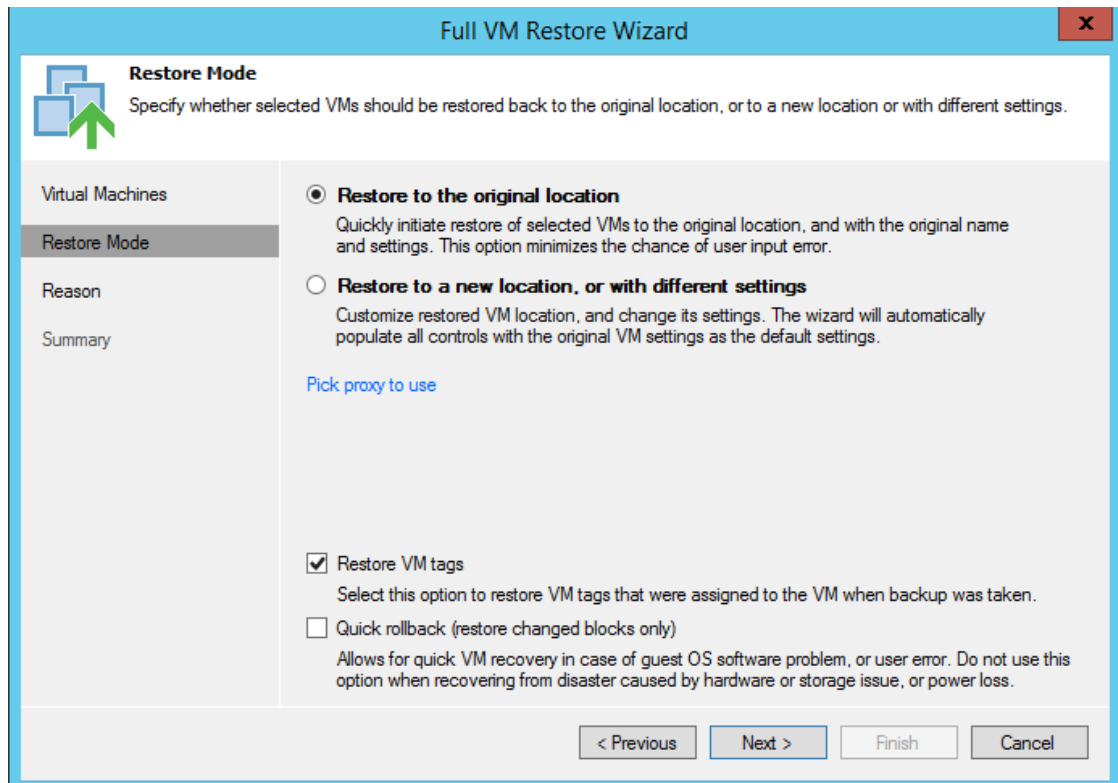


Kuvio 45. Restore Point

Mikäli kyseessä olisi palautus laiterikon jälkeen tilanteessa, jossa fyysinen host palvelin olisi vioittunut, valittaisiin vaihtoehto Restore to a new location ja palautettaisiin virtuaalikoneen toiminta rinnakkaiselle hostille (ks. Kuvio 46).

Mikäli kyseessä olisi guest käyttöjärjestelmän vika, voitaisiin valita myös Quick rollback, jolloin Veeam Backup & Replication tekee incremental VM restoren ja palauttaa vain valitun palautuspisteen jälkeen muuttuneet datablokit. Näin ollen palautusprosessi olisi myös nopeampi (ks. Kuvio 46).

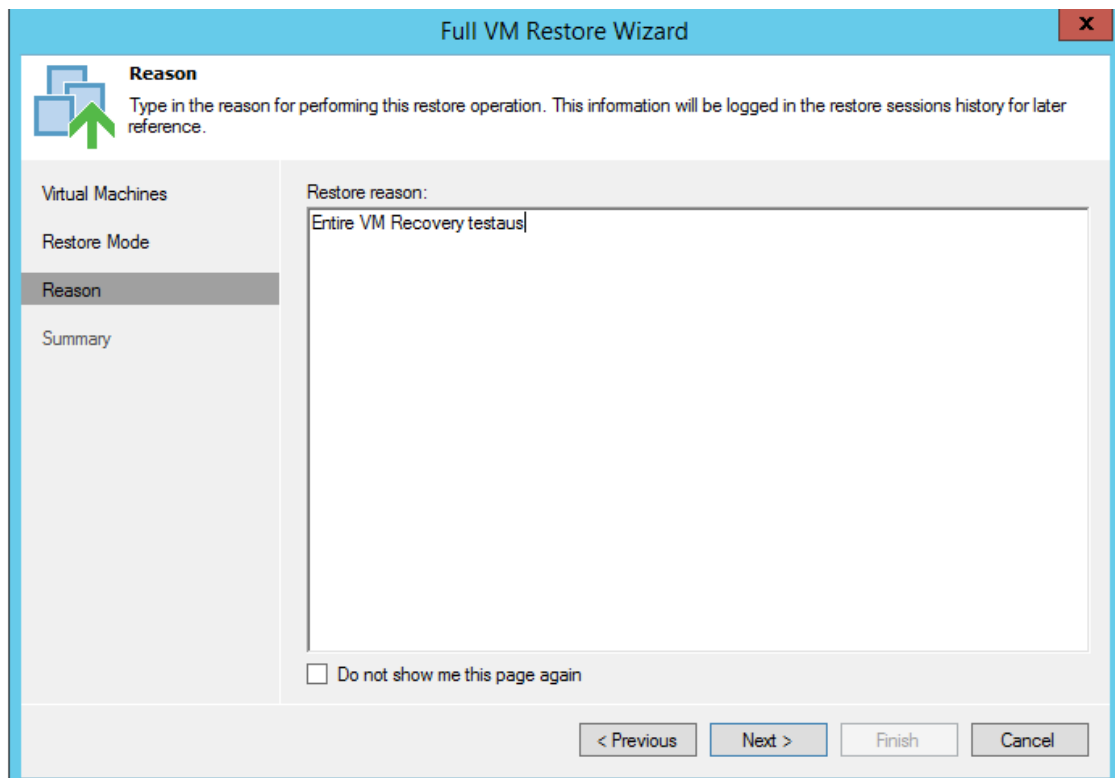
Valittiin Restore to the original location ja Restore VM tags joka on automaattisesti valittuna. Tämän jälkeen siirryttiin kohtaan Reason valitsemalla Next.



Kuvio 46. Restore Mode

Reason kohdassa on hyvä laittaa selite tehdyille palautukselle, jotta muut verkon ylläpitäjät näkevät myös miksi palautus on tehty, sekä voidaan myöhemmin tarkastella palautusten syitä, kun ne on kirjattu palautuksen yhteydessä (ks. Kuvio 47).

Siirryttiin kohtaan Summary valitsemalla Next.

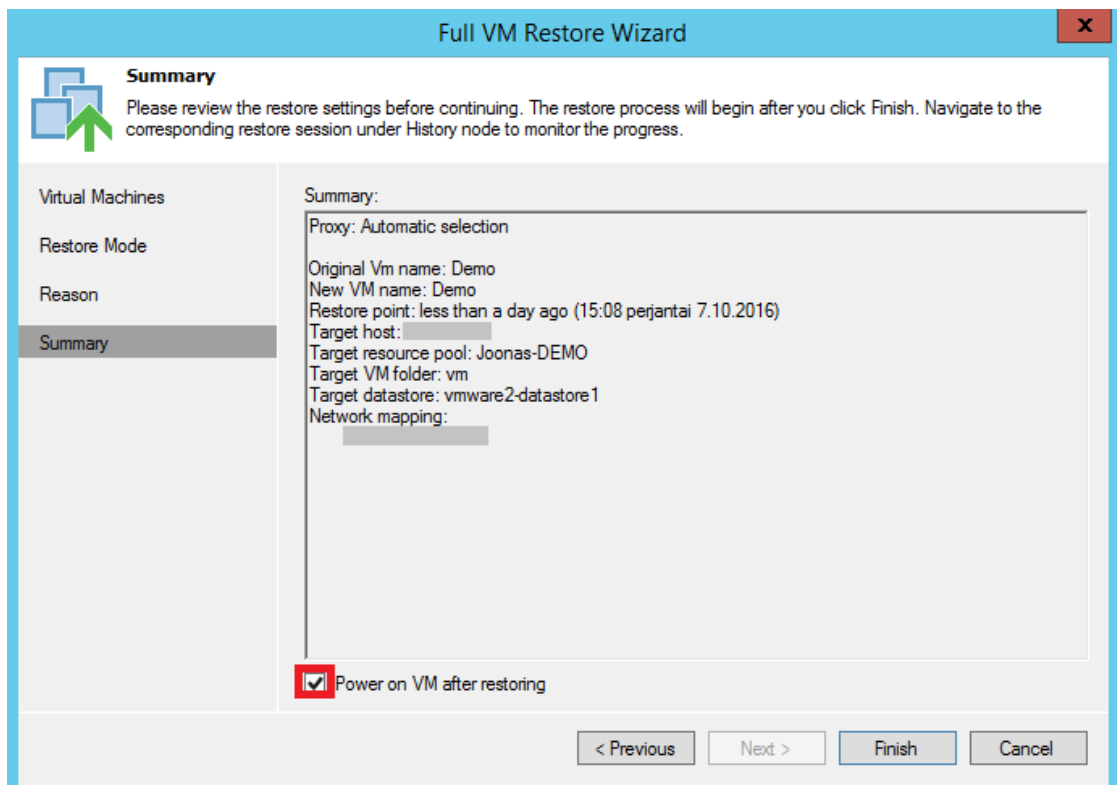


The screenshot shows the 'Full VM Restore Wizard' window, specifically the 'Reason' step. The window has a blue title bar with the text 'Full VM Restore Wizard' and a close button (X) in the top right corner. Below the title bar, there is a header area with a blue icon of three overlapping squares and an upward-pointing green arrow, followed by the title 'Reason' and a subtitle: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' On the left side, there is a vertical navigation pane with four items: 'Virtual Machines', 'Restore Mode', 'Reason' (which is highlighted with a dark grey background), and 'Summary'. The main area of the wizard is a large text box labeled 'Restore reason:' containing the text 'Entire VM Recovery testaus|'. Below the text box, there is a checkbox labeled 'Do not show me this page again' which is currently unchecked. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Kuvio 47. Restore reason

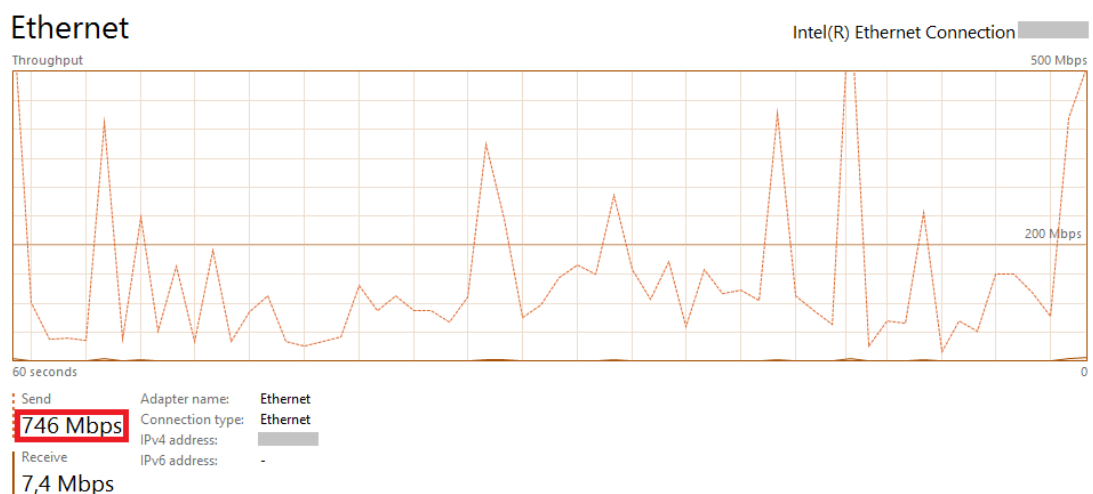
Valittiin Power on VM after restoring, jotta virtuaalikone käynnistyy itsestään palautuksen jälkeen. Välilehdellä on kooste palautuksen asetuksista. Näin voidaan vielä varmistua, että asetukset ovat oikein (ks. Kuvio 48).

Painettiin Finish ja siirryttiin tarkastelemaan palautuksen suoritusta.



Kuvio 48. Summary

Veeam Backup & Replication palvelimen verkkokortin monitoroinnista voidaan tarkastella, millä nopeudella palautettava varmuuskopio siirtyy kohde hostille. (ks. Kuvio 49).

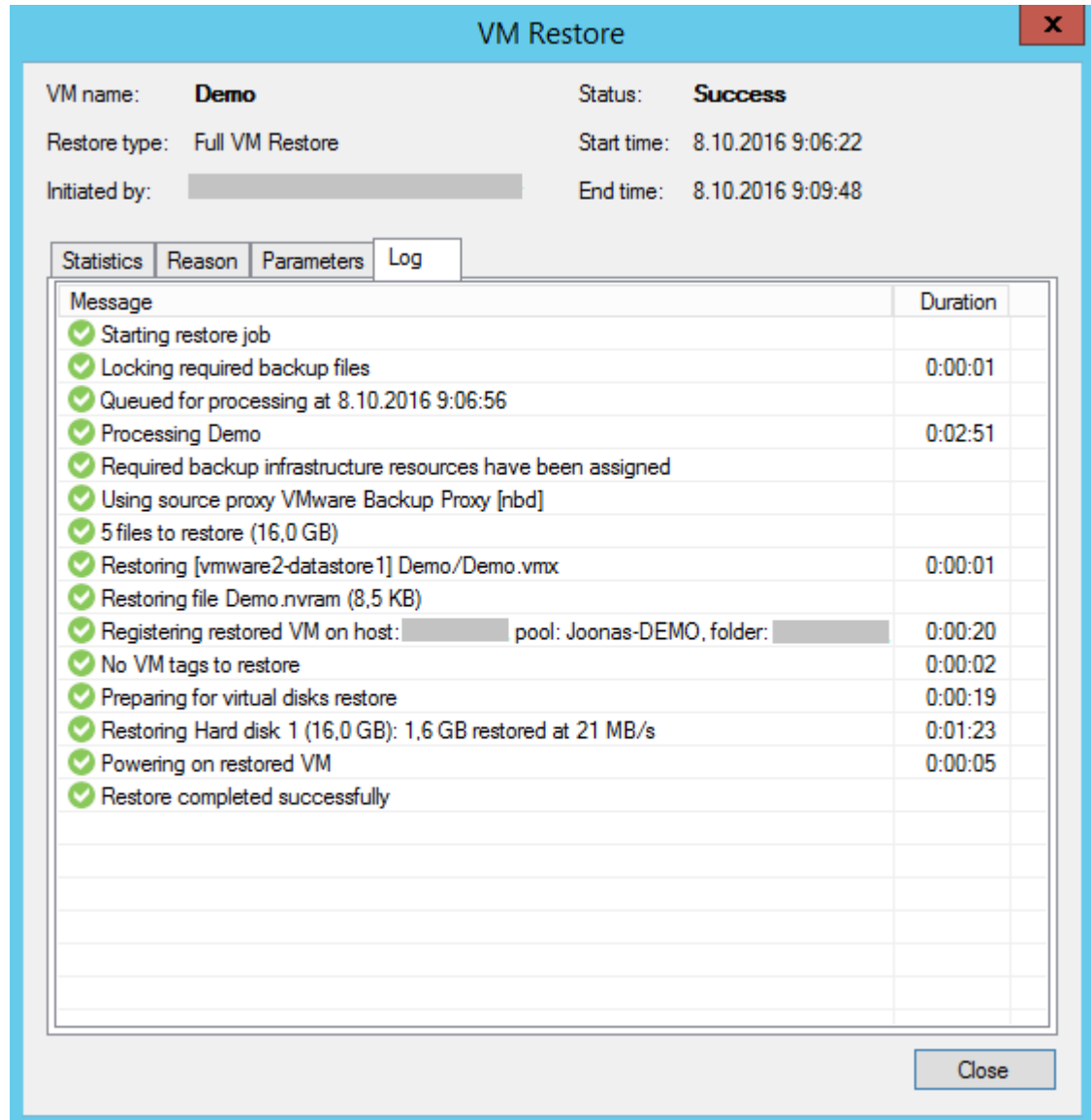


Kuvio 49. Upload nopeus

Palautuksen lokitiedot ilmestyvät näkyviin suorituksen aikana. Niitä tarkastelemalla voi seurata palautuksen vaiheita (ks. Kuvio 50).

Virtuaalikoneen onnistuneen palautuksen jälkeen Status tilana näkyy Success, ja tilan alla näkyy aloitus- ja lopetusajat.

Todettiin palautustyöhön kuluneeksi 3 minuuttia 26 sekuntia.



Kuvio 50. Restore logs

Avattiin vSphere client ja katsottiin että palautettu virtuaalikone on käynnissä alku- peräisellä hostilla (ks. Kuvio 51).



Kuvio 51. VM:n tilan tarkistus

Avattiin SSH yhteys virtuaalikoneeseen ja todettiin toiminta (ks. Kuvio 52. VM:n toiminta).

```
[root@██████████ ~]# uptime -p
up 2 minutes
[root@██████████ ~]#
```

Kuvio 52. VM:n toiminta

5 Yhteenveto

5.1 Pohdinta

Opinnäytetyön tavoitteena oli luoda palautumissuunnitelma Keski-Suomen Valokuituverkot Oy:n GPON-verkkolaitteistolle, joihin kuuluivat GPON-kytkinten hallintapalvelin ja eri kunnissa sijaitsevat Access kytkimet. Palauttamista testattiin testilaitteistolla yrityksen toimitiloissa, ja testin tuloksena vikaantunut Calix E7-2 saatiin korvattua varalaitteella. Kytkinten hallintapalvelimen palauttaminen testattiin demovirtuaalikoneella ja palautus toteutettiin käytännössä samalla tavalla kuin hallintapalvelimen palautus tehtäisiin todellisessa tilanteessa. Työssä tutkittiin, millaisella ajalla eri kunnissa sijaitsevat laitteet saadaan palautettua, mikäli vika vaatii laitteen korvaamista uudella laitteella. Ajat muodostuivat arvioidusta tilanteen kartoituksesta, matkustusajasta, sekä itse palauttamisprosessiin kuluva ajasta. Työn toteutuksessa käytiin myös läpi, kuinka laitteiden varmuuskopiointi saadaan konfiguroitua.

Tavoitteena itselläni oli oppia tuntemaan verkon ja verkkolaitteiston toimintaa vaikuttavia riskejä, sekä suunnittelemaan palautumista vikatilanteista. Tavoitteena oli myös kehittää omaa ammattitaitoa työskentelemällä internetpalveluita tarjoavassa yrityksessä. Opinnäytetyön teon aikana opin paljon uutta PON tekniikasta ja laitteista, sekä niihin vaikuttavien riskien tunnistamisesta. Uuden oppiminen tapahtui itse työn toteutusta tehdessä, sekä lähdemateriaaleihin tutustuessa.

Palautumissuunnittelusta työn aikana opin sen, että palveluntarjoajan laajuudessa verkossa riskeihin varautumiseen ja reagointiin tarvitaan taustalle monta henkilöä. Esimerkiksi runkoverkon kuitukatkoksen korjaamiseen tarvitaan kumppaniyrityksen apua hitsaamisessa ja mahdollisesti vianpaikannuksessa. Verkon monitoroinnilla, hä-

lytyksillä ja vikasietoisen verkon suunnittelulla on iso vaikutus vikatilanteisiin reagoimisessa. Automaattisten hälytysten ansiosta vikoihin pystytään reagoimaan nopeasti. Tärkeänä osana palautumissuunnittelua on huolehtia siitä, että palautumissuunnitelua koskevia laitteita on varalla aina, sekä kriittisiä vikoja korjaamaan on aina riittävä henkilöstö saatavilla.

Työ vaikutti aluksi yksinkertaiselta ja suunnittelin, että tekisin työssä palautumissuunnitelman verkon jokaiselle kriittiselle laitteelle, mutta ensimmäisten viikkojen aikana totesin, että aihetta pitää rajata paljon. Työ oli haastavuudeltaan itselleni sopiva ja koen että opin työstä paljon hyödyllistä tulevaisuutta varten.

5.2 Jatkokehitysideat

Jatkokehitysideana CMS-palvelimen, sekä Calix E7-2:n palauttamista olisi hyvä testata säännöllisesti eri kokoonpanoilla, jotta voidaan olla varmoja palauttamisen onnistumisesta vikatilanteessa. Maantieteellinen toiminta-alue on sen verran laaja, että varalaitteistoa tulisi hajasijoittaa verkon alueelle enemmän. Tällä tavoin palautusaikoja tietyissä ongelmatilanteissa saataisiin lyhyemmiksi. GPON-laitteiston, kuten muidenkin verkkolaitteiden elinkaari tulisi ottaa huomioon. Huolellisella suunnittelulla ja toiminnan testauksella saadaan ennaltaehkäistyä tulevia vikoja.

Lähteet

Calix E7-2 Ethernet Service Access Platform. N.d. Tuotetiedot Enkom Active Oy:n verkkosivulla. Viitattu 14.9.2016. http://www.enkom-active.fi/site/assets/files/1706/e7-2_system.pdf

Disaster Recovery: Best Practices. 2008. Cisco Systems Inc verkkosivu. Viitattu 26.8.2016. https://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-453495.pdf

FTTX Optiset liityntäverkot. 2015. Viitattu 29.9.2016.

GPON-4 r2 line card. N.d. Manuaali Calix Inc verkkosivulla. Viitattu 5.9.2016. https://portal.calix.com/portal/calixdocs/e-series/sysop/e7/r23/gpon_app/index.htm?toc3656213.htm?42342.htm

Gregory, P. 2007. IT Disaster Recovery Planning For Dummies. Indianapolis, Indiana: Wiley.

ITU-T G.984.3. 2014 Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification. Viitattu 1.10.2016. <https://www.itu.int/rec/T-REC-G.984.3-201401-I/en>

JHS-XXX IT-palveluiden palvelutasoluokitus. N.d. http://www.jhs-suositukset.fi/c/document_library/get_file?folderId=62114&name=DLFE-1530.pdf

Kananen, J. 2008. Kvali. Kvalitatiivisen tutkimuksen teoria ja käytänteet. Jyväskylä: Jyväskylän ammattikorkeakoulu julkaisuja. Viitattu 25.8.2016.

Kananen, J. 2011. Kvantti. Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu julkaisuja. Viitattu 25.8.2016.

Keski-Suomen Valokuituverkot Oy:n verkkosivu. 2016. Viitattu 16.8.2016. <http://www.ksvv.fi/ksvv-oy-2>

Nopea laajakaista -hanke tuo huippunopeat internetyhteydet haja-asutusalueille. 2016. Tiedote Viestintäviraston verkkosivulla. Viitattu 16.8.2016. <https://www.viestintavirasto.fi/ohjausjavalvonta/laajakaista2015.html>

Reinikainen, V., Arvinen, M. 2013. APC-liittimet tekevät tuloaan optisiin verkkoihin. Viitattu 1.10.2016. http://www.sahkoala.fi/ammattilaiset/artikkelit/tietoliikennetekniikka/fi_FI/APC-liittimet/

Saaranen, A., Puusniekka, A. 2006. Toimintatutkimus. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 11.11.2016. http://www.fsd.uta.fi/menetelmaopetus/kvali/L5_4.html

Simplify Network Operations from a Single Element Management System. N.d. Artikkelit Calix Inc verkkosivulla. Viitattu 3.9.2016. <https://sc9prod.calix.com/software/cms/>

Vasseur, J-P., Pickavet, M. & Demeester, P. 2004. Network Recovery. Morgan Kaufmann Publishers Inc. Viitattu 5.9.2016.

Veeam Backup & Replication for VMware vSphere Version 9.0. Evaluator's Guide. 2016. Viitattu 4.10.2016.

https://www.veeam.com/pdf/guide/veeam_backup_9_0_evaluators_guide_vsphere_en.pdf

Veeam Backup & Replication Version 9.0. User Guide for VMware vSphere. 2016. Viitattu 9.10.2016.

https://www.veeam.com/pdf/guide/veeam_backup_9_0_user_guide_vsphere_en.pdf

Veeam Backup & Replication What's New in v9?. 2016. Viitattu 10.10.2016.

https://www.veeam.com/pdf/new/veeam_backup_9_0_whats_new_en.pdf

Liitteet

Liite 1. Riskianalyysi

riski	Kohde	Vaikutus	Miten huomioitu	Jatkotoimenpiteet
Kuitukatkos	Runkoverkon yhteysvälit	Liikenne siirtyy varayhteydelle	Ilmoitetaan urakoitsijalle ja tilataan korjaus	Kun kuitu on hitsattu, liikenne takaisin ensisijaiselle yhteydelle
Konfigurointivirhe	Aktiivilaitteet, palvelimet	Verkon häiriöt, palvelun estyminen	backup konfiguraatio, backup hallintayhteys, NMS hälytykset, lokitietojen kerääminen	
Sähkökatkos	Aktiivilaitteet, palvelimet	Sähkönsyöttö akustolta tai UPS laitteelta	Verkkolaitteiston sähkönsyöttö on akuston tai UPS laitteen takana	Varauksen seuranta, palautumisen seuranta
Laitevika	Aktiivilaitteet, palvelimet, SFP moduulit	Palvelukatkos, palvelun häiriöt	Varalaitte saatavilla, päivystys, palautumissuunnitelma	Toiminnan varmistus laitevaihdon jälkeen
Ilkivalta	Laitetilat, jakamot	Palvelukatkos, palvelun häiriöt, laiteviat	Lukot, kulunvalvonta	Vaikutusten tarkastus, uusien laitteiden vaihto rikkottujen tilalle
Lämmitys ei toimi	Aktiivilaitteet, palvelimet	Laitteiden häiriöt, laiterikot, palvelun estyminen	Huollon tilaus, lämmityksen korjaus	Lämmityksen toiminnan varmistaminen tarkkailemalla
Jäähdytys ei toimi	Aktiivilaitteet, palvelimet	Laitteiden häiriöt, laiterikot, palvelun estyminen	Varajäähdytys suunnitteilla, jäähdytys monitoroitu ja korjaus automaattinen	Korjauksen tilan tiedustelu

Tietoturvaloukkaukset	Aktiivilaitteet, palvelimet	Palvelun häiriöt, palvelukatkos	Palomuuraus, ACL, RADIUS, hallintayhteys salattu	Tekijän selvittäminen, ilmoitus viranomaisille, aukon korjaus
Asennustyöstä johtuvat häiriöt / katkokset	Kuidut, kaapelit	palvelun häiriöt, palvelukatkos	NMS hälytykset, varayhteys, asennuksen jälkeiset tarkastukset	
Päivityksistä aiheutuvat ongelmat	Aktiivilaitteet, palvelimet, päätelaitteet	palvelukatkokset	Testataan ennen tuotannon toteutusta	