# PALVELUKUVAUS - VARMUUSKOPIOINTIPALVELU

## SISÄLLYS

# Varmuuskopiointi yleisesti

Varmuuskopiointiin liittyen on tärkeä huomioida, että asiakas on loppu viimein aina itse vastuussa datastaan. Esimerkiksi vastoin yleistä luuloa, Microsoft ei varmuuskopioi pilvessään olevaa dataa, ja samaa linjaa noudattavat lähes kaikki muutkin toimijat, mukaan lukien TNNet. Asiakkaan vastuulle jää siis käytännössä aina huolehtia käyttämiensä sovellusten, palvelimien ja työasemien tietoturvasta, varmuuskopioista sekä päivityksistä kaikissa mahdollisissa sijainneissa. TNNet tarjoaa kuitenkin erillisenä lisäpalveluna palvelimien, työasemien ja Microsoftin M365-ympäristöjen varmuuskopiointia.

Datan varmuuskopiointi on ennen kaikkea tietoturvatoimi. Jos varmuuskopioinnit on tehty oikein, on esimerkiksi ransomware-hyökkäyksistä mahdollista toipua jopa täysin ilman datan häviämistä. Varmuuskopiot suojaavat yrityksen dataa myös perinteisiltä tietojen vahinkokatoamisilta, kuten laitevahingoilta ja käyttäjien virheiltä, sekä tiedostojen korruptoitumiselta.

Varmuuskopiointiratkaisua valittaessa kannattaa aina miettiä, millaisia tilanteita varten varmuuskopiointia hankitaan ja miten siitä voidaan kyseisissä tilanteissa hyötyä. Olennaisinta on myös pohtia, miten lähelle tai kauas historiaan pitää pystyä palautumaan (RPO) ja miten pitkään palautustyö saa kestää (RTO). Nämä kaksi asiaa määrittämällä voidaan suunnitella juuri oikean kokoinen liiketoiminnan jatkuvuuden turvaava ratkaisu ilman asiakkaalle koituvia kuluja liian laajaksi mitoitetusta palvelusta.

Varmuuskopiointeja toteuttaessa on ehdottoman tärkeää varmistua siitä, että varmuuskopiointityöt onnistuvat päivittäin. Tärkeää on myös suorittaa säännöllinen testaus, sekä olla selvillä siitä, miten palautus tehdään ja mitä toimia se vaatii asiakkaalta. Ihannetilanteessa jokaisella yrityksellä tulisi olla dokumentoitu toimintamalli tilanteisiin, joissa dataa pitää palauttaa varmuuskopioista. Lisäksi on ehdottoman tärkeää, että edes yksi varmuuskopioista olisi sellainen, mihin ei pääse yrityksen verkosta käsiksi.

## 3-2-1 -sääntö

Varmuuskopioinnin hyvä peruspilari on jo yli 20 vuotta vanha yleisesti tunnettu 3-2-1 -sääntö:

- 3 eri kopiota datasta
- 2 eri mediaa
- 1 offsite-kopio datasta

TNNetin varmuuskopiontipalvelu vakiomuotoisena toteuttaa tätä sääntöä sisältäen kuitenkin poikkeaman datan kopioiden määrässä: kopioita datasta on kaksi kappaletta (tuotantodata ja yksi varmuuskopiointidata). Varmuuskopiointia voidaan kuitenkin kustomoida niin, että mukaan otetaan myös kolmas kopio datasta. Data voi olla TNNetin hallitsemassa ympäristössä, mutta suosittelemme kuitenkin hankkimaan täysin TNNetistä riippumattoman paikan kolmannelle kopiolle. TNNet voi olla tässä mukana auttamassa ja konsultoimassa parasta mahdollista ratkaisua.

# Palvelun sisältö

Varmuuskopiointipalvelu toteutetaan yleisesti Veeamin ratkaisuilla. Joissain tapauksissa voidaan Linux-palvelimia varmuuskopioida myös TNNetin kehittämällä Rsync-skriptalla. Backup-datat sijaitsevat TNNetin ylläpitämässä, jaetussa Veeam-ympäristössä. Huolimatta jaetusta ympäristöstä, ovat asiakkaat kuitenkin eroteltuna toisistaan. Halutessa on myös mahdollista pystyttää oma backup-ympäristö joko Veeamia tai jotakin muuta backup-järjestelmää hyödyntäen.

Varmuuskopiointipalveluun sisältyy mahdollisesti tarvittavat lisenssit, backup-infran laskenta- ja levytilakapasiteetti, sekä vähintään 10G:n verkko backup-palvelimille. Lisäksi palvelussa valvotaan backupien onnistumista automatiikalla Veeamin raportoimaa backup-jobin tilaa hyödyntäen. Mahdollisiin epäonnistuneisiin varmuuskopiointitöihin reagoidaan asiantuntijoidemme toimesta arkipäivisin. Palveluun sisältyy myös ongelmien korjaaminen, mikäli ne eivät ole asiakkaan toimista johtuvia ongelmia.

## Backupien testaus ja palautussuunnitelma

TNNet ei omatoimisesti testaa backupien toimivuutta, vaan se on aina asiakkaan vastuulla. Paras tapa testata backupien toimivuutta on tehdä TNNetille työtilaus backupista palauttamisesta, ja kertoa siinä, mitä halutaan palauttaa ja minne.

Backupien testausta tulisi kuitenkin suorittaa säännöllisesti, ja jokaisella yrityksellä pitäisi olla tehtynä kirjallinen suunnitelma siitä, miten toimia, kun backupista palauttamista tarvitaan. TNNet tarjoaa näihin liittyen konsultaatiota. TNNetin omille backup-asiakkaille sisältyy tunnin kestävä ilmainen konsultaatio palautussuunnitelman tekemiseksi.

## Immutable backup

Veeam varmistuksissa on mahdollista hyödyntää immutable backupeja. Immutable-ominaisuus ei jaetussa backup-ympäristössä itsessään maksa ekstraa, mutta se kuluttaa enemmän levytilaa. Immutable backup tarkoittaa sitä, että backupissa olevaa dataa ei voi poistaa tai muuttaa, ennen kuin se on määriteltyä ajanjaksoa vanhempaa.

## S3-levytila

Backupeja voidaan tallentaa myös S3-yhteensopivaan levytilaan, joka voidaan Veeamilla määritellä immutableksi. S3-levytilaa voidaan tarjota backup-tarkoitukseen myös pelkkänä levytilana, mikäli asiakkaalla itsellään on S3-levytilaa tukeva varmistusjärjestelmä jo käytössä.

## Serverit ja työasemat

Veeamissa yleisimmin hyödynnetään varmistettavalle laitteelle asennettavaa Veeam-agenttia, mutta myös muut Veeamin tukemat varmistusmetodit ovat mahdollisia. Normaalisti agentti lisensoidaan Veeamin Cloud Connect -lisenssillä, joka sisältää käyttöjärjestelmäkohtaisesti kattavat ominaisuudet. Jos käytetään muita varmistusmetodeita, esimerkiksi suoraan VMware hypervisorilta backupaamista, voidaan tarvittavat lisenssitasot katsoa tapauskohtaisesti.

Varmuuskopion säilytysaikaa ja tiheyttä voidaan säätää hyvin joustavasti. Vakiona määritämme backup-datan kierroksi 90 vuorokautta siten, että kerran viikossa otetaan palvelimesta aktiivinen täysvarmistus ja muina päivinä vain muuttuneet datat edellisestä backupista (inkrementaalinen varmistus). Näin backup ketju pysyy viikon mittaisena, eikä siitä tule liian virheherkkää. Vanhin backup-ketju poistetaan vasta, kun määritelty kiertoaika on kulunut, ja sen jälkeen on otettu uusi aktiivinen täysvarmistus.

Asiakkaan on mahdollista tehdä palautustoimet omatoimisesti sellaiselta koneelta, jolle on asennettuna backup agent, tai hypervisorilta, jolla backupeja otetaan. Vaihtoehtoisesti asiakas voi kirjallisella työpyynnöllä tilata TNNetiltä haluamansa palautuksen.

Backup tilasta laskutetaan kuukausittain perusmaksun lisäksi toteutuneen datakulutuksen mukaan. Datakulutuksella tarkoitetaan backupissa sijaitsevaa datan määrää, johon vaikuttaa muun muassa backupien säilytysajan pituus ja varmistettavalla palvelimella tapahtuvan datamuutosten määrä, sekä muut varmistustöiden asetukset. TNNet voi antaa arvion mahdollisesti lopullisesta datamäärästä, mutta toteutuneessa lukemassa on niin paljon muuttujia, että arvio ei ole sitova. Laskutusperuste toteutuneelle datalle on aina käsitellyn datan määrä, eli toisin sanoen Veeamin raportoima datan kulutus.

## M365

Vastoin yleistä käsitystä, Microsoft ei vastaa palvelussaan olevasta datasta, eikä Microsoft varmuuskopioi dataa. M365-palvelussa on olemassa jonkin tasoinen versiohallinta ja lyhyt roskakori poistetulle datalle, mutta nämä eivät itsessään ole varmuuskopioita. Jos data esimerkiksi korruptoituu tai sen katoaminen huomataan liian myöhään, ei data ole enää pelastettavissa ilman erillistä varmuuskopiota. TNNetin M365-backupissa data otetaan talteen pois Microsoftin pilvestä, joka mahdollistaa datan palauttamisen, vaikka Microsoftin palvelut olisivat saavuttamattomissa. Tämä on myös aiemmin mainitun 3-2-1 -periaatteen mukainen tapa ottaa varmuuskopioita.

M365-backupissa voidaan varmuuskopioida organisaation sähköpostin, OneDriven, Teamsin ja SharePointin datat. M365-palvelu lisensoidaan käyttäjäkohtaisesti. Palvelua käyttöönottaessa voidaan määritellä tarkasti, mitkä käyttäjät tai datat halutaan varmuuskopioida. SharePointin tapauksessa tulee kuitenkin huomioida, että kaikki käyttäjät, joilla on pääsy varmuuskopioitavaan dataan, tulee olla lisensoituna. Datan säilytysaika on vuosi, jota voi erillisestä lisämaksusta pidentää.

M365-backupin käyttöönottaminen vaatii TNNetille global admin -tunnukset M365-ympäristöön. Jaetussa backup-palvelussa oleville M365-backupeille ei ole mahdollista suorittaa palautusta asiakkaan toimesta, vaan itsepalveluportaali vaatii asiakaskohtaisen oman ympäristön.

## Salesforce

Salesforce backup poikkeaa palveluna muista tässä palvelukuvauksessa esitellyistä ratkaisuista. Datan ottaminen ja palauttaminen Salesforcesta vaatii Salesforce-osaamista, jota TNNet ei tarjoa. Suosittelemme Salesforcen tapauksessa hyödyntämään Salesforce-kumppania. Salesforcen tapauksessa TNNet ei samasta syystä valvo backupien onnistumista, vaan se on asiakkaan ja/tai varmuuskopiotöiden tekijän vastuulla. Varmuuskopiointitöihin on kuitenkin mahdollista määrittää ilmoitukset lähetettäväksi haluttuihin sähköpostiosoitteisiin. Salesforcessa jokainen asiakasympäristö on omia ympäristöjään, eli muista varmuuskopioinneista poiketen jaettu ympäristö ei ole mahdollinen. Salesforce lisensoidaan käyttäjien mukaan siten, että kaikki aktiiviset salesforce-käyttäjät tulee olla lisensoituna. Lisenssit on ostettava aina vuodeksi kerrallaan, ja niiden minimäärä on 10 käyttäjää. Lisenssit voi hankkia joko itse tai TNNetin kautta.

TNNetin vastuulla Salesforce backupin tapauksessa on tuottaa Salesforce backup -palvelin ja huolehtia siitä, että varmistuspalvelin käynnistyy ja sillä on levytilaa sekä toimiva internetyhteys. Lisäksi TNNet huolehtii itse varmistuspalvelimen tietoturvasta suorittamalla sekä palvelimen että Veeamin päivityksiä.

# Lisätietoja

Lue myös TNNet yleinen palvelukuvaus.

Varmuuskopiointipalvelua liittyy olennaisesti ainakin useisiin TNNetin tuottamiin palveluihin, joten suosittelemme lukemaan myös ainakin seuraavat palvelukuvaukset:

- Openstack virtuaalipalvelimet
- Yksityinen pilvi
- Webhosting