PALVELUKUVAUS - OPENSTACK-VIRTUAALIPALVELIMET

SISÄLLYS

Palvelun sisältö

TNNetin Openstack-virtuaalipalvelin on täysin kotimaisesti tuotettu palveluratkaisu. Virtuaalipalvelimet tuotetaan korkean turvallisuuden laitesaleista, jotka täyttävät viestintäviraston määräyksen 54A/2012M mukaisen korkeimman luokituksen ”Tärkeysluokka 5”.

Palveluratkaisuissa käytetään Intel-palvelinalustoja, ja virtualisointi toteutetaan KVM Hypervisorilla Openstack-ratkaisulla. Ratkaisu mahdollistaa tuoreimmat tekniset toteutukset kustannustehokkaasti. Virtualisoituna voidaan suorittaa mm. Linux-, BSD- ja Windows-käyttöjärjestelmiä.

Virtuaalipalvelimet tarjotaan vakioituina resurssikokonaisuuksina muistin ja ydinten osalta. Vakioidut kokonaisuudet mahdollistavat laskenta- ja IO-resurssien ennakoinnin ja tasa-arvoisen jakamisen palvelussa.

Prosessoreina palvelussa käytetään Intelin Xeon Scalable Gold -sarjan suorittimia. Yksi tarjottu ydin vastaa vähintään hyperthreading corea 2,9 GHz suorittimelta.

Palvelu on tyypiltään ns. pilvipalvelu. Tavoitteena on tuottaa asiakkaan käyttöön runsaasti kapasiteettia kustannustehokkaasti ja toteuttaa vikasietoisuus sekä varmennusratkaisut jakamalla palvelutoteutus riittävän monelle palvelualustalle ja saatavuusalueelle. Yksittäinen tuotantoalusta on varmennettu tyypillisimpiä vikatilanteita vastaan (kahdennettu verkko, virransyöttö ja redundantit levyjärjestelmät). Vikatilanteessa alustan puolella ei ole virtuaalikoneille automaattista viankorjausta (failover) tai muuta palautusautomatiikkaa. Ratkaisu takaa sen, että itse alustan varmennusjärjestelmä ei voi tuottaa yllättäviä ongelmatilanteita ja toimia ristiin virtuaalipalvelimilla toimivien järjestelmien kanssa. Pelkästään pilvipohjaista levykapasiteettia käyttävät palvelimet voidaan vikatilanteessa käynnistää nopeasti uudelleen muilla palvelimilla.

TNNet voi tarvittaessa avustaa asiakasta toteuttamaan tilanteeseen parhaiten sopivan varmennusratkaisun. Palvelimeen on mahdollista pyytää käyttöjärjestelmän lisäksi esiasennettuna myös ohjelmistoja. Lisäasennukset tehdään tuntityönä TNNetin hinnaston mukaisesti tai etukäteen erikseen sovitun hinnan mukaisesti.

Muokattava kokonaisuus

Virtuaalipalvelimet ovat hyvin kustomoitavissa, ja niiden resursseja voidaan muuttaa käynnistyksen jälkeenkin. Virtuaalipalvelimien resursoinnissa on kuitenkin joita rajoitteita, jotka on esitelty tässä kappaleessa.

Rajoitteet

Virtuaalipalvelimeen on liitettävissä muistia ja laskentaytimiä niin, että yhtä ydintä kohden on aina vähintään 4Gt RAM-muistia aina 32 ydintä/128Gt muistia asti. RAM-muistia voi siis olla enemmänkin kuin 4GiB per ydin. Myös suuremmat kokoonpanot ovat erikseen neuvoteltavissa.

Palvelimen käyttöjärjestelmälevy (Windowsissa perinteisesti C:-asema, Linuxissa esim. sda) on uusissa virtuaalipalvelimissa maksimissaan 60 GiB. Että Windows mahtuisi päivityksineen levylle ongelmitta, on myös Windows-servereissä pienin sallittu levykoko käyttöjärjestelmälevylle 40 GiB. Linux-koneita voidaan luoda myös pienemmille levyille. Konsultoimalla TNNetin teknisiä asiantuntijoita on mahdollista saada 60GiB:ä suurempi käyttöjärjestelmälevy, jos sille todetaan olevan hyvä käyttötarkoitus. Suositeltavaa on kuitenkin pitää käyttöjärjestelmälevy ainoastaan käyttöjärjestelmällä ja asentaa kaikki sovellukset ja data erillisille datalevyille.

Asiakkaat eivät voi itse luoda uusia flavoureita (resurssikokonaisuuksia), joissa määritetään käynnistettävän palvelimen resurssit (ytimet, RAM-muisti ja käyttöjärjestelmälevy). Uudet flavourit tulee aina pyytää

TNNetiltä, mutta sen luomisesta ei veloiteta mitään. Luotua flavouria voi kuitenkin uudelleenkäyttää rajattomasti. Lisälevyjä (volume) asiakas voi luoda ja käyttää omatoimisesti haluamallaan tavalla.

Skaalaus

Virtuaalipalvelimen flavouria voi vaihtaa, jos palvelimen resurssitarve muuttuu. RAM-muistia ja ytimien määrää voi sekä kasvattaa että pienentää. Flavourissa määrättyä käyttöjärjestelmäosiota ei voi pienentää, mutta sitä voi kuitenkin kasvattaa. Flavourin muuttaminen pakottaa virtuaalipalvelimelle aina uudelleenkäynnistyksen, joten siitä aiheutuu palvelimelle pieni käyttökatkos.

Datalevyjä, eli volumeita, voi lisätä ja poistaa palvelimeen lennosta. Tällöin tulee huomioia datan korruptoitumisriskit, jos levyllä on kirjoitusoperaatioita käynnissä levyä irrottaessa. Volumeja voi myös kasvattaa ja niiden levytyyppiä voi muuttaa palvelimen ja levyn ollessa käytössä. Levyä kasvattaessa tulee kuitenkin huomioida, että alustajärjestelmä ei automaattisesti kasvata levyosiota virtuaalipalvelimen käyttöjärjestelmätasolla, vaan se on tehtävä erikseen virtuaalipalvelimella.

Volumea ei voi suoraan pienentää, mutta pienennysoperaatio on tehtävissä siten, että palvelimelle liitetään kiinni uusi (pienempi) volume, jolle datat kopioidaan alkuperäiseltä levyltä. Kun datat on kopioitu, voidaan vanha levy poistaa ja käyttöjärjestelmässä ottaa uusi levy sen tilalle käyttöön.

Levytila

Levytila on SSD-pohjaista levytilaa, joka on palvelimeen sidottuna lokaalina levytilana tai pilvipohjaisena kapasiteettina. Oletusluontoisesti käyttölevytila on pilvipohjaista tallennustilaa. Lokaalista levytilasta on sovittava erikseen. Taustalevyinä käytetään nopeita ja laadukkaita Intelin Datacenter SSD-levyjä.

Levytila on varmennettu fyysiseen palvelimeen sidotun levytilan osalta raid1-tasoisella tallennuksella. Pilvikapasiteettina tuotettava levytila on varmennettu siten, että järjestelmä kestää vähintään kahden levyn tai palvelimen vikaantumisen ilman datahäviötä tai tuotantokatkosta.

Levyjärjestelmä on rakennettu CEPHin päällä, eli levy on verkon yli toimivaa levypintaa. Verkon tuoma latenssi voi näkyä palvelimen levyoperaatioissa kirjoitusten suorituskyvyssä, jos siellä pyörivät sovellukset eivät ole suunniteltuja pilvikäyttöön. Verkon yli toimiva levytila on käytännössä aina jonkin verran hitaampaa kuin perinteinen lokaali levytila.

Vaihtoehtoisena levytilana nopeampia levyn kirjoitusoperaatioita varten on myös database-ssd-levytyyppi (Linstor), joka pyrkii vähentämään verkon latenssia sijoittamalla datat samalle alustakoneelle, kuin millä itse virtuaalikone pyörii. Database-ssd on myös hieman vikaherkempää, kuin oletuksena tarjottava CEPH:n päällä toimiva ssd-levytila.

Jos virtuaali vaatii poikkeuksellisen nopeaa levyä, voidaan tapauskohtaisesti neuvotella täysin lokaalin levyn käyttöönotosta. Lokaali levy on kuitenkin pilvilevyjä huomattavasti vikaherkempi ratkaisu, ja sen kanssa suositellaan aina käytettävän vähintään kahdennettuja virtuaalipalvelimia.

Palveluun liittyvät tietoliikenneyhteydet

Virtuaaliratkaisut liitetään Palveluntarjoajan runkoverkkoon aina täysin kahdennetusti. Yksittäiselle virtuaalipalvelimelle kuuluu aina 1000Mbps/1000Mbps-verkkoliityntä ilman liikennerajoitusta yhdellä julkisella IP-osoitteella (IPv4/IPv6). Datan liikuttaminen sisään tai ulos Openstack-järjestelmästä ei maksa mitään. Kaikkiin virtuaaliratkaisuihin on kustomoitavissa asiakkaan haluama verkkoratkaisu esimerkiksi liittäen palvelimet osaksi olemassa olevaa yritysverkkoa tai perustamalla palvelimien eteen uusi palomuuripalvelu.

Openstack varaa itselleen jokaisesta verkosta 5 IP-osoitetta omaan käyttöönsä. Tyypillisesti TNNetin asiantuntijat varaavat verkosta ensimmäiset kymmenen osoitetta, joista ensimmäinen on yhdyskäytävä, seuraavat neljä varauksia tulevaisuuden tarpeisiin ja osoitteet .5 – 9 Openstackin käyttöön. Verkkojen kokoa ei ole kuitenkaan rajattu, joten asiakkaalle jää varmasti tarvittava määrä osoitteita käyttöön.

Openstackissa ei oletuksena voi liikennöidä palvelimelta muulla osoitteella, kuin minkä Openstack on palvelimelle määritellyt. Tämä suoja-asetus on kuitenkin mahdollista määrittää pois päältä asiakkaan omissa verkoissa, mutta TNNetin julkisissa verkoissa se ei ole mahdollista. Käyttötapaus tällaiselle tarpeelle voisi olla esimerkiksi jokin kontitettu palvelu, jonka pitää liikennöidä ulos kontin omalla osoitteella. Yhdellä palvelimella voi myös olla liitettynä useita eri verkkoja ja verkkokortteja, jos haluaa liikennöidä suoraan palvelimien välillä sisäverkon osoitteilla.

Kiinteä julkinen IP-osoite

Palvelimille tulee oletuksena DHCP-alueelta IP-osoite. Osoite pysyy samana niin kauan kuin palvelinta ei poisteta. Palvelimen voi siis sammuttaa siten, että sen IP-osoite ei vaihdu. DHCP-alueelta allokoidulle IP-osoitteelle ei voida kuitenkaan tehdä esimerkiksi rDNS-osoituksia, eikä sitä saa käyttöön, jos palvelin pitää luoda uudestaan. Virtuaalipalvelimen sisällä verkkokorttia ei siis tarvitse asettaa kiinteäksi, vaan se saa aina saman osoitteen DHCP:lta.

Lisäpalveluna on mahdollista allokoida palvelimelle käyttöön kiinteä julkinen IP-osoite, jota voidaan uudelleen käyttää ja siirrellä tarvittaessa eri virtuaalikoneiden välillä. Kiinteälle julkiselle IP-osoitteelle voidaan määritellä myös rDNS-osoitukset.

Palvelimien verkotus

Asiakkaat voivat itse luoda eri verkkoja OpenStackin sisällä ja määritellä miten ne linkittyvät toisiinsa. On siis esimerkiksi mahdollista luoda virtuaalinen palomuuri OpenStackini ja liittää siihen palvelimia sisäverkon (RFC1918) IP-osoituksilla.

Mikäli Openstackin ulkopuolella oleva verkko halutaan liittää palvelimiin, se tulee tehdä TNNetin asiantuntijoiden toimesta. Myös kaikki TNNetin tuottamat palomuuri- ja verkkopalvelut ovat Openstackin ulkopuolisia, eli TNNet ei toteuta muita palveluita Openstackissa vikasietoisuuden vuoksi. Verkkoja voidaan kuitenkin luoda erillisien projektisuunnitelman mukaisesti etukäteen valmiiksi odottamaan käyttöönottoa, jolloin asiakas voi omatoimisesti ottaa niitä käyttöön haluamallaan aikataululla.

S3 Object storage

Openstackista on mahdollista ottaa käyttöön S3-yhteensopivaa levytilaa. S3-levytila suositellaan sijoittamaan eri projektiin kuin missä itse palvelimet sijaitsevat. TNNet luo S3-projektin ja tunnukset asiakkaan pyynnöstä ilman lisäkustannuksia.

Kun S3-projekti luodaan, me toimitamme asiakkaalle tarvittavat Access ja Secret Keyt, jonka jälkeen asiakas voi itse luoda haluamiaan säiliöitä (bucket). Suosittelemme S3-työkaluksi Amazonin tekemää AWS CLI -työkalua.

Tiedostojen polut ovat muotoa *https://s3.vaultstack.fi/tenantuuid:bucketname/tiedosto.txt*

Käytettävät palvelinimaget

Palvelussa on oletuksena TNNetin lisäämiä yleisimmin käytettyjä imageja, kuten esimerkiksi tuetut Windows-, Ubuntu- ja Debian-serverit. Jos listalta ei löydy asiakkaan haluamaa imagea, on palveluun mahdollista lisätä itse haluamansa image, tai pyytää TNNetiä lisäämään haluttu image erillistyönä.

Suosittelemme ehdottomasti muuttamaan imagen RAW-muotoon ennen sen lisäämistä Openstackiin. Myös muut formaatit, kuten QCOW2, toimivat, mutta RAW on nopein käynnistymään. Suosittelemme imagen formaatin vaihtamiseen qemu-img-työkalua.

Cloud-init

TNNetin lisäämille levykuville on asetettuna Cloud-init, joka mahdollistaa erilaisten skriptojen ajamista palvelimen käynnistyksen yhteydessä. Lisäksi palvelimet saavat metatietoja alustalta Cloud-initin kautta. Openstackin hyödyntämä Cloud-init mukailee Amazonin EC2 Cloud-init formaattia.

Tyypillisiä tehtäviä Cloud-initillä palvelimen luonnin yhteydessä ovat esimerkiksi käyttäjätunnusten tai SSH-avaimien lisääminen sekä palvelimen päivitys. Tarvittaessa apua haluttujen Cloud-init skriptojen tekemiseen voi pyytää TNNetiltä.

Ensimmäinen kirjautuminen virtuaalipalvelimelle

TNNetin luomissa Linux-imageissa ei ole oletuksena toimivia käyttäjätunnuksia. Palvelinta luodessa palvelimelle pitää liittää SSH-avainpari, tai luoda käyttäjätunnus Cloud-initiä hyödyntäen. Suositus on käyttää SSH-avainparia, joka on huomattavasti salasanakirjautumista tietoturvallisempi vaihtoehto. Apua SSH-avaimien käyttöön saa pyytäessä TNNetiltä.

Windows Servereissä 2016- ja 2019-versiot pyytävät käynnistymisen jälkeen luomaan salasanan consolesta. Windows Server 2022-versiossa käyttäjätunnus pitää luoda Cloud-initä hyödyntäen palvelinta luodessa.

Tilannekuvat (Snapshot)

Palvelimista ja levyistä on mahdollista ottaa tilannekuva, eli snapshot. Snapshot ei kuitenkaan ole varmuuskopio, vaan se säilytetään samassa järjestelmässä kuin missä itse virtuaalipalvelimet ja niiden datat sijaitsevat.

Palvelimesta otettava tilannekuva ei ota tilannekuvaa palvelimille liitetyistä levyistä, vaan jokaisesta levystä tulee ottaa oma tilannekuvansa. Palvelimen snapshot -toiminto ottaa tilannekuvan ainoastaan palvelimen boottilevystä.

Tietoturva

Palvelu perusmuotoisenaan ei sisällä mitään rajoitteita, eli internetliittymä on täysin avoin internetin suuntaan. Palveluntarjoajalla on oikeus puuttua mahdollisiin väärinkäytöksiin sekä rajoittaa yhteyttä viranomaismääräysten mukaisesti.

Varmuuskopiointi

Virtuaalipalvelimia ei varmuuskopioida palveluntarjoajan toimesta. Asiakkaan on itse huolehdittava halutun datan varmuuskopioinnista. Varmuuskopioinnin voi toteuttaa itse haluamallaan tavalla, tai hyödyntää palveluntarjoajan tarjoamaa varmuuskopiointipalvelua (kts. Varmuuskopiointi-palvelukuvaus).

Päivitykset

TNNet huolehtii virtualisointialustan ja tietoliikennelaitteiden päivityksistä. Asiakkaan vastuulla on huolehtia virtuaalipalvelimien käyttöjärjestelmän ja käytettävien sovellusten päivityksistä. Palveluntarjoajalla on lisäpalveluna myös eri tasoisia päivityspalveluita (kts. Päivityspalvelut-palvelukuvaus).

Datan salaus

Palvelussa olevaa dataa ei salata TNNetin toimesta. Jos data halutaan salata, voi asiakas itse käyttää haluamaansa salausmetodia käyttöjärjestelmätasolla. Levyjärjestelmän suunnitteluperiaatteiden takia data on kuitenkin erasure-koodattua, jolloin yksittäiseltä kovalevyltä on käytännössä mahdotonta saada dataa ulos luettavassa muodossa.

Palomuuraus

Openstack hallintaliittymässä on mahdollista tehdä tietoliikenneportti tai virtuaalikonekohtaisia security groupeja. Security groupit ovat käytännössä tilallisia access-listoja, eli niissä ei ole mitään edistyneitä palomuuriominaisuuksia. Jos palvelimet halutaan keskitetyn palomuurin piiriin, tai halutaan hyödyntää moderneja NGFW-ominaisuuksia, voi palvelimiin liittää joko oman palomuurin tai TNNetin palomuuripalvelun.

Oletuksena TNNetin luomat asiakasvirtuaalit ovat aina kaiken sallivalla security groupilla, sillä emme voi tietää mistä ja mitä portteja palvelimelle tulee avata. Asiakkaan vastuulla on huolehtia palvelimen palomuuraus joko erillisellä lisäpalvelulla tai omalla palomuurauksella tietoturvan takaamiseksi.

Antivirus, XDR ja MDR

Palvelimia ei skannata virusten varalta alustan kautta. TNNet tuottaa erillisenä lisäpalveluna XDR- ja MDR-palveluita palvelimille (Tietoturvapalvelut).

Tietoturvaskannaukset / verkkoskannaukset

TNNet skannaa omaa verkkoaan, mukaan lukien palvelinverkot, ja puuttuu vakaviin haavoittuvuuksin. Skannit suoritetaan siten, että niistä ei koidu asiakaskoneille käyttökatkoksia tai muuta haittaa. Skannit löytävät vain tunnettuja haavoittuvuuksia, eikä niissä yritetä esimerkiksi murtaa salasanoja.

Lisäpalveluna on saatavilla myös tarkempia skannauksia säännöllisin väliajoin.

Lisenssit

Käytettäessä Microsoftin käyttöjärjestelmiä on palveluntarjoajalla sopimus SPLA-lisenssointimallista (Service Provider License Agreement), jolloin asiakas voi hankkia lisenssit osana palvelua kuukausimaksulla. Ympäristössä ei voi käyttää oletusarvoisesti omia Microsoft lisenssejä, vaan ne on sovittava aina yhdessä palveluntarjoajan kanssa. Open source -ratkaisut ovat käytettävissä ilman lisäkuluja.

Hallintakäyttöliittymä

Hallintakäyttöliittymä tarjotaan Openstack-työkalulla. Hallintaliittymä mahdollistaa etäkonsolin ja virtuaalikoneen tilan hallinnan sekä yleisimmät ylläpitotoimet. Graafisen käyttöliittymän lisäksi hallintaa on mahdollista tehdä API-rajapinnan läpi.

Hallintakäyttöliittymä on avoinna internetiin (julkinen pilvipalvelu), eikä sitä ole mahdollista rajata mihinkään IP-alueeseen. Hallintatunnukset on mahdollista suojata myös OTP-tyyppisellä MFA:lla. MFA:n kytkeminen päälle ei ole mahdollista asiakkaan toimesta itsenäisesti, mutta TNNetin asiantuntijat voivat tehdä sen erillisestä pyynnöstä ilman lisäkustannuksia. Suosittelemme joka tapauksessa pitämään käyttäjien lukumäärän mahdollisimman vähäisenä, sekä huolehtimaan siitä, että salasanat ovat aidosti pitkiä ja hyviä, eikä niitä käytetä missään muissa palveluissa.

TNNet ei oletuksena luo hallintakäyttöliittymään lainkaan tunnuksia, vaan ne tulee pyytää erikseen. Näin asiakkaan projektiin ei ole käyttämättömiä tunnuksia, joiden salasanojen laaduista kukaan ei huolehdi.

Vaihtoehtoinen tapa saada hallinta omiin projekteihin on sovellustunnuksilla (API-key). TNNet voi luoda asiakkaalle API-avaimen, jolloin perinteistä tunnusta ei tarvita ollenkaan. API-avain on mahdollista asettaa vanhenemaan halutussa ajassa.

Virtuaalipalvelimen resurssien monitorointi

Opentackista ei ole mahdollista nähdä virtuaalipalvelimelle allokoitujen resurssien käyttöastetta, sillä Openstack ei asenna mitään agenttia palvelimille. Resurssien käyttöä on kuitenkin mahdollista valvoa erillisellä lisäpalvelulla. Lisäpalveluissa resurssien käyttöasteesta on mahdollista saada myös hälytyksiä joko tekstiviestillä tai sähköpostilla haluttuihin osoitteisiin.

Palvelutaso

Virtuaalipalvelimiin on mahdollista liittää palvelutasosopimus lisäpalveluna. Valvontaan oikeuttavaan palvelutasosopimuksessa palvelin liitetään palvelinvalvontaan, jolloin käyttöjärjestelmän perustilaa seurataan palveluaikana ja mahdollisiin ongelmatilanteisiin reagoidaan välittömästi. Normaalipalvelutasoissa palveluntarjoaja takaa, että virtuaalipalvelin käynnistyy palvelutason puitteissa tavoitettavaan tilaan [1]. Plus-palvelutasoissa palveluntarjoaja sitoutuu toimittamaan konsulttiapua palvelutason puitteissa myös asiakkaan palvelimen käyttöjärjestelmän tai ohjelmistokonfiguraation osalta [2]. Palvelutasojen ominaisuudet ovat kuvattuna tarkemmin alla olevassa taulukossa.

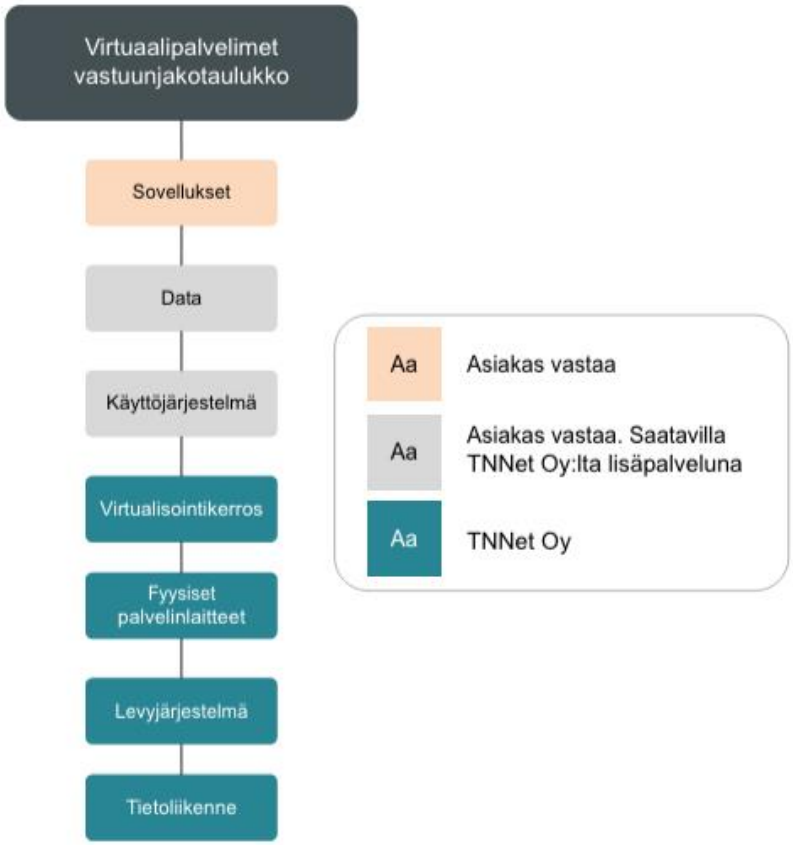
SLA	Viankorjauksen taso	Valvonta	Palveluaika [SH]
Perus	Korjataan tuntityönä hinnaston mukaisesti	-	Ma-Pe 09.00 - 16.00 (Ei arkipyhinä)
Pronssi	Virtuaalipalvelin toiminnassa hintaan sisältyen	Yksi mittauspiste	Ma-Pe 09.00 - 16.00 (Ei arkipyhinä)
Pronssi Plus	Virtuaalipalvelin toiminnassa hintaan sisältyen + konsultointi 0,5h per case, max 1 case/kk	Yksimittauspiste	Ma-Pe 09.00 - 16.00 (Ei arkipyhinä)
Hopea	Virtuaalipalvelin toiminnassa hintaan sisältyen	Max 3 mittauspistettä	Ma-Pe 08.00 - 18.00 (Ei arkipyhinä)
Hopea Plus	Virtuaalipalvelin toiminnassa hintaan sisältyen + konsultointi 1h per case, max 2 casea/kk	Max 3 mittauspistettä	Ma-Pe 08.00 - 18.00 (Ei arkipyhinä)
Kulta	Virtuaalipalvelin toiminnassa hintaan sisältyen	Max 6 mittauspistettä	24/7/365
Kulta Plus	Virtuaalipalvelin toiminnassa hintaan sisältyen + konsultointi 1h per case, max 3 casea/kk	Max 6 mittauspistettä	24/7/365

[1] Asiakkaan omista toimista johtuvien ongelmien aiheuttamaa häiriötä ei katsota epäkäytettävyysajaksi eikä korjaus sisälly palvelun hintaan.

[2] Konsultointiapu aloitetaan palvelutason puitteissa, mutta työn kestoa ei katsota epäkäytettävyysajaksi mukaan kuuluvan työn ylittävä aika tuntityönä asiakkaan hyväksynnällä.

Jaettu vastuu

Ilman lisäpalveluita palveluntarjoajan vastuulla on huolehtia tietoliikenneverkon, levytilan ja virtualisointialustan sekä virtualisointikerroksen toimivuudesta: Jos virtuaalikone käynnistyy sille asetetulta levyltä ja virtuaalikoneella on mahdollisuus liikennöidä internetiin, edellä olevat vastuualueet toimivat. Vastuu sisältää toimivuuden lisäksi myös datan eheyden ja järjestelmien päivitysten ajantasaisuuden. Osaan asiakkaan vastuulla oleviin asioihin on tarjolla myös lisäpalveluita, joista sovitaan aina erikseen. Alla olevassa kuviossa vielä havainnollistettuna, miten vastuut jakautuvat.



Lisätietoja

Lue myös TNNet yleinen palvelukuvaus.

Lisäpalveluista löytyy lisätietoja ainakin seuraavista palvelukuvauksista:

- Varmuuskopiointi
- Päivityspalvelu
- SLA
- Tietoturvapalvelut

- Pfsense-Palomuuri
- Palomuuripalvelu Sophos (SD-WAN)
- Valvonta ja monitorointi