Learning diary and answers

Student name: Eliel Selmgren

Email address (prefer your @students.oamk.fi email if you have such address): t0seel00@students.oamk.fi

Save the final version of this document as PDF and submit it for peer reviews via Moodle's workshop tool before the deadline. Last course week is for peer reviews.

Week 1

Question 1: Describe with short examples: SaaS, PaaS and Iaas

Answer 1:

XaaS on uusimpia pilvipalvelumalleja ja sillä tarkoitetaan kirjaimellisesti mitä tahansa. XaaS voi siis sisältää sovellukset (SaaS), infrasturkuutin (Iaas) ja/tai sovellusalustan (PaaS)

SaaS (Software as a Service)

- Yksi kolmesta pilvipalvelun tärkeästä palvelumallista (PaaS ja Iaas ovat kaksi muuta). Näistä kolmesta SaaS on eniten käytetty. SaaS on pilvessä oleva ohjelmisto ja se tarjoaa ohjelmistoja ja sovelluksia (tai näiden yhdistelmiä), yleensä verkkoselaimella ja maksu on vuokraus periaatteella. Perinteisessä ohjelmistomallissa maksetaan etukäteen kustannus sekä mahdollinen tukipalvelun maksu. Tavallisimmin SaaS:n hinnoittelu on kiinteällä kuukausimaksulla. SaaS-palvelusta voidaan maksaa myös esimerkiksi henkilömäärän mukaan. SaaS:ia ylläpitää palveluntarjoaja joka myös omistaa vuokrattavan ohjelmiston. Palveluntarjoaja myös vastaa tietoturvasta ja hallitsee ohjelmistoa.
- SaaS-palveluista on saatavilla erilaisilla tuotevariaatioilla eri käyttötarpeiden mukaan vaikkakin sama tuotantoympäristo palvelee useampaa asiakasta. Useimmiten erilaisten tuotevariaatioiden määrä on 2-4.
- SaaS-palvelun asiakkaan ei siis itse tarvitse fyysisen cd-levyn kautta erikseen asentaa ohjelmistoa ja maksaa siitä lisenssimaksuja sekä huolehtia ohjelmiston päivittämisestä ja tietoturvasta.
- Esimerkkejä SaaS palvelusta ovat: Office 365, Google Apps collection, SAP ja Dropbox.

Paas (Platform as a Service)

- PaaS on palvelualustan ulkoistaminen (yleensä) pilvipalveluna. PaaS alustaa voi laajentaa tarpeen mukaan eli kehittäjien ei tarvitse huolehtia ohjelmiston skaalautuvuudesta eikä käyttäjämäärien kasvusta johtuvasta tehotarpeesta. Näitä sovellusalustoja usein ohjelmistokehityksen tarpeisiin. Web käyttöliittymän lisäksi PaaS-palvelu tarjoaa vaihtoehtoisia tapoja yhteyden muodostamiseen palveluihin esimerkiksi suorat yhteydet palvelimiin (FTP/SFTP, SSH), komentorivityökalut (CLI) ja API-rajapinta. API:n avulla toimenpiteitä voidaan automatisoida. Yhtenä erona SaaS:iin on siis se, että asiakkaan vastuulle jää sovelluksen tietoturva sekä julkaisujärjestelmään liittyvät päivitykset. PaaS-palvelussakin maksaminen on joustavaa perustuen käyttöön ja asiakas siirtää sovelluksensa palveluun. Esimerkiksi pilveen perustetussa tietokannassa data on käyttäjän vastuulla, mutta palvelun ylläpito kuuluu PaaS -palveluntarjoalle.
- Esimerkkejä PaaS palveluista ovat: Amazon Web Services, Google App Engine ja Heroku

IaaS (Infrastucture as a service)

- IaaS on infrastruktuuri palveluna. Eli siinä ulkoistetaan palvelimet ja palvelinsalit. IaaS -palvelu antaa asiakkaalle infrastruktuurin eli mm. reitittimet, kovalevyt, palvelimet ja niiden ylläpito. IaaS on siis sopiva sellaisille asiakkaille joilla ei ole varaa ostaa omia laitteita, mutta haluavat kehittää itse oman ohjelmiston. Myös asiakkaat joilla on oma IT -osasto usein käyttävät IaaS -palveluita, koska he itse vastaavat tietoturvasta, asennuksista ja ohjelmista. IaaS:in kaksi päätehtävää ovat siis tallennustilan ja laskentatehon tarjoaminen.
- Esimerkkejä IaaS -palveluista ovat: Microsoft Azure, Google Compute Engine ja IBM SmartCloud Enterprise.

Näistä kolmesta palvelusta (SaaS, PaaS ja IaaS) asiakkaan vastuulle eniten jää IaaS:ssa (Sovellukset, käyttäjärjestelmät, tietokannat ja tietoturva), PaaS:ssa asiakkaan vastuulle jää sovellukset ja SaaS saat niin sanotusti palveluna “koko paketin”.

Question 2: Describe with short examples: Private cloud, public cloud and hybrid cloud

Answer 2:

Private cloud

- Yksityinen pilvipalvelu on tarkoitettu ainoastaan yhdelle organisaatiolle tai yritykselle ja se sijaitsee yksityisessä verkossa. Yksityinen pilvi tarjoaa mahdollisuuden sisällön ja suorituskyvyn mukauttamiseen yksilöllisesti asiakkaan tarpeiden mukaan. Usein esimerkiksi julkisen sektorin toimijat, rahoitusalan yritykset ja suuret tai keskisuuret yritykset käyttävät yksityistä pilvipalvelua. Palvelun asiakas voi päättää, että ylläpitääkö pilvipalvelua itse vai ulkoistetaanko se jollekin toiselle toimijalle. Yksityinen pilvipalvelu tarjoaa korkean tietoturvan sekä häiriötöntä ja muusta verkkoliikenteestä riippumatonta tiedonsiirtonopeutta. Monien ohjelmistojen ja sovellusten käyttöehdot vaativat palveluiden suorittamisen jaetuista palveluympäristöistä erotettuna, tällöin yksityinen pilvipalvelu jää ainoaksi vaihtoehdoksi.

Public cloud

- Julkinen pilvipalvelussa palvelut ovat saavutettavissa Internetin yli ja näiden omistaja ja hallinnoija on aina pilvipalveluiden tuottaja. Julkisen pilvipalvelun voi hankkia käyttöönsä kuka tahansa. Esimerkkejä julkisen pilven alustoista ovat: Microsoft Azure, Google Cloud Platform ja Amazon Web Services (nämä ovat myös ne suurimmat julkisen pilvipalvelun tarjoajat). Julkiseen pilvipalvelun asiakkaiksi päätyvät usein sellaiset joiden täytyy testata ja kehittää ohjelmistokoodia tai sellaiset joilla on tarvetta lisätä prosessiin suorituskykyä kuormitushuippujen takia. Julkisen pilvipalvelun hyviä puolia ovat myös sen automaattinen skaalautuminen tarpeen mukaan ja se on kustannustehokas.

Hybrid cloud

- Hybridi pilvipalvelussa käytetään sekä julkista, että yksityisstä pilveä siten, että kumpikin säilyvät erillisinä. Esimerkiksi liiketoiminnan data on yksityisessä pilvessä, mutta analytiikikaan ja raportointiin käytetään julkisen pilven resursseja. Toinen esimerkki hybridi pilvipalvelun käytöstä on, kun halutaan tehdä raskasta laskentaa ja käyttää tietokantoja mahdollisimman kustannsutehokkaasti yksityisestä pilvestä, mutta palvelua tarjoillaan selaimen kautta ympäri maailmaa hyödyntäen julkista pilveä.

Question 3: Describe usual cloud service related privacy and security issues, worries and challenges

Answer 3: Pilvipalveluiden yksityisyys ja turvallisuus

- Ongelmat
  - Kyberturvallisuuden suhteen datakeskukset voivat tarjota suurempaa turvaa, mutta tietosuojan suhteen pilvipalvelut voivat olla ongelmallisia. Syynä on se, että kun arkaluonteinen tieto siirtyy pilveen, organisaatio menettää osan heidän kontrollistaan tietooon, sillä pilvi on ulkopuolinen ympäristö jota ylläpitää kolmas osapuoli. Huolimatta siitä onko pilvipalvelu IaaS, PaaS tai SaaS, asiakkaalle jää vastuu heidän tiedon ja käyttäjien pääsyn turvaamisesta.
  - Ongelmana pilvipalveluissa on myös se, että tietopalvelimien paikka määrittää sen, että mikä tietosuojalaki pätee arkaluonteiseen tietoon. Se voi myös tarkoittaa, että tietopalvelimien täytyy noudattaa sen maan tietosuojalakia missä ne sijaitsevat, mutta nämä lait eivät välttämättä päde niin maihin joista data on alkujaan lähtöisin. Riippuen laista, yritykset saattavat tarvita erilisen suostumuksen rekisteröityneeltä keräysmään ulkopuolelle.
  - Yhtenä esimerkkinä on, kun Amazonin Yhdysvaltojen itärannikon datakeskukseen tuli sähkökatkos ja myös varageneraattoreihin tuli vikaa. Lopputuloksena osa asiakkaiden datasta katosi ja sitä ei saatu enää takaisin. Eli pilvipalveluun tallentaminen ei tarkoita, että tietoja ei tarvitse varmuuskopioida muualle.
- Huolet
  - Suurimpina pilviopalveluiden turvallisuushuolina tutkimuslaitos Forrester listasi
    - Turvallisuus ja yksityisyys
    - Asetusten ja standardien mukaisuus
    - Lakeihin ja sopimuksiin liittyvät seikat.
  - Julkisissa pilvissä yksityisyys ja turvallisuus on suurin huoli, sillä tuolloin tiedot ja sovellukset ovat hajautettu ympärio maailmaa ja useampi yritys/henkilö käyttää samoja palveluja.
  - Yksityisen pilven huolia ovat taas esimerkiksi ulkopuolisen pilvipalvelun tarjoajan henkilökunnan pääsy tietoihin, varautuminen odottamattomiin ongelmiin ja varmuus palvelun toiminnan jatkuvuudesta.
- Haasteet
  - Esimerkiksi EU:n yleisellä tietosuoja-asetuksella (GDPR) tai Kalifornian yksityisyyden suojaa koskevalla laillla (CCPA) on ekstraterritoriaalisuus lausekkeet. Tämä tarkoittaa, että asetus/laki pätee huolimatta siitä, missä yritys tai palveluntuottaja sijaitsee. Eli jos yritys kerää henkilökohtaisia tietoja EU:n tai Kaliforniaan rekisteröityneeltä, datan turvatoimien täytyy noudattaa GDPR:ää tai CCPA:ta. Tämä tuottaa omia haasteita palvelun tuottajille.
  - Auditoitavuus tuo myös haasteita, sillä pienellä toimijalla ei ole resursseja auditoida pilvipalvelun tarjoajaa. Heidän on siis luotettava dokumemtaatioonsa tai jo aikaisemmin tehtyihin auditointeihin.
  - Kiteytettynä tiedon sijainti, saatavuus ja tietoturvan sekä tietosujan tason auditoiminen aiheuttavat erityisiä haasteita pilvipalvujen käyttöön

Queston 4: What is “shadow IT” and why it is causing significant troubles for many organisations and enterprises? Especially cloud shadow IT. Use examples

Answer 4: Tarkoittaa IT-hankkeita joita käsitellään yrityksen IT-osaston ulkopuolella tai ilman, että IT-osasto tietää niistä. Tämä syntyy silloin, kun liiketoiminnalla on tarve, johon yrityksen IT:ltä ei löydy ratkaisua tai ratkaisun saaminen omalta IT-organisaatiolta on tehty hankalaksi. Tämä aiheuttaa tiedon hajautumiseen ja teknologia-alustojen määrän kasvuun.

Esimerkiksi työntekijä käyttää pilvipalvelua vapaa-ajallaan tiedostojen siirtoon ja tallentamimseen ja ottaa sen omin pain käyttöönsä työpaikalla. Tai työntekijä katselee työtietokoneelta jotakin ohjelmaa ja vahingossa asentaa työkoneelle haitallisen lisäosan. Tässä kaksi esimerkkiä varjo IT:stä ja tätä syntyy silloin, kun työntekijät tekevät päätöksiä ilman, että IT-puoli tietää näistä. Nämä esimerkit ovat sellaisia, missä työntekijä ei ole tiennyt toimintansa seuraamuksista. Varjo IT:n voi myös tietoisesti hyväksyä, jolloin se on riskinotta, mutta tällöin se yleensä tapahtuu yrityksen IT -puolelta ja heillä asemansa puolesta pitäisi olla käsitys siitä, mitä he ovat tekemässä ja millaisia riskejä he ottavat, kun hyväksyvät ns. villit sovellukset.

Jos yrityksessä annetaan jokaisen yksikön vapaasti toimia pilviympäristössä, yritykseen muodostuu siiloja, jotka eivät tiedä toistensa tekemisistä. Tietorakenteet ja perustiedot eriytyvät yksiköiden välillä, vaikka tarvittaisiin yhteinen näkemys yritystason perustiedoista. Ongelma on myös se, että järjestelmien ja niissä olevan tiedon omistajuus voi hämärtyä. Käytännössä tietojen omistaja on se joka hankkii uuden järjestelmän, ottaa sen käyttöön ja käyttää sitä. IT:n hallinnan piiriin kuulumattomien sovellusten osalta voidaan päätyä tilanteeseen, ettei oikeastaan kukaan vastaa mistään. Yrityksissä kuitenkin täytyisi pystyä varmistanaa, että yksiköiden asiantuntijat tai jokin muu taho tekee tarvittavat tietoturvapäivitykset yrityksen pilviympäristöön tuotuihin sovelluksiin.

Mitä enemmän varjo-IT:tä syntyy, sitä enemmän syntyy dataa eri paikkoihin. Tästä syntyy useita haittoja, **tietoturvan huolehtiminen** vaikeutuu tiedon levitessä ja **tietoa myös hukkuu**. Työntekijät erilaisissa rooleissa toimivat osittaisen tiedon varassa ja tämä **heikentää tehokkuutta** sekä vaikeuttaa työn tekemistä.

Week 2

Question 1: Describe what is serverless architecture?

Answer 1: Palveliton arkkitehtuuri mahdollistaa todellisen muutoksen työpanoksen kohdentamiseen digitaalisten palveluiden rakentamisessa. Palvelittomassa mallissa keskitytään liiketoiminan lisäarvoa tuottavien osien rakentamiseen, ei alla olevan infrastuktuurin rakentamiseen tai ylläpitoon. Palveliton arkkitehtuuri ei siis tarkoita etteikö oikeasti jossakin palvelinsalissa olisi palvelimia, vaan että nämä palvelimet eivät ole tietyn organisaation, esimerkiksi yrityksen vastuulla. Näiden palvelinten tietoturvasta, ympäristöstä, verkotuksesta ja toiminnasta on vastuussa palveluiden tarjoaja, kuten Amazon Web Services, Google Cloud Platform tai Microsoft Azure.

Palvelittoman arkkitehtuurin palveluiden ideana on siis vastuun siirto ympäristöstä ja siihen liittyvistä asioista palveluntarjoajalle. Asiakkaan vastuulle jää liiketoiminnan rakentaminen näiden palveluiden päälle. Palvelun hinta perustuu usein käytön perusteella maksettua palvelinkapasiteettia pilvipalvelussa.

Palvelittomassa arkkitehtuurissa palveluntarjoaja hoitaa liikenteen jakamisen vapaille palvelimille, joen kehittäjän ei tarvitse siitä huolehtia. Kehittäjät voivat rakentaa ja ajaa palveluita ilman, että heidän tarvitsee hallinnoida taustalla olevaa infrasturkuuria. Kehittäjien kirjoittaessa ja ajaessaan koodia, pilvipalveluiden tarjoaja huolehtii palvelimien toimivuudesta sovellusten, tietokantojen ja tallennusjärjestelmien käyttämiseksi missä tahansa mittakaavassa.

Function as a Service (FaaS) on palvelittoman tietojenkäsittelyn pilvipalvelumuoto ja tämä on yksi suosituin palvelittoman arkkitehtuurin muoto. FaaS:ssa kehittäjät kirjoitavat heidän sovelluksen ohjelmaa erillisinä funktioina. Jokainen funktio suorittaa tarkkaa toimintoa, kunnes tälle toiminnolle tulee tarve, esimerkiksi saapuva sähköposti tai HTTP -pyyntö. Testausvaiheen jälkeen kehittäjät ottavat käyttöön funktionsa pilvipalvelun tarjoajan palvelussa. Kun funktiota kutsutaan, pilvipalvelun tarjoaja joko suorittaa function käynnissä olevalla palvelimella tai, jos palvelin ei ole käynnissä, uusi palvelin otetaan käyttöön, jotta toiminta voidaan suorittaa. Kehittäjiltä jää näin siis yksi vaihe prosessissa kokonaan pois.

Question 2: Compare application containers to microservices

Answer 2: Sovelluskontit ja mikropalvelut voivat toimia joko yksinään tai yhdessä.

Sovelluskonttien suurin etu on siinä, että niiden rakenne on erilainen, sillä kaikki on rakennettu omiin säiliöihinsä ja kaikki tarvittavat resurssit on niputettu funktioihin. Kehityksen yksinkertaisuuden kannalta tämä on suuri etu, sillä käyttäjän tarvitsee huolehtia vain itse säiliöstä.

Kolikon toisena puolena on, että yllämainittu aiheuttaa tehottomuutta. Useat konttijärjestelmät tarkoittavat päälekkäisiä resursseja ja toimintoja sekä joissakin tapauksissa täysin päälekkäisiä palveluita. Tämä tarkoittaa, että resursseihin verrattuna saa paljon vähemmän laajennettavuutta ja joustavuutta vaikkakin kehitysmallien kautta laajentavuutta ja joustavuutta voidaan hieman saada hankittua lisää.

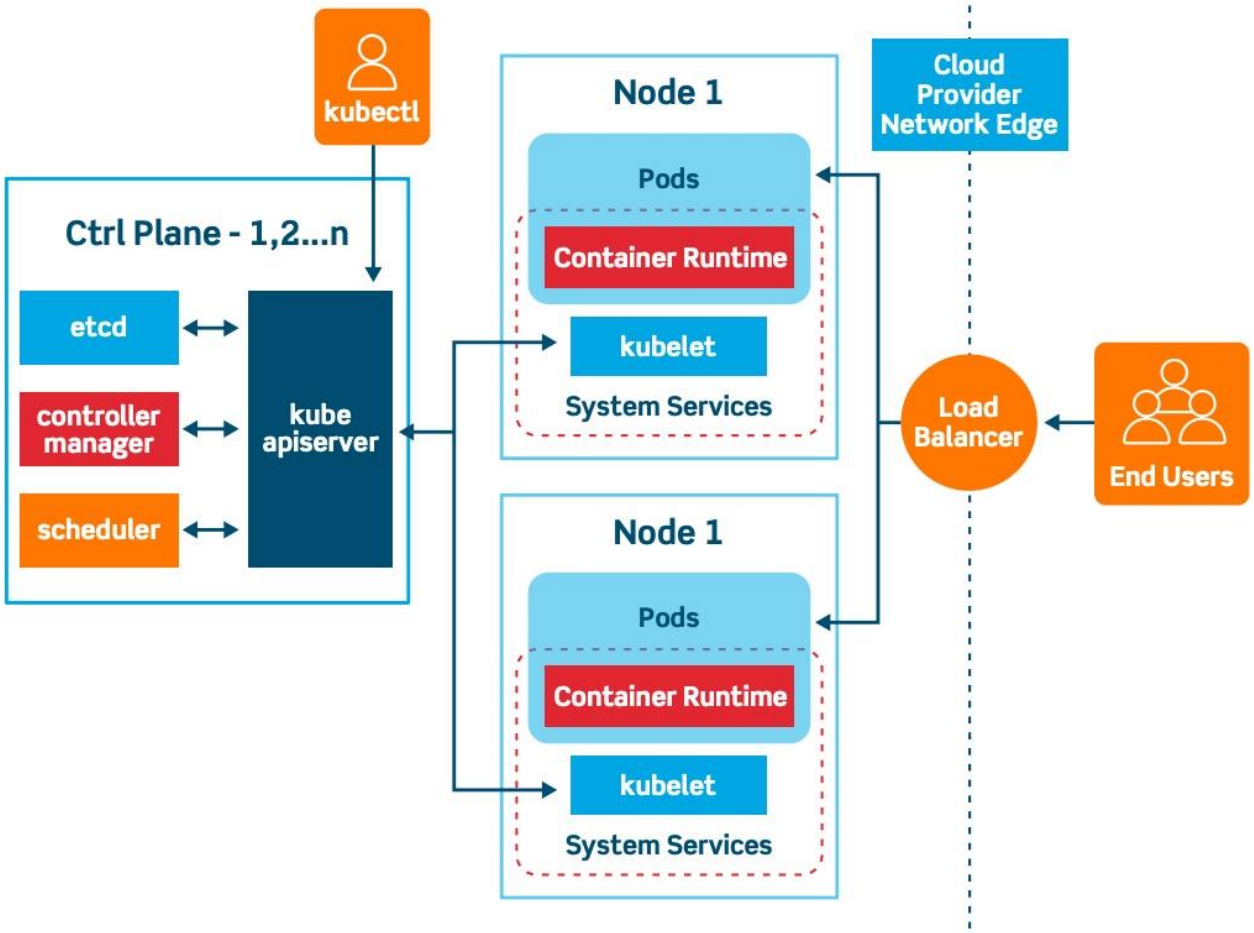
Mikropalvelut tarjoavat laajennattavia ja skaalautuvia ratkaisuja, sillä jokainen palvelu voi liikkua helposti eri segmenttien ja alustojen välillä. Tämä tarkoittaa, että mikropalvelut voivat olla kevyitä verrattuna muihin ratkaisuihin, sillä jokainen uusi mikropalvelu on osa suurempaa massaa verrattuna siihen, että mikropalvelu vaatisi uuden kokonaisuuden luomista resursseillaan.

Mikropalveluiden huono puoli on se, että niistä voi tulla hyvinkin monimutkaisia. Tämä johtuu siitä, että jokainen mikropalvelu on olennaisesti osa suurempaa palveluekosysteemiä. Jokainen yksittäinen mikropalvelu on rakennettava ja suunniteltava monimutkaisen kontekstuaalisen järjestelmän sisällä.

Question 3: Describe shortly what is Kubernetes and what alternatives are there?

Answer 3: Kubernetes on avoimeen koodiin perustuva järjestelmä, jota tarvitaan konttien ajamiseen ja hallintaan palvelunklusterin päällä. Kluberneteksen avulla voidaan käynnistää sovelluksen tarvitsema ryhmä kontteja ja päättää millä palvelimilla kontit käynnistetään. Kubernetiksella voidaan myös käynnistää sovelluksen tarvitsema ryhmä kontteja ja päättää millä palvelimilla kontit käynnistetään. Sillä voidaan myös seurata, toimiiko nämä kontit halutusti. Kubernetes muodostaa konesalin palvelimista yhden suuren laskentaresurssin, jonka käyttöä se optimoi ja automatisoi ilman, että ihmisen tarvitsee tehdä päätöksiä siitä, minkä palvelien päällä kontteja ajetaan.

Kubernites on tärkeimpiä työkaluja, mitä modernissa pilviympäristössä tarvitaan.



Question 4: List some information security risks when using third party (for example Docker) containers?

Answer 4: Kontin ympäristömuuttujat ovat helposti luettavissa, jos hyökkääjä pääsee konttiin sisälle. Tämän vuoksi täytyy olla tarkka mitä ympäristömuuttujiin tallentaa, esimerkiksi henkilötunnusten tai luottokorttitietojen tallentamien ympäristömuuttujiin ei ole järkevää.

Jos kontille ei ole määritelty käyttäjätunnusta, sen oletuskäyttäjätunnus on root. Hyökkääjän päästessä kontin läpi palvelimelle, hän saa myös palvelimella root -käyttäjän oikeudet. Tämän seurauksena hyökkääjä voi ajaa palvelimella mitä tahansa komentoja.

Verifoimaton paketti, joka on ladattu konttiin, voi vaarantaa suuresti kontin tietoturvaa ja tämän kautta antaa hyökkääjälle pääsyn kontin sisään.

Jos kontin juurta ei ole asetettu “vain luku” -tilaan, hyökkääjä voi kirjoittaa konttiin päästyään jotakin sellaista millä hän voi tehdä haitallisia toimenpiteitä.

Jos konttiin lataa muita kontteja eikä käytä tarkkaa versionumeroa, välimuistin takia uusinta versiota ei ladata vaan käytetään edelleen vanhaa versiota. Vanhassa versiossa voi olla tietoturva-aukkoja.

Jos konttiin ei ole asetettu muisti- ja pid-limit –rajoitusta, hyökkääjä voi tehdä DOS-hyökkäyksen palvelimelle kaapaten palvelimen muistin tai prosessorin tehon kokokaan, näännyttää palvelimen muut kontit ja lopulta kaataa koko palvelin

Jos konttien välistä verkkoliikennettä ei ole estetty, hyökkääjän murtautuessa yhteen konttiin, hän pääsee ottamaan yhteyttä myös muihin palveluihin.

Week 3

Question 1: Describe reasons why so many (most?) companies are using cloud based email and calendar services?

Answer 1: Pilvipohjaista sähköpostia käytettäessä sähköpostiin pääsee käsiksi millä tahansa laitteella, joka pääsee verkkoon. Käytettävyys on siis helppoa ja nopeaa, kun käyttää pilvipohjaista palvelua. Kustannussäästöjä myös tulee pilvipohjaisen palvelun kanssa. Yrityksen ei itse tarvitse huolehtia palvelimen kustannuksista, ei tarvitse ostaa käyttöjärjestelmää, sähköpostialustaa ja palvelintelinettä. Tämän lisäksi sähkö, jäähdytys ja ylläpitohenkilöstöstä tulee lisäkustannuksia. Pilvipalvelun kautta tulee myös tietoturva ns. kaupan päälle eikä yrityksen tarvitse itse käyttää siihen ylimääräisiä resursseja, sillä palveluntarjoaja huolehtii päivityksisätä ja tietoturvasta. Pilvipohjaisen palvelun kautta myös sähköpostin skaalautuvuus hoituu helposti ja yrityksen ei tarvitse itse miettiä oman datakeskuksen skaalautuvuudesta vaan vastuu on palveluntarjoajalla. Myös virusten kannalta pilvipohjainen palvelu on järkevää, sillä silloin menetettyjen tiedostojen palauttaminen on helpompaa ja todennäköisempää, koska pilvipohjaisessa sähköpostialustassa vikasietoituus on sisäänrakennettua. Pilvipohjaisessa sähköpostipalvelussa ongelmatilanteen ratkaisu on myös tehokkaampaa, sillä palveluntarjoajan tuki ongelmatilanteissa kykenee resurssiensa puolesta auttamaan tehokkaasti ongelman kanssa.

Question 2: Compare few cloud data storage provider features and pricing (either for home users of for enterprises)

Answer 2:

- Elisa (Pilvilinna Plus 1000, 1000 Gt, 6,90 €/kk. Pilvilinna Plus 5000, 5000 Gt, 9,90 €/kk)
    - Kaikentyyppisilli tiedostoille
    - Mobiililaitteille ja tietokoneelle
        - Nettisilaimet Mozilla Firefox, Google Chrome)
        - Windows- ja Mac –tietokoneille asennettava työpöytäsovellus
        - Android ja iOS -mobiililaitteille
    - Tiedostojen jakaminen toisille henkilöille
    - Tiedostot tallenetaan salattuna Elisan Suomessa sijaitseville palvelimille.
    - Elisan asiakaspalvelun tuki
- Rajaton Gigantti Cloud –pilvitallennuspalvelu, 79 €/12 kk)
    - Rajaton tallennustila
    - Henkilötiedot suojataan Norjan lainsäädännön mukaisesti
    - Älypuhelimlle, tietokoneelle ja tabletille
    - Kaikentyyppisten tiedostojen tallennuspaikka
    - Tiedostojen ja kuvien automaattinen varmuuskopiointi
    - Kirjautuminen mahdollista mistä tahansa, kunhan on internet yhteys
    - Kuvien ja videoiden varmuuskopiointi suoraan puhelimesta
    - Gigantti Cloudin voi asentaa poistamaan ne tiedostot puhelimesta, jotka on jo ladattu pilveen
    - Kuvien ja videoiden järjestys ajan ja paikan mukaan
    - Kuvien ja videoiden alkuperäinen laatu ja koko säilyy
- Google Drive (15 Gt maksuton)
    - Basic, 100 Gt 19,99 €/vuosi

        - Asiantuntijoiden käyttö
        - Tiedostojen jako viiden henkilön kanssa
        - Jäsenten lisäedut
    - Standard, 200 Gt, 29,99/vuosi
        - Basic:iin ero vain tallennustilan koko
    - Premium, 2 Tt, 99,99 €/vuosi
        - Edellisiin lisänä VPN Android puhelimille
    - Premium 5 Tt, 249,99 €/vuosi
        - Premium 2 Tt:uun ero vain tallennustilan koko
    - Premium 10 Tt, 49,99 €/kk
        - Premium 2 Tt:uun ero vain tallennustilan koko
    - Premium 30 Tt, 149,99 €/kk
        - Premium 2 Tt:uun ero vain tallennustilan koko
    - Salattu ja turvallinen pääsy tiedostoihin
    - Jaetut tiedostot tarkastetaan ennakoivasti ja sisältö poistetaan, jos siinä havaitaan haittaohjelmia, roskasisältöä, kiristysohjelma tai tietojenkalastelua
    - Integroituu saumattomisti pilvipohjaisiin Docs-, Sheets- ja Slides –sovelluksiin
    - Yhteiskäyttö myös Microsoft Office –tiedostojen kanssa, tiedostomuotoja muuttamatta
    - Tallennus ja muokkaus tukevat yli sataa muuta tiedostotyyppiä
    - Drive hyödyntää Googlen hakuominaisuuksia
        - Prioriteetti ja monet muut ominaisuudet ennakoivat hakua tekoälyn avulla ja nostaa esiin henkilölle sopivinta sisältöä
- Microsoft OneDrive (Basic 5 Gt, maksuton)
    - Toimii mobiililaitteilla ja selaimessa
    - Standalone 100 Gt, 2 €/kk
    - Microsoft 365 Personal, 69 €/vuosi
        - 1 Tt tallennustilaa
            - Voi maksua vastaan laajentaa 2 Tt
        - Pakettiin sisältyy OneDriven lisäksi Skype, Outlook, Word, Excel ja Powerpoint
            - Office sovellukst voi asentaa viiteen PC- tai Mac –tietokoneeseen
        - Tiedostojen jakaminen
        - Tiwtosuoja
        - Suojaa tärkeimmät tiedostot, valokuvat ja videot käyttäjätietojen tarkistamisella
        - Jakamislinkkeihin voi asentaa vanhentumispäivän ja käyttöoikeuden rajoitetuksi ajaksi
        - Kiristysohjelmien tunnistus ja tiedostojn palautus edeltävään tilaan 30 päivää hyökkäyksen jälkeen
        - Salasanalla suojatut jakamislinkit
        - Puhelimella voi skannata ja tallentaa sivuja tulostetuista asiakirjoista, kuiteista, käyntikorteista tai valkotaulujen muistiinpanoista
        - Offline tila, jolla voi käyttää kansioita mobiililaitteella
        - PC-kansioiden varmuuskopiointi
        - Tiedostojen synkronointi PC- tai Mac –tietokoneen ja pilven välillä
        - Tiedostojen haku avainsanojen tai päivämäärän mukaan
        - Puhelimen kameran kuvien automaattinen tallentaminen pilveen
    - Microsoft 365 Family, 99 €/vuosi
        - Enintään kuusi käyttäjää, 1 Tt jokaiselle
            - Tallennustilaa voi maksua vastaan laajentaa 2 Tt

        - + muut samat ominaisuudet, jotka tulevat 365 Personal:ssa
- Dropbox
    - Plus

Question 3: Select and describe 2-3 well-known Amazon S3 data leak incidents. What went wrong? List some automated S3 bucket search engines and attack tools

Answer 3:

- 198 miljoonan yhdysvaltalaisten äänestäjien henkilökohtaisten tietojen vuotaminen. Republikaanipuolueen tukema suuri datayritys Deep Root Analytics vaaransi henkilökohtaiset tiedot ja äänestäjien profilointitiedot tallentamalla ne laajalle avoimelle S3-palvelimelle. Julkisesti saatavilla oleva tieto äänestäjistä yhdistettin ylimääräisiin markkinatutkimustietoihin, jotta yksittäisistä äänestäjistä saatiin tarkempaa tietoa heidän todennäköisestä äänestyskäyttäytymisensä tulevissa vaaleissa.
- Markkinointi- ja analytiikkayritys Alteryx, joka myy tietojen yhdistämistä ja analytiikkaa markkinointitarkoituksiin, vaaransi 123 miljoonan yhdysvaltalaisen kotitalauksen arkaluonteiset tiedot. Vuotanut tietokanta sisälsi kotitalouden osoitteet, puhelinnumerot, asuntolainaomistukset, etnisyyden ja henkilökohtaiset tiedot, mm. onko henkilö koira- tai kissaharastaja. Data ei kuitenkaan sisältänyt henkilöiden nimia, henkilöturvatunnuksia ja luottokorttien tietoja. Nämä tiedot oli saatavilla julkisesta S3-tallennusvälimuistissa.
- Pentagonin online-tiedonkeruutapojen yksityiskohtien paljastumiset. Tietoa paljastui teratavujen verran vakoiluarkistosta, ansioluettelo tiedustelutehtäviin, mukaanlukien turvallisuusselvitykset ja toimintahistoria, vultuustiedot ja metatiedot viraston sisäisestä tiedustelutietojen jakamisalustasta. Vuodot tapahtuivat huonosti konfiguroitujen S3 ämpäreiden vuoksi.
- buckets grayhatwarfare
- thebuckhacker
- Teh s3 bucketeers
- S3 Scanner

Question 4: What would a mid-size company store to the Amazon Glacier? What not? Why? What other large cloud backup or mass storage providers are there?

Answer 4: Amazon Glacier on hyvä paikka tietojen arkistointiin ja pitkäaikaiseen tallennukseen. Se on ensisijaisesti suunniteltu staattisen datan arkistointiin, jota ei muuteta tai jota ei käytetä pitkiin aikoihin (kuukausista vuosikymmeniin). Glacieriin arkistoidut tiedot pysyvät muuttumattomia sillä niitä ei voi muokata, siirtää tai kopioidaan. Eli ne voi ainoastaan ladata ja poistaa. Näiden syiden vuoksi Glacierin käyttö ei sovellu aktiivisen tiedon tallentamiseen, jota joudutaan muokkaamaan usein.

Glacierista tiedon hakuprosessi on hyvin hidasta ja monimutkaista joka on myös yksi syy miksi Glacier ei toimi, jos tarvitsee päästä nopeasti tietoihin käsiksi jotka sinne on tallentanut. Kun Glacieriin laittaa palautuspyynnön, viive vastaukseen on 3-5 tuntia ja vasta tämän jäkeen arkistot on ladattavissa. Myös jokainen palautuspyyntö maksaa ja maksu perustuu palautettavan tiedon kokoon.

Vaihtoehtona Amazon Glacierille on esimerkiksi Google Cloud Storage, Azure Archive Storage ja Blackblaze.

Week 4

Question 1: Your thoughts why small, mobile and portable devices, benefit greatly from cloud services

Answer 1: Pilvipalveluiden avulla tietoihin jotka ovat tallennettu pilveen pääsee helposti ja nopeasti käsiksi mistä vain. Varsinkin puhelin on nykyään lähes jokaisella melkein aina mukana. Puhelimen avulla on helppo tallentaa tärkeitä tietoja/tiedostoja ja nämä voi kätevästi puhelimesta varmuuskopioida pilveen. Työkannettava kulkee helposti mukana ja pilvipalveluiden avulla useita töitä voi tehdä käytännössä mistä tahansa, kunhan saa yhteyden internettiin. Puhelimissa ja muissa pienissä kannettavissa laitteissa muistin määrä on hyvin rajallinen ja pilvipalvelut auttavat muistin riittämisessä. Pienet kannettavat laitteet myös menevät helpommin rikki esimerkiksi tippumalla, sillä niitä kuljetetaan paljon paikasta toiseen. Kun tärkeimmät tiedot laitteista on varmuuskopioitu pilveen, uuteen laitteeseen saa helposti synkronoitua kaikki tarvittavat tiedot. Ylipäätään jos on tarve uudelle kannettavalle laitteella sen päivittäminen uuteen käy varmuuskopioitujen tietojen kautta kätevästi.

Question 2: Study MQTT and CoAP protocols for M2M/IoT communications. What to use and when? Locate some services or cloud data broker and analysis provides supporting either or both

Answer 2: MQTT on nopeimmin yleistyvä kevyt protokolla ja sitä käytetään tiedonsiirtoon rajoitettujen laitteiden ja palvelinsovellusten välillä. Se on alunperin tarkoitettu IoT-laitteisiin, joissa muistia on vain rajallisesti. MQTT käyttää jonkin verran enemmän resursseja vaativaa TCP-protokollaa ja kuluttaa siksi enemmmän tehoa, mutta toisaalta viestien koko voi olla vain kaksi tavua eli vähemmän mitä CoAP-protokolassa jonka viestien koko on neljä tavua. MQTT:n toteuttaminen on myös helppoa, koska protokolla on avoin ja esimerkiksi AWS:n IoT käyttää MQTT:tä viestien kuljetukseen. MQTT sopii M2M sovelluksiin, sillä se pitää kaistanleveysvaatimuksen minimissä ja vaatii vain vähän toteutusta kehittäjiltä.

CoAP:ta käytetään yleensä M2M sovelluksiin, kuten älykkäisiin energia- ja rakennusautomaatiolaitteisiin. CoAP on tehokas viestintäprotokolla vähän virtaa vaativille IoT-laitteille IoT-verkoissa. Se mahdollistaa resurssien estämät anturisolmut, kodin automaatiotyökalut ja muut yhdistety objektit, jotka vaativat vähemmän kaistanleveyttä tai laskentatehoa kommunikoidakseen internetin kanssa.

MQTT tarjoajia ovat mm Mosquito, Mosca-Now Aedes ja Python Test Broker.

KESKEN

Question 3: Describe few open source chatbot projects, frameworks and examples. List chatbot use cases where you could use chatbots either as user or provider (or both)

Answer 3:

- Microsoft Bot Framework (MBF) – tarjoaa skaalautuvia, integroituja yhteyksiä ja kehityspalveluja tarjoavia yritysliikennepalveluja. Se auttaa kehittäjiä luomaan älykkäitä botteja, joita voidaan käyttää useilla alustoilla. Bottia voidaan käyttää 141 maassa, koske se tarjoaa pilvipohjaista palvelua ja on monikielinen. Kehitystuokalu on järjestetty Microsoft Bot Builder SDK:n kanssa, johon .NET- ja Node.js kehittäjät pääsevät. Microsoftin lähestymistapa on ensisijaisesti koodipohjainen ja suunattu nimenomaan kehittäjille. MBF antaa kehittäjän täysin hallita chatbotin rakennuskokemusta. Kehysympäristössä on suuri määrä työkaluja jotka auttavat chatbotin tekemisessä. MBF:ää ei voida pitää täysin avoimen lähdekoodin ohjelmana, sillä NLU-mootori Luis

jota se käyttää, on patentoitu ohjelmisto. Kohdeympäristönä ovat: verkkosivusto, sovellus, Cortana, Microsoft Teams, Skype, Facebook Messenger ja Slack.

- BotKit – Microsoftin ostama avoimen lähdekoodin alusta. Botkit on enemmän visuaalisen keskustelun rakentaja, jossa keskitytään enemmän käyttäjän käytettävissä oleviin käyttöliittymä toimintoihin. Visuaalisen keskustelun rakentaja auttaa chatbottien kehittämisessä ja sen avulla käyttäjät, joilla ei ole paljon koodauskokemusta pystyvät mysö osallistumaan chatbotin luontiin. Myös BotKit on koodikeskeinen alusta ja kehittäjien on helppo käyttää sitä. Botkit on yksi osa laajempaa sarjaa kehittäjätyökaluja ja SDK:ita, jotka kattavat MBF:n. Bot Framework SDK tarjoaa perustan, jolle BotKit on rakennettu. Myös BotKit käyttää NLU-moottori Luis:ta, mutta se voidaan tarvittaessa integroida muihin NLU-moottoreihin. BotKit on saatavilla useilla eri ohjelmointikielillä. BotKit:ssä on paljon erilaisia laajennuksia eri chat-alustoille, kuten Webex, Slack, Facebook Messenger ja Google Hangout.

- Rasa – avoimen lähdekoodin bottien kehysympäristö joka on keskittynyt tarinalliseen lähestymistapaan chatbottien rakentamisessa. Rasa on keskittynyt tekoälyyn ja rakentamaan sellaisen kehysympäristön joka sallii kehittäjien jatkuvasti parannella heidän tekoälyapulaistaan. Rasa ei ole itse määritellyt visuaalista kulkua eikä tavoitteita alustan sisällä vaan antaa kehittäjille mahdollisuuden itse luoda tarinoita (koulutus esimerkkejä), joiden tarkoituksena on kouluttaa bottia. Rasan standardi NLU-moottori on täysin avointa lähdekoodia. Rasa X:ssä on erilaisia työkaluja joiden avulla kehittäjät voivat tarkastella keskusteluja ja parantaa avustajaa. Jokainen chatbot alusta tarvitsee tietyn verran koulutusdataa, mutta Rasa toimii parhaiten, kun siihen asetetaan suuri määrä koulutusdataa, yleensä asiakaspalvelun chat-logien muodossa. Asiakaspalvelu chat logit jäsennellään, järjestetään ja luokitellaan ja lopuksi niitä käytetyään NLU-moottotin kouluttamiseen. Yksi mahdollinen ongelma tarinnallisessa lähestymistavassa on se, että voi olla vaikea ennustaa, mitä botti aikoo tietyllä hetkellä sanoa, sillä kukaan ei pysty vaikuttamaan taustalla olevaan logiikkaan. Tätä riskiä yritetään pienentää suurella harjottelumäärällä.

Question 4: Search and describe ecamples of CAP theorem in cloud services contect

Answer 4: CAP-teoreema käsittelee kolmea ominaisuutta:

- Ristiriidattomuus (Consistency) tarkoittaa, että kaikilla palvelimilla on sama data samaan aikaan siten, että datan käyttäjä saa saman vastauksen riippumatta siitä miltä palvelimeta vastaus annetaan. Järjestelmä ei kuitenkaan pysty välittömästi tallentamaan data muutoksia kaikkille palvelimille. Tämän vuoksi tavoitteena on, että datan muutosten tallentaminen tehdään riittävän nopeasti jolloin viivettä on lähes mahdotonta huomata.
- Saatavuus (Availability) tarkoittaa, että jokaiseen käyttäjän tekemään pyyntöön (datan lukemiseen tai muokkaamiseen) tulee saada järjestelmältä vastaus vaikka toiminto epäonnistuisi.
- Osittamistoleranssi (Partition tolerance) tarkoittaa, että järjestelmä jatkaa toimintaansa huolimatta siitä, että yksittäinen palvelin ei olisikaan toiminnassa tai saavutettavissa. Palvelimen ongelmat voivat johtua esimerkiksi verkkoyhteysvirheestä tai serverin kaatumisesta

CAP-teoreeman mukaan hajautettu järjestelmä, joka käyttää jaettua dataa, voi ylläpitää täydellisesti korkeintaan kahta ominaisuutta. Pilven koostuessa sadoista tuhansista koneista on osittamistoleranssi pakollinen ominaisuus tietoverkon hallintajärjestelmälle, joten silloin täytyy valita

- peruutetaanko toiminto jolloin saatavuus-ominaisuus ei täyty, mutta ristiriidattomuus säilyy
    - Esimerkkinä pankki, jonka toiminnassa ristidiidattomuuden täytyy aina täyttyä, sillä ei voi olla tilannetta jossa pankkikortilta nostetaan rahaa vaikka sitä ei todellisuudessa tilillä olisi.

- Vai jatkketaanko operaatiota jolloin saatavuus varmistetaan, mutta ristidiidattomuus ei täyty.
    - Esimerkkinä sosiaalinen media, jonka on oltava aina saatavilla ja järjestelmän toiminta on hajautettu useammalle koneelle. Tällöin järjestelmälle on annettava mahdollisuus lähtettää palvelun käyttäjälle myös vanhentunutta tietoa (esimerkiksi toisen käyttäjän päivittämä kuva ei välttämättä näy käyttäjällä).

Week 5

Question 1: Describe pros and cons of cloud WAFs

Answer 1:

- Pilvipohjaisen WAF:t ovat edullinen vaihtoehto ja ne on helppo ottaa käyttöön. Käyttäjät maksavat kuukausittain tai vuosittain turvallisuudesta palveluna.
- Pilvipohjaiset WAF:t voi myös tarjota ratkaisun, jota päivitetään jatkuvasti uusimpien uhkien estämiseksi ilman käyttäjälle aiheutuvaa lisätöitä tai kustannuksia.
- Pilvipohjainen WAF on yös helposti vaihdettavissa uuteen/toiseen.
- Pilvipohjaisessa WAF:lla pystyy hallitsemaan käyttöoikeuksia suoraan ja yksittäisen liikennevirran pystyy estämään tiettyyn sovellukseen ilman, että se vaikuttaa sisäisiin käyttäjiin.
- Haittana on käyttäjän siirtämä vastuu kolmannelle osapuolelle, joten jotkin WAF:n ominaisuudet voivat olla heille musta laatikko.
- Haittapuolena on myös luotettavuus, pilvipohjaisen WAF:n on ohjattava tehokkaasti kaikki liikenne verkkosovellukseen. Kun WAF:n suorituskyky on heikko, niin myös verkkosovelluksen suorituskyky on heikko.
- Haittana myös se, että pilvipohjaisella WAF-toimittajalla on monia asiakkaita, jotka käyttävät samaa palvelua. Jos toimittajien palvelimet ovat ylikuormitettuja tai alhaalla, tietoturva voi kärsiä.

- Ennaltaehkäisee evästemyrkytyksiä/istuntokaappauksia
    - Kyberrikollinen manipuloi tai väärentää evästettä ohittaakseen turvallisuuden tai päästäkseen palvelimelle varastaakseen tietoja. Tällaisia hyökkäyksiä käytetään, kun käyttäjän on kirjauduttava sisään tilille ja kyberrikollinen sieppaa evästeen poimiakseen siitä tallennettuja tietoja, kuten automaattisesti täytettyjä henkilökohtaisia tietoja.
    - WAF:t pystyvät estämään edellämainitun tapahtuman suojaamalla ja salamalla henkilökohtaisia tunnistetietoja sekä tunnistamalla manipuloituja tai väärennettyjä evästeitä pääsemästä palvelimelle.
- Estää SQL-injektion (Structured Query Language injection)
    - Tarkoittaa sitä, kun kyberrikollinen muuttaa sovelluksen tekemiä kyselyitä, jotka voivat antaa kyberrikolliselle pääsyn tärkeisiin henkilökohtaisiin tai taloudellisiin tietoihin.
    - WAF kykenee estämään edellämainitun suorittamalla sääntöjä, jotka edellyttävt SQL-injektioiden täyttävän tiettyjä ehtoja, ja jos ehdot eivät täyty, se estää käyttäjältä pääsyn verkkosovellukseen
- Estää cross-site scripting:ing (XXS)
    - Evästemyrkytyksen tavoin XXS on eräänlainen injektio, johon liittyy haitallisia komentosarjoja. Kyberrikollinen lähettää haitallista koodia verkkosovelluksen kautta suoraan toiselle loppukäyttäjälle yrittääkseen päästä selaimeen tallennettuihin evästeisiin tai muihin arkaluontoisiin tietoihin joita verkkosovellus käyttää.
    - WAF voi auttaa estämään edellämainitun konfiguroiduilla käytännöillä, jotka tarkistavat ja valvovat näitä pyyntöjä ja estää ne, kun turvallisuusehdot eivät täyty.
- Estää hajautetun palveluestohyökkäyksen (Distributed Denial of Services, DDoS)
    - Hyökkäys koskee useita laitteita, jotka ovat saaneet tartunnan haittaohjelmasta, joka on vallannut verkkosovelluksen aiheuttamalla epätavallisen määrän liikennettä. Tästä

aiheutuu noraalin liikenteen palveluneston, joka aiheutaa suorituskykyongelmia ja heikentää suojauskerroksia.
- WAF pystyy tunnistamaan ja estämään tämän tyyppisen epätavallisen toiminnan avainindikaattoreiden perusteella, kuten korkea liikenteen määrä tietystä IP-osoiteessta, epätavalliset liikennöinnit tai tietyn sivun suuri liikenne.

Question 2: Search and describe some already implemented systems, how blockchains are being used by corporations

Answer 2: Lohkoketjuteknologiaa käytetään jäljentämään ja tellentamaan tuotteiden logistiikka- tai tuotantoketjuja. Tämmöisiä yrityksiä ovat esimerkiksi ShipChain ja Provenance. Logistiikka- ja tuotantoketjujen lisksi lohkoteknologia helpottaa välillistä toimintaa eli ylimääräisen paperityön jäädessä vähemmäksi tehottomuutta saadaan pienemmäksi. Lohkoketjuteknologian poistaessa välikäsiä myös kustannukset pienentyvät. Tästä voi myös aiheutua uutta liiketoimintaa, joka ei olisi mahdollista välikäsien kanssa. Lohkoteknologiaa käytetään myös rahoitusalalla, jossa lohkoteknologian avulla pyritään kehittämään järjestelmää, jossa asunto-osakekirjat voitaisiin säilyttää lohkoketjussa. Myös sosiaali- ja terveydenhuollossa pyritään käyttämään lohkoteknologiaa mm. Tietojen käsittelyyn ja turvaamiseen, maksuliikenteeseen ja sähköisiin sosiaali ja terveyspalveluihin. Esimerkiksi Mediledger, joka on lääketeollisuudelle suunnattu yksityinen lohkoketjualusta. Sen tarkoituksena on valvoa lääkkeiden toimitusketjua ja sitä kautta taata, että lääkkeiden hinnat ovat aina säädeltyjä. Dentocoin on hammasalalle suunnattu sovellus, jossa käyttäjiä palkitaan heidän tuottamastaan tiedosta liittyen palvelun laatuun ja arviointiin. Microsoft tarjoaa lohkoketjupaluna ratkaisuja, eli pilvipohjaisia kehitysympäristöjä lohkoketjujen kehittäjille. Saksalainen energiayhtiö RWE on lanseerannut lohkoketjuja hyödyntävän sähköautojen latausverkoston. Tarkoituksena on laajentaa verkoston toimintaa myös muualle Eurooppaan. Volkswagen-konerni on perustanut oman I0TA-kryptovaluuttaa hyödyntävän lohkoketjuprojektin. Lohkoketjuteknologian mahdollisuuksia nähdään esimerkiksi huoltotoiminnassa ja itseajavissa autoissa.

Question 3: List and describe shortly different open source or commercial internet networking (peer-to-peer) solutions where multiple hosts can share the host network connection(s) and other resources

Answer 3:

- ANts P2P: avoimen lähdekoodin anonyymi vertaisverkko-ohjelma joka on tehty Java-kielellä. ANts P2P kryptaa kaiken lähetetyn tai vastaanotetun liikenteen muilta ja välittää liikenteen osapuolten välillä verkossa tehdäkseen peräisin olevien IP-osoitteiden määrittämisen vaikeammaksi. ANts P2P antaa käyttäjien tarjota web-palvelimia anonyymisti eli näihin palvelimiin pääsee ainoastaan ANts P2P-verkon sisältä. ANts P2P ei välitä verkkopalvelinliikennettä ulos antaen käyttäjiä pääsemästä tavallisiin Internet-palveuihin.
- Freenet: keskuspalvelimeton hajautettu tietovarasto joka käyttää vertaisverkkotekniikkaa. Freenetin tarkoituksena on tarjota sähköinen sananvapaus vahvan anonymiteetin avulla. Freenetin käyttäjät voi julkaista ja pyytää materiaalia anonyymisti ja pyydetyn datan yksilöintiin ja paikallistamiseen Freenet käyttää avainpohjaista reititystä ja hajautettuja tiivisteitä.
- Napster: Ensimmäinen laajasti käytetty vertaisverkko-ohjelma. Ohjelmisto oli helppokäyttöinen ja se oli tarkoitettu digitaalisten musiikkitiedostojen jakamiseen. Alkuperäinen Napster suljettiin kesällä 2001 reilun puolentoista vuoden olemassa olon jälkeen. Nykyään Napster toimii samantyyppisenä maksullisena musiikkipalveluna kuin Spotify.

- GNUnet: Pääosin C-kielellä kirjoitettu vertaisverkolle oleva keskukseton runkojärjiestelmä ja se tarjoaa linkkitason salauksen sekä palvelut muiden verkon solmujen löytämieen ja resurssien jakoon. GNUnet on anonymisoiva, sensuuria ehkäisevä tiedostonjakopalvelu ja sen käyttäjät pystyy anonyymiosti julkaisemaan ja hakeman kaikenlaista tietoa. GAP-protokollaa käytetään pyyntöjen ja vastausten reititykseen.

Question 4: List and describe (with tiny examples) some commonly used data formatting standards, markup languages and syntaxes used to store or request data via cloud service APIs

Answer 4:

- JSON (JavaScript Object Notation): Asiakaspuolen komentosarjojen käsittelyssä oleva formaatti. JSON on usein nopeampi ratkaisu verrattuna muihin vaihtoehtoihin kuten XML:lle. JSON ei ole yhtä tehokas tai laajasti käytetty kuin muut vaihtoehdot, mutta sen tuki moniin ominaisuuksiin tekee siitä hyvän kilpailijan verrattuna muihin. JSON tuntee eron numeron, merkkijonon ja booleanin välillä ja tämä ominaisuus puuttuu XML:stä. Toisaalta XML pystyy käsittelemään sekoitettua sisältöä paremmin kuin JSON varsinkin silloin, kun kyseessä on sekasolmutaulukot jotka vaativat yksityiskohtaisia lausekkeita.
- XML (EXtensible Markup Language): Käytetään formaattina tiedonvälitykseen järjestelmien välillä ja tiedostomuotona dokumenttien tallentamiseen. XML on rakenteellinen kuvauskieli joka auttaa jäsentämään laajoja tietomassoja selkeämmin.
- YAML: Ei ole merkintäkieli vaan suora datamuoto. JSON ollessa kevyt ja sen ominaisuuksien ollessa suppeita ja XML:n ollessa monipuolinen, muta usein vaikeakäyttöinen, YAML on helppolukuinen, kevyt ja JSON sekä XML:n välillä oleva muoto. Vaikka YAML on luokiteltu suoraksi datamuodoksi, sillä sitä käytetään jäsentämään kokoonpano asetuksia ja relaatiokyselyitä, YAML:ää käytetään monissa järjestelmissä perustietokantana.
- RSS (Rish Site Summary): Yleisin käytetty syötetietomuoto. Vakiintanut paikkansa syötemenetelmäksi WordPressin ja muiden blogialustojen toimesta. RSS on yksinkertainen formaatti käyttää, mutta sulkee pois hyvin muodostetut XML-merkinnät suosien pelkkää tekstiä ja pakotettua HTML-koodia.

Extra bundle A

Describe these terms and concept

- **Bare metal server** – fyysinen palvelin joka on omistettu yhdelle asiakkaalle. Palvelimen asiakas voi optimoida palvelimen tarpeidensa mukaan suorituskyvyn, turvallisuuden ja toiminnan mukaan. Bare metal server:ssä operoiva järjestlmä on asennettu suoraan palvelimelle, elimoiden pinot ja toimitten paremman suorituskyvyn. Bare metal sever:ssä on pieni viive, nopea prosessointi kyky ja sopii parhaiten töihin jotka vaativat suurta laskenta voimaa kuten: suurien datamäärien käyttöön, grafiikan ja animaation renderöintiin ja kun IT-ympäristössä tarvitsee tietoturvaan täyden kontrollin.
- **Cloud broker** - välittäjä, yhteys tekniikan ja yrityksen välillä. Pilvipalveluiden välittäjiäon sekä sisäisiä että ulkoisia. Tällä hetkellä suurin osa on ulkoisia, eli he toimivat yrityksen ulkopuolella (vrt. Kiinteistönvälittäjä tai vakuutusasiamies). Ulkoinen pilvipalvelunvälittäjä voidaan jakaa vielä kolmeen eri osaan: yksinkertainen pilvivälittäjä, täydellisen infrastruktuurin välittäjä ja SaaS-välittäjä. Yksinkertainen pilvivälittäjä tarjoaa tietoa ja apua yhdessä pilvisegmentissä, joko IaaS tai PaaS palveluissa. Täydellinen infrastruktuurin välittäjä tarjoaa palvelua julkisen, yksityisen ja hybridipilvien välityksellä ja voi tarjota laajanpalvelutarjonnan. SaaS-välittäjä tutkii SaaS-palveluntarjoajia ja pystyy tarjoamaan ennakkomyynnin ehdotuksia ja myynnin jälkeisiä palveluita, kuten yhtenäisen laskutuksen, palvelutasosopimuksen, seurannan ja sopimushallinnan.
- **Microservice(s**) - arkkitehtuurityyli jossa sovelluskokonaisuus on hajautettu ja jaettu itsenäisiksiprosesseiksi, usein eri palvelimille tai pilvipalveluun. Mikropalveluiden avulla voidaan toteuttaa toiminnallisuudet omina palveluina, jotka keskustelevat toistensa kanssa rajpintojen välillä. Mikropalvelu arkkitehtuuri mahdollistaa suurten ja monimutkaisten sovellusten nopean, toistuvan ja luotettavan toimituksen. Esimerkiksi jos liiketoiminann pyörittämiseen liittyy useita toimittajia ja tietojärjestelmiä, mikropalvelu on sopiva vaihtoehto. Monitoimittajaympäristössä toimivat organisaatiot voisivat hyötyä ketteryydestä ja saada samalla kustannussäästöjä.
- **Elastic computing** – pilvipalvelun käsite, jossa pilvipalveluntarjoaja voi laskea tai nostaa resursseja helposti alas. Pilvitarjoaja pystyy tarjoamaan joustavaa optimointia milloin ja missä tahansa. Näiden resurssien joustavuus voi koskea esimerkiksi prosessointitehoa, tallennusta tai kaistanleveyytä.
- **Cloud federation** – kaksi tai useampi pilvipalveluympäristöä jakavat liikenteen kuormituksen tasapainoittamiseksi ja huomioivat kysynnästä johtuvat piikit. Sitä harjoitetaan niin yksityisessä, julkisessa kuin yhteisöpilvipalveluissa. Esimerkiksi ohjelmisto, infrastruktuurti ja alustapalvelu tekevät keskenään yhteistyötä, jotta voivat taata asiakkailleen nopeamman ja tehokkaamman palvelun.
- **AWS Lambda** – palveliton laskentapalvelu jonka tarjoaa Amazon. Sen avulla voi suorittaa taustakodeja ilman palvelimen hallintaa ja käyttöönottoa. Asiakas maksaa vain kuluneesta laskennallisesta ajasta, ajasta jonka koodi on käynnissä, ei tarvitse maksaa. AWS Lambda voidaan määrittää sisällyttämään ylimääräinen kooddi ja sisältö eri kerrosten muodossa. Nämä kerrokset ovat: Suojakerrokset, Kerrosten seuranta ja sovellusten hallintakerrokset.
- **FaaS –** palvelittoman tietojenkäsittelyn pilvipalvelumuoto ja tämä on yksi suosituin palvelittoman arkkitehtuurin muoto. FaaS:ssa kehittäjät kirjoittavat heidän sovelluksen ohjelmaa erillisinä funktiointa. Jokainen funktio suorittaa tarkkaa toimintoa, kunnes tälle toiminnolle tulee tarve. (FaaS:sta kerrottu tarkemmin viikko 2:n tehtävä 1:ssä).
- **DaaS** – pilvipalvelu joka toimitaa virtuaaliset sovellukset ja työpöydät turvallisesti pilvestä mihin tahansa laitteeseen. Tätä hallitun työpöydän virtualisointiratkaisua käytetään tarjoamaan niin turvallista SaaS:ia ja perinteisiä sovelluksia kuin myös Windows pohjaisia virtuaalisia työpöytiä ja

näitä pystytään käyttämään työpaikoilla. Maksaminen DaaS:ssa on käytöstä perustuvaa ja palvelua voi helposti laajentaa ja supistaa käyttötarpeen mukaan.

- **SSO** – single sing-on, kertakirjautuminen. Menetelmä, jossa pääsy useisiin palveluihin toteutetaan yhdellä käyttäjän todennuksella. Ideana on, että käyttäjälle ei tarvitse toistuvasti suorittaa autentikointitarkastuksia ja tätä kautta sovelluspalveluiden käyttö sujuvoituu. Käyttäjätunnus voi olla joko sama tai erilainen ja kertakirjautumisratkaisun älykkyydetä riippuen käyttäjätunnuksen erilaisuus joko hyväksytään tai hylätään.
- **Managed DNS –** asiakas ei itse hallitse DNS -servereitä vaan ostaa palveun palveluntarjoalta, esimerkiksi Amazon Route 53, Cloud DNS tai Cloudflare. Palveluntarjoaja pystyy tarjoamaan paljon joustavamman yhteyden palvelimille. Palveluntarjoaja pystyy ohjaamaan resurssiensa puolesta liikenteen dynaamisesti ja tätä kautta he lyhentävät DNS latausaikaa. Palveluntarjoajat voivat myös tarjota turvallisuuspalveluita, esimerkiksi web-sovelluksen palomuurin.
- **Origin server** – tarkoituksena on käsitellä ja vastata Internet -asiakkailta saapuvia internet pyyntöjä. Origin server -käsitettä käytetään yleensä reunapalvelimen tai välimuistipalvelimen käsitteiden kanssa. Origin server on siis tietokonen, jossa on käynnissä yksi tai useampi ohjelma, jotka ovat suunniteltu kuuntelemaan ja prosessoimaan tulevia pyyntöjä tai liikennettä.
- **Google Firebase –** sovellusalusta, joka on tarkoitettu mobiili (iOS ja Android) ja web -sovellusten luontiin. Firebase tarjoaa työkalut seuranta analytiikkaan, sovellusten kaatumisen raportointiin ja korjaamiseen, markkinoinnin ja tuotekokelun luomiseen. Firebase tarjoaa monia palveluita, kuten esimerkiksi: analysoinnin, todennuksen, reaaliaikaisen tietokannan, testilaboratorion.
- **LAMP** – kokoelma avoimen lähdekoodin ohjelmia, jotka yhdessä muodostavat WWW-palvelimen, jonka avulla voidaan palvella dynaamisia verkkosicvuja asiakasohjelmille. Dynaamiset verkkosivut käyttävät jollain ohjelmointikielellä tehtyjä ohjeita, joita suorittamalla palvelin tuottaa HTML-sivun vastauksena HTTP-pyyntöön. Ohjelmat, jotka sisältyvät LAMP:iin: Linux, Apache, MySQL/MariaDB ja PHP, Perl ja/tai Python.
- **Mashup service –** palvelu, jossa on yhdistelty erilaisia digitaalisia tiedostomuotoja tai lähteitä, kuten karttoja, musiikkia, valokuvia, videoita ja animaatioita. Esimerkiksi Trendsmap on yksi suosittu mashup service. Se yhdistää Twitterin trendaavat aiheet toisen Twitter-aihesivuston tietoihin ja näyttää sen interaktiivisella kartalla.
- **Middleware –** väliohjelmisto, on ohjelmistokomponentti, joka toimii osien tai sovelluksien välisenä rajapintana tai palveluna. Väliohjelmiston avulla ohjelmistokehittäjien on helpompi toteuttaa viestintää ja syöttöä/lähtöä, jotta he voivat keskittyä sovelluksensa tiettyyn tarkoitukseen. Väliohjelmistotyyppejä on: tapahtumaorientoitu (IBM CICS, BEA Tuxedo, Transarc Encina), viestiperustainen (IBM MQSeries, Sun Java Message Queue), proseduuripohjainen (RPC kaikkine variaatioineen), objekti- ja komponenttipohjainen (CORBA, DCOM, Java RMI, EJB,SOAP, .NET).
- **Ubiquitous computing –** jokapaikan tietotekniikka, on huomaamattomasti toimivaa ja ympäristöönsä suolautuvaa kaikkialla olevaa tietotekniikkaa. Se ei häiristee käyttäjäänsä eikä keskeytä hänen muuuta toimintaansa. Se toimii ihmisten ja yritysten arkitoimissa kaikkialla ja koko ajan. Arjen esitneet ja koneet viestivät langattomasti keskenään sekä säätävät toimintaansa itsenäisesti. Esimerkiksi äly-kodin valot, ilmastointi turvallisuus ja viihde ovat automatisoitu.
- **SLA –** Service Level Agreement (palvelutasosopimus), asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot. Sopimusta mitataan erityyppisillä mittareilla ja palvelutason alittamisesta seuraa yhteisesti sovittu sanktio. Tarkasti laadittu sopimus tarjoaa myös keinot ongelmien korjaamiseksi. Sopimuksen piiriin voi kuulua esimerkiksi logistiikan ostaminen yrityksen ulkopuolelta, tai se voidaan määritellä yhtiön sisäisten kustannusyksiköiden välillekin.

- **TCO –** Total cost of ownership, taloudellinen arvio, jonka avulla ostajat ja omistajat määrittelevät tuotteen tai palvelun välittömät ja välilliset kustannukset. Kokonaiskkustannusten osalta ostajien tulisi vaihtoehtoisten järjestelmien välillä tehdessään ottaa huomioon paitsi ostohinta myös pitkäaikainen hinta. Järjestelmällä, jolla on alhaisemmat kokonaiskustannukset, on korkeampi arvo pitkällä aikavälillä.
- **Vendor lock-in** – toimittajaloukku, tilanne, johon varomaton tietojärjestelmän ostaja joutuu valittuaan järjestelmälle toimittajan: kaikki muutostyöt on pakko ostaa samalta toimittajalta, ja tämä voi rahastaa niillä lähes miten haluaa. Myös huono laatu ja hitaus ongelmien korjaamisessa kulkevat yleensä käsi kädessä toimittajaloukun kanssa.
- **Utility computing** – malli missä laskentakapasiteetti jota tarjotaan tilauksesta maksettavan laskutusmenetelmän avulla. Se on laskennallinen liiketoimintamalli, jossa palveluntarjoaja omistaa, hallinnoi ja hallinnoi laskentainfastruktuuria ja resursseja, ja tilaajat käyttävät sitä tarvittaessa vuokrauksen tai mitatun perusteella. Tämä on yksi suosituimmista IT-palvelumalleista pääasiassa sen tarjoaman joustavuuden ja taloudellisuuden vuoksi. Kuluttajalla on lähes rajoittamaton tarjonta laskentaratkaisuja Internetin tai virtuaalisen yksityisen verkon välityksellä, ja ne voidaan hankkia ja käyttää aina tarvittaessa. Taustainfrastruktuurin sekä laskennallisten resurssien hallintaa ja toimitusta hallinnoi palveluntarjoaja.
- **Fog computing (fogging)** – arkkitehtuurimalli jossa data, käsittely ja sovellukset ovat keskittyneet laitteisiin verkon reunalla sen sijaan, että ne olisivat lähes kokonaan pilvessä. Tämä tarkoittaa, että tietoja voidaan käsitellä paikallisesti älylaitteilla sen sijaan, että ne lähetettäisiin pilveen käsittelyä varten. Tällöin Fogging vähentää palveluviitettä ja parantaa QoS:ää, mikä johtaa parempaan käyttökokemukseen. Fogging on yksi tapa käsitellä jatkuvasti kasvavien Internet-laitteiden määrää, joita joskus kutsutaan esineiden Internetiksi (IoT)
- **Network Slicing** – verkon suorituskyvystä voidaan joustavasti varata tietty osa, viipale, tietyille käyttäjille tai käyttötarkoitukselle. Esimerkiksi viipaloinnilla 5G-verkkoa saadaan joustavasti mukautettua vastaamaan erilaisiin tarpeisiin. Viipaloinnin kautta yhteys voidaan muokata tietylle yritykselle tai tieytyn kuluttajan tarpeisiin. Viipalointi mahdollistaa myös sen, että yrityksen oma verkkoliikenne pystytään eriyttämään muusta verkkoliikenteestä ja sille voidaan varata sama kapasiteetti kaikissa tilanteissa, muusta dataliikenteesät riippumatta. Tämä lisää toimintavarmuutta ja turvallisuutta.
- **Websocket** – verkkoselaimen ja -palvelimen välinen tiedonsiirtoyhteys, rakennettu TCP:n päälle. Se on suunniteltu siten, että se on yhteensopiva nykyisen verkkoinfrastruktuurin kanssa. Osana websocketin suunnitteluperiaatteina määritellään, että websocket-yhteys alkaa ensin HTTP-yhteytenä. Tämän tarkoituklsena on taata täydellinen taaksepäin yhteensopivuus edeltävien protokollien kanssa. Tämä yhteensopivuus saavutetaan käyttämällä TCP-portteja.

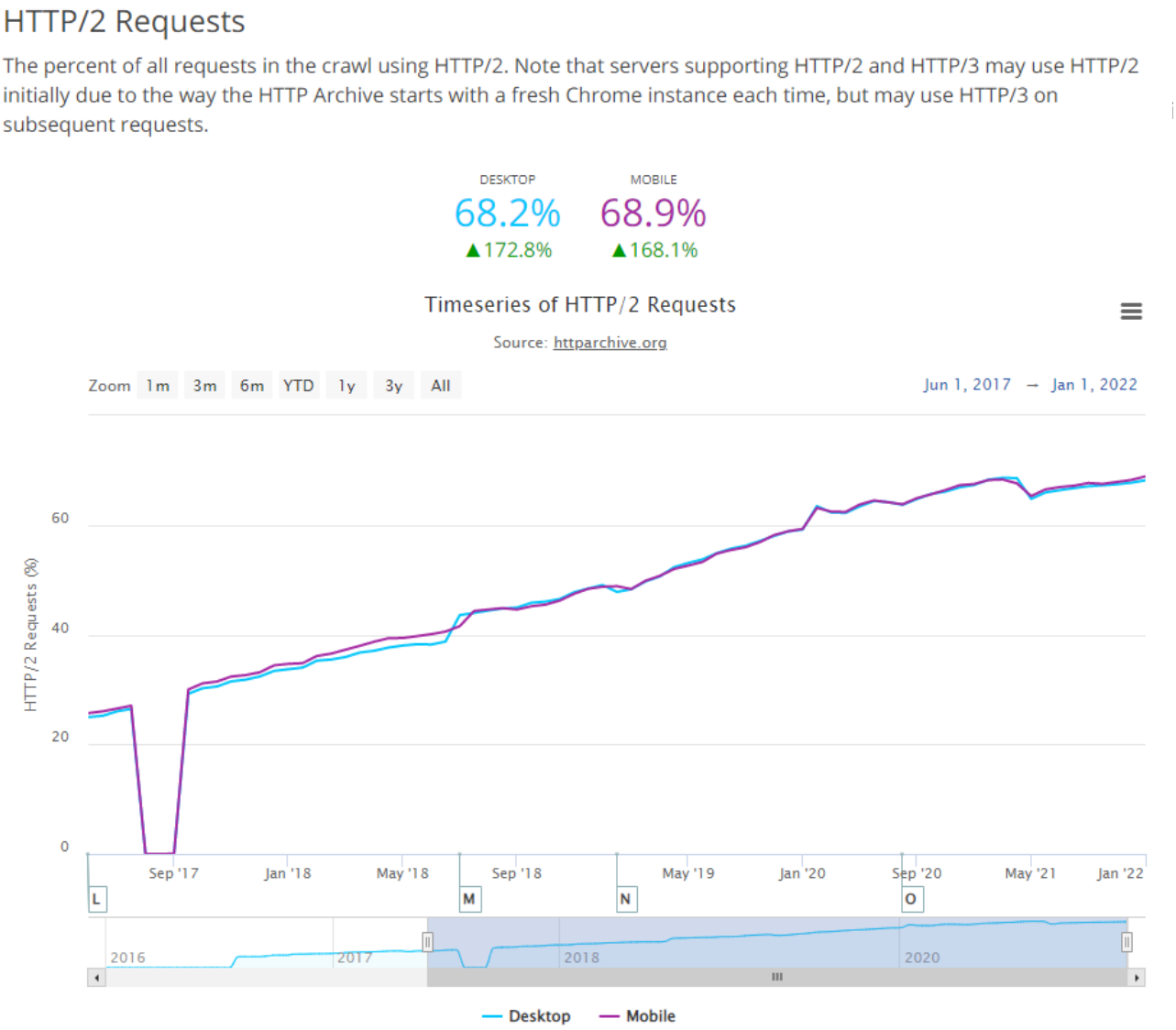
Extra bundle B

Research and answer all these questons. Few word answers are now enough. Use examples.

- **What to consider and compare when choosing a VPS server provider and VPS server features?**
  - Virtuaalipalvelimen fyysinen sijainti, esimerkiksi jos virtuaalipalvelimelle aikoo laittaa pystyyn nettisivuja, on palvelimen hyvä olla mahdollisimman lähellä loppukäyttäjää, jotta sivujen latausaika pysyy pienenä
  - RAM-muistin määrä, jos aikoo virtuaalipalvelimessa pyörittää nettisivujen lisäksi esim. sähköpostin välitystä ja sähköpostin roskapostisuodatusta, tarvitsee RAM-muistia olla tarpeeksi.
  - Kovalevyn koko ja millainen kovalevy on. Esim. SSD-kovalevy on huomattavasti nopeampi, kuin perinteinen HDD.
  - Prosessori, mitä enemmän ytimiä, sitä nopeammin tieto kulkee.
  - Yhteysnopeus ja liikennoitiraja, jos odottaa nettisivuilleen paljon vierailijoita, se tarkoitaa myös paljon tiedonsiirtoa.
  - Käyttöjärjestelmä, käyttöjärjestelmän vaihtaminen myöhemmässä vaiheessa on vaikeata, ns. turvallista on valita 64-bittinen.
  - Palvelun hinta, hintaa katsoessa hinta on hyvä suhteuttaa ylläoleviin seikkoihin sekä mistä muista asioista hinta koostuu
- **The benefits, risks and challenges of hybrid cloud computing**
  - Hyödyt
    - Jos kapasiteettitarpeet vaihtelevat, tai jos tarvitsee nopeasti uutta kapasiteettia on hybridipilvi hyvä ratkaisu.
    - Varmuuskopiot, pilvessä on tarjolla suhteessa halpaa säilytystilaa datalle, jota tarvitaan harvoin.
    - Pilvi varastokonesalina on yksi vaihtoehto
    - Pilvipalveluun sisältyy paljon erilaisia palveluita, joita on helppo ja nopea ottaa käyttöön.
  - Riskit
    - Tietovuoto/Puutteita turvatarkistuksessa, esimerkiksi inhimillisen virheen, vaarantuneen päätepisteen (esim. kadonnut älypuhelin) tai jos pilvihallinan sovellusliittymiä ei ole otettu käyttöön ja suojattu oikein.
    - Huonosti laadittu SLA, voi johtaa esim. ylihinnoitteluun.
    - Huono suojaus/ ei suojausta laisinkaan, hybridipilvessä on riskejä, jotka johtuvat tietojen siirtämisestä pilviympäristöstä toiseen.
    - Verkkoyhteyden katkeaminen, koko verkkoarkkitehtuurissa voi olla yksittäisiä vikakohtia, jotka voivat johtaa laajaan pilvipalveluiden häiriöön
  - Haasteet
    - Valmiuden puute tiedonsiirtoon, hybridipilvipalveluun siirtyminen toistesta pilvestä tai tietoverkosta on aikaa vievää ja haastavaa.
    - Taito- ja asiantuntemuksen puutteet, asiakas luottaa usein liikaa palveluntarjoajaan hybridiympäristön hallinnassa. Liiallinen riippuvuus ulkoistettuun apuun johtaa tehottomaan päätöksentekoon, mahdollisiin vaaroihin ja harvempiin liiketoimintamahdollisuuksiin.

- Yhteensopivuusongelmat, useat infrastruktuurit ja teknologiapinot yhdessä arkkitehtuurissa voivat helposti johtaa työkalujen ja prosessien yhteensopimattomuuteen.
- Näkyvyyden ja hallinnan puute, asiakkailla on vaikeuksia tarkastella ja hallita kaikkia järjestelmiä hybridi-infrastruktuutissa.

- **Why HTTP/2 (and HTTP/3) will/may speed-up many web based cloud services? What is the current HTTP/2 adaptation rate now?**
  - HTTP/2 nopeuttaa liikennettä siirtäen kaikki tiedot binäärimuodossa HTPP/1.1:n tekstimuotoon verrattuna.
  - Samassa yhteydessä voidaan siirtää useita eri tiedostoja.
  - HTTP/3 mahdollistaa vielä nopeamman ja turvallisemman tiedonsiirron hyödyntäen Quick UDP Internet Connection (QUIC)-protokollaa. HTTP/2:n heikkouden ollessa, että virhetilanteissa kaikkien samaa yhteyttä käytettävien sisältöjen siirtäminen epäonnistuu.



Extra bundle C

Research and answer all these questons. Few word answers are now enough. Use examples.

- **List and describe shortly 3-5 cloud based firewall and SIEM solutions**
  - CloudFlare WAF
    - Tarkkailee säännöllisesti Internettiä mahdollisten hyökkäysten ja haavoittuvuuksien varalta.
    - Verkkosovellusten palomuuri otetaan automaattisesti käyttöön kaikesta sellaisesta, jota pidetään uhkana suurimmalle osalle asiakkaista.
    - Päivitetään jatkuvasti ja tämän kautta varmistetaan, että CloudFlaren suojaus on aina ajantasainen.
    - Suuren asiakaskunnan vuoksi CloudFlare pystyy luottamaan kollektiiviseen älykkyyteen uhkien poistamisessa.
      - Eli kun yksi asiakas luo uuden säännön palomuurille, CloudFlare tarkistaa tarvitseeko saman säännön ottaa käyttöön muillekin asiakkaille.
  - AWS WAF
    - Käyttäjät voivat itse luoda räätälöidyt säännöt jotka ovat suunniteltu estämään yleiset hyökkäysmallit, kuten sivustojen väliset komentosarjat.
    - AWS:ssä on täysin varusteltu ohjelmointirajapinta jonka avulla käyttäjät voivat autamatisoida kaikkien käytössä olevien sääntöjen luomisen, käyttöönoton ja ylläpdon.
  - Sophos Firewall
    - Sophos Firewall suojaa sovellukset ja on langaton yhdyskäytävänä.
    - Käyttäjät pystyvät hallinnoimaan palomuuriasetuksia ja apuohjelmien kojelautaan. Apuohjelmien kojelaudassa pystyy tarkastelemaan verkkoa, käyttäjiä ja sovelluksia.
    - Erikseen lisättävä Sophos ‘iView’, joka tarjoaa keskitetyn raportoinnin useiden palomuurien välillä.
    - Hallintaliittymä antaa käyttäjälle yleiskatsauksen ominaisuuksista, kuten liikennetiedot, järjestelmätilastot ja palomuurisäännöt.
  - Datadog Cloud SIEM
    - Tarjoaa vakaan uhkien havaitsemisen dynaamisiin, pilvitason ympäristöihin.
    - Datadog Cloud SIEM:n avulla pystyy analysoimaan toiminta- ja suojauslokeja reaaliajassa, riippumatta siitä kuinka paljon analysoitavaa on sekä hyödyntämään valikoituja, valmiita integraatioita ja sääntöjä uhkien havaitsemiseen.
    - Yksityiskohtaisten havaintotietojen hyödyntäminen joka auttaa nopeuttamaan tietoturvatutkimuksia yhdellä alustalla.
  - SolarWinds Security Event Manager (SEM)
    - Tarjoaa pääsyn lokitietoihin rikosteknisiä ja vianetsintä tarkoitusta varten sekä työkaluja, jotka auttavat hallitsemaan lokitietoja.
    - Hyödyntää kerättyjä lokeja, analysoi ne reaaliajassa ja ilmoittaa ongelmasta ennen kuin ongelma aiheutta lisävauriota.
    - Esimerkiksi kehittyneet uhat voivat johtua verkkotapahtumien yhdistelmästä, kuten ohjelmistoasennuksista, todennustapahtumista sekä saapuvasta ja lähtevästä verkkoliikenteestä. Lokitiedot sisältää kaikki tiedot näistä tapahtumista. SolarWinds SEM tunnistaa uhkatoiminnan ja ilmoittaa mahdollisista poikkeavuuksista.

    - Splunk Enterprise Security (ES)
        - Antaa tietoa järjestelmässä liikkuvasta datasta ja kertoo, jos on syntymässä mahdollisia ongelmatilanteita.
        - Kerää tietoa reaaliaikaisesti ja tallentavasti.
        - Pystyy indeksoimaan kaiken tiedon, riippumatta tiedon lähteestä, muodosta tai käyttötarkoituksesta.
- **Companies using Software Defined Networking (or cloud networking solutions like Maraki) benefit from cloud services. Why? List some SDN vendors and products**
    - Pilvipalvelun avulla SDN:stä saa herkemmän ja sen käyttäminen on halvempaa.
    - Resurssien siirtäminen yrityksiin on nopeampaa ja läpinäkyvämpää
    - Tietoturva- ja käytäntötietojen jakaminen johdonmukaisesti koko yrityksessä.
    - Myyjiä
        - Andara Networks – Andara Sky Controller
        - Cisco – Cisco Open SDN Controller
        - Extreme Networks – Extreem Networks SDN Solution
- **List and describe few recent (or possible) software supply chain security incidents and issues where application source code is fetched from the cloud service during the build process**
    - Alex Brisman tunkeutui mm. Applen ja Microsoftin järjestelmiin ujuttamala niihin omia ohjelmistopaketteja. Brisman käytti murtautumisessa hyväkseen virhetilanteita laajasti käytettyjen ohjelmointikielten pakettihallinnassa. Brisman selvitti mahdollisimman monien sisäisten pakettien nimiä ja loi omat pakettinsa identtisin nimin asianmukaisiin julkisiin pakettivarastoihin.
    - SolarWinds Orion Platform -hallintatyökaluun lisätty takaovi. Takaovi onnistuttiin levittämään tuhansiisn organisaatioihin. Takaovea on voitu käyttää organisaation palveluihin tunkeutumiseen ja sillä mahdollistettiin haitallisen sisällön lisääminen.
    - Asusin palvelimen kaapanneet murtautujat onnistuivat syöttämään haittaohjelmia sadoille tuhansille tietokoneilla. Kohteena olivat tietyt tietokoneet ja niihin asennettiin erityisiä räätälöityjä haittaohjelmia.
- **“If the cloud product is free. Then you are the product” -Explain the logic and meaning. Note: This phrase and logic is somewhat controversial**
    - Jos yritys antaa jotakin ilmaiseksi, silloin yritys saa rahaa jollain muulla keinolla ja se on usein myymällä tietoja käyttäjältä. Myytävät tiedot voivat olla henkilökohtaisia tietoja tai yritys voi käyttää tehokkaamaa mainontaa, jotta käyttäjä hankkisi maksullisen palvelun.

…