Mitä pilvipalvelut oikeastaan ovat?

Digisauruksille Huhtikuu 09. 04. 2024

Kristian Salmi

Mitä?

Eikö pilvipalvelut ole turvallisia?

Tapaus CloudNordic marraskuu 2023
”CLOUDNORDICIN KALTAINEN TAPAUS olisi Nordcloudin teknologiajohtajan Ilja Summalan mielestä mahdollinen myös Suomessa.”
”CloudNordic osoitti, mitä voi tapahtua, kun yritetään itse liian pienillä resursseilla. Ransomwaresta on tullut jo ihan oma toimialansa, ja roistoilla on usein enemmän rahaa ja energiaa kuin monella yrityksellä. Heillä on myös paremmat kannustimet onnistua, Summala sanoo.”
”Riskejä lisää, että pilvipalvelut ovat tuoneet perinteisestikin hankalaan ict-hallintaan lisää vaikeuskerrointa. Kokonaisuuden hallinta voi osoittautua haasteelliseksi.”

Pilvipalveluiden historia

Pilvipalvelun historia osa 1

Pilvipalveluilla on rikas historia, joka juontaa juurensa 1960-luvulle. Time-sharing-konseptilla, jossa useat käyttäjät voivat käyttää yhtä tietokonejärjestelmää samanaikaisesti, oli merkittävä rooli pilvipalveluiden kehityksessä. Tässä on joitain tärkeitä virstanpylväitä pilvipalvelun historiassa:

1. 1960-luku: Aikajaon käsite syntyi, jolloin useat käyttäjät pystyivät käyttämään yhtä tietokonejärjestelmää samanaikaisesti. Tämä loi pohjan ajatukselle laskentaresurssien jakamisesta.

2. 1990-luku: Termi "pilvilaskenta" keksittiin, vaikka käsitettä ei tuolloin laajalti tunnettu. Painopiste oli virtualisoidun IT-infrastruktuurin ja -palvelujen tarjoamisessa.

3. 2000-luvun alku: Amazon esitteli verkkopohjaiset vähittäismyyntipalvelunsa vuonna 2002, mikä oli yksi ensimmäisistä suurista pilvipalvelun sovelluksista. Amazon Web Services (AWS) nousi myöhemmin johtavaksi pilvipalvelujen

Pilvipalvelun historia osa 2

4. 2006: Google julkaisi Google Appsin, pilvipohjaisten tuottavuustyökalujen, mukaan lukien G mailin, Google Docsin ja Google Driven. Tämä oli merkittävä askel pilvipohjaisten ohjelmistosovellusten käyttöönotossa.

5. 2008: OpenStack-projektin, avoimen lähdekoodin pilvilaskenta-alustan, julkaisu vauhditti entisestään pilviteknologioiden kehitystä ja käyttöönottoa.

6. 2010: Yhdysvaltain hallitus käynnisti Federal Cloud Computing Initiativen, jonka tavoitteena on edistää pilvipalveluiden käyttöönottoa liittovaltion virastoissa.

7. Nykyhetki: Pilvipalveluista on kehittynyt olennainen palvelu monille nykyaikaisille organisaatioille. Se tarjoaa skaalautuvuutta, joustavuutta ja kustannustehokkuutta, minkä ansiosta yritykset voivat käyttää laskentaresursseja tarpeen mukaan ilman laajoja infrastruktuuri-investointeja.

Huomaa, että tämä on vain lyhyt katsaus pilvipalvelun historiaan. On monia muita kehityssuuntia ja

Pilvipalveluiden tekniikka

Yksinkertaisen pilvipalvelu-laitteiston kokoonpano(tieto peräisin vuodelta 2012 azure)

1. Suoritin ja muisti: On suositeltavaa, että sinulla on vähintään 2 uusinta Intel-tyyppistä CPU-kantapalvelinta, joissa on vähintään 128 Gt muistia paremman suorituskyvyn saavuttamiseksi.

2. Heterogeenisten järjestelmien tuki: Laitteistosi tulisi tukea erilaisia järjestelmiä varmistaakseen yhteensopivuuden erilaisten pilvipalvelujen kanssa.

3. Palvelunhallinta: Laitteistolla tulee olla tehokkaan palvelunhallinnan ominaisuudet, joiden avulla voit valvoa ja hallita pilvipalveluita tehokkaasti (dynaamisesti).

4. Dynaaminen työtaakka ja resurssien hallinta: Laitteiston tulee tukea dynaamista työtaakkaa ja resurssien hallintaa, jotta voit allokoida ja hallita resursseja tehokkaasti kysynnän mukaan.

5. Luotettavuus, saatavuus ja suojaus: Laitteiston tulee tarjota korkea luotettavuus-, käytettävyys- ja suojaustaso pilvipalvelusi moitteettoman toiminnan varmistamiseksi ja tietojesi suojaamiseksi.

On tärkeää huomata, että nämä ovat yleisiä näkökohtia, ja erityiset laitteistovaatimukset voivat vaihdella pilvipalvelusi laajuuden ja erityistarpeiden mukaan.

Pilvipalvelun verkkorakenne

Millaisia tietoliikennelaitteita tarvitaan täydelliseen toiminnalliseen pilveen

Täysin toimivan pilviinfrastruktuurin saamiseksi tarvitset erilaisia tietoliikennelaitteita tukemaan sen toimivuutta. Tässä on joitain olennaisia komponentteja:

1. Palvelimet: Nämä ovat minkä tahansa pilviinfrastruktuurin selkäranka. Palvelimet vastaavat tietojen tallentamisesta ja käsittelystä, sovellusten suorittamisesta ja virtuaalikoneiden hallinnasta.

2. Verkkokytkimet: Kytkimet yhdistävät useita laitteita verkossa, jolloin ne voivat kommunikoida. Pilviympäristössä kytkimet käsittelevät tiedonkulkua palvelimien, tallennuslaitteiden ja muiden verkkokomponenttien välillä.

3. Reitittimet: Reitittimet mahdollistavat viestinnän eri verkkojen välillä. Ne määrittävät optimaalisen reitin datapakettien kulkemiseen verkosta toiseen varmistaen tehokkaan tiedonsiirron.

4. Palomuurit: Palomuurit tarjoavat verkon turvallisuutta valvomalla ja ohjaamalla tulevaa ja lähtevää verkkoliikennettä. Ne suojaavat pilvi-infrastruktuuria luvattomalta käytöltä, haittaohjelmilta ja muilta uhilta.

5. Kuormituksen tasaajat: Kuormanjakolaitteet jakavat verkkoliikenteen useiden palvelimien kesken varmistaakseen optimaalisen suorituskyvyn ja estääkseen yksittäisen palvelimen ylikuormituksen. Ne auttavat saavuttamaan korkean käytettävyyden ja skaalautuvuuden pilviympäristössä.

Millaisia tietoliikenneratkaisuja tarvitaan täydelliseen toiminnalliseen pilveen 2

6. Storage Area Network (SAN): SAN-verkot tarjoavat nopean keskitetyn tallennustilan pilvi-infrastruktuurille. Niiden avulla useat palvelimet voivat käyttää ja jakaa tallennusresursseja, mikä tarjoaa joustavuutta ja skaalautuvuutta.

7. Virtual Private Network (VPN): VPN:t luovat suojattuja yhteyksiä julkisten verkkojen yli, jolloin etäkäyttäjät tai -sivustot voivat käyttää pilvi-infrastruktuuria turvallisesti. VPN-verkot salaavat tiedot ja tarjoavat todennuksen varmistaen luottamuksellisuuden ja eheyden.

8. UPS (Uninterruptible Power Supply): UPS-järjestelmät tarjoavat varavirtaa sähkökatkojen varalta. Ne varmistavat, että pilvi-infrastruktuuri pysyy toimintakuntoisena myös sähkökatkojen aikana, mikä estää tietojen katoamisen tai palvelukatkoksia.

9. Valvonta- ja hallintatyökalut: Nämä työkalut auttavat valvomaan pilvi-infrastruktuurin suorituskykyä, saatavuutta ja turvallisuutta. Ne antavat tietoa järjestelmän kunnosta, resurssien käytöstä ja auttavat vianmäärityksessä ja kapasiteetin suunnittelussa.

On tärkeää huomata, että tarvittavat tietoliikennelaitteet voivat vaihdella pilvi-infrastruktuurisi laajuuden ja vaatimusten mukaan. Ammattilaisen tai pilvipalveluntarjoajan konsultoiminen voi auttaa sinua määrittämään tarkat laitteet, joita tarvitset juuri sinun käyttötilanteeseesi.

Ja yhteydet pilvipalveluihin

Esimerkiksi Security Service Edge

Security Service Edge (SSE) on käsite, joka viittaa suuralueverkko- (WAN) ja tietoturvapalvelujen toimittamiseen pilvipalveluina suoraan yhteyslähteeseen perinteisen datakeskuksen sijaan. Se tunnetaan myös nimellä Secure Access Service Edge (SASE). SSE antaa nykyaikaisille yrityksille mahdollisuuden vastata hajautetun työvoiman tarpeisiin tarjoamalla yhtenäisen pilvipohjaisen tietoturva- ja verkkoratkaisun.

Tässä on joitain avainkohtia Security Service Edgestä (SSE):

• SSE tarjoaa pilvipohjaisen, integroidun suojauksen, joka mahdollistaa turvallisen pääsyn verkkosivuille, SaaS-sovelluksiin ja yksityisiin sovelluksiin.

• Se turvaa pääsyn verkkoon, pilvipalveluihin ja yksityisiin sovelluksiin.

• SSE tarjoaa ominaisuuksia, kuten pääsynhallinnan, uhkien suojauksen ja suojatun yhteyden.

• Sitä kuvataan SASE-arkkitehtuurin palveluiden tietoturvapinoksi.

• SSE on nopea, helppokäyttöinen ja varmistaa verkkoyhteyksiesi turvallisuuden.

Kaiken kaikkiaan Security Service Edge (SSE) on moderni lähestymistapa verkko- ja tietoturvapalveluihin, joka hyödyntää pilvilaskentaa ja tarjoaa turvallisen ja tehokkaan pääsyn resursseihin hajautetuille työntekijöille.

Pilvipalveluiden kyberturvallisuus

Tästä lähdetään:

”Pilvipalveluiden perusturvallisuus muodostetaan siinä käsiteltävästä datasta!”

Siis

>>Käsiteltävä data määrittelee sen mistä kompnenteista pilvi tulee koostumaan<<

Julkisen pilven tietoturvariskit

Pilvipalveluiden kyberturvallisuus on tärkeä aihe, joka koskee pilvipalveluiden turvallisuutta ja suojausta kyberuhkilta.

Pilvipalvelut ovat palvelumalleja, joissa tietoteknisiä resursseja jaetaan useiden käyttäjien kesken.

Esim. Kyberturvallisuuskeskus on julkaissut useita asiakirjoja ja arviointikriteeristöjä, jotka käsittelevät pilvipalveluiden turvallisuutta.

Seuraavissa kalvoissa tuodaan esille yleisimmät kyberuhat sekä suositukset niiden ehkäisemiseksi.

Julkisen pilven tietoturvariskit

Esimerkiksi Vaikka julkiset pilvijärjestelmät tarjoavat skaalautuvuutta, joustavuutta ja kustannustehokkuutta, ne voivat myös aiheuttaa merkittäviä riskejä, jos niitä ei ole suojattu asianmukaisesti.

Kaikilla pilvi- (ja IT-)ympäristöillä on yhteisiä tietoturvaongelmia ja -ratkaisuja, mutta julkisen pilven käyttäjille vaatimustenmukaisuus, kulunvalvonta ja oikeat konfigurointikäytännöt ovat suorastaan kriittisiä.

Tietovuodot

Miten ne tapahtuvat:

Luvaton pääsy arkaluontoisiin tietoihin voi johtua haavoittuvuuksista ja virheellisistä määrityksistä, kuten virheellisistä, liian laajoista käyttöoikeuksista tai suojaamattomista arkaluontoisista tiedoista.

Ennaltaehkäisy:

Ota käyttöön vankka salaus, pääsynrajoitukset, tietojen luokittelu, suojatut yhteydet ja tapausvastausstrategia.

Käyttöoikeuksien valvonta

Miten ne ilmenevät:

Väärin määritetyt käyttöoikeudet voivat antaa luvattomille henkilöille pääsyn sovelluksiin ja tietoihin, mikä saattaa johtaa tietovuotojihin ja tietomurtoihin sekä muihin tietoturvariskeihin.

Ennaltaehkäisy:

Käytä vähimmän oikeuksien mallia tai ”zero trust" -mallia, suorita usein pääsytarkastuksia ja käytä Identity and Access Management (IAM) -työkaluja. Turvattomat testaamattomat, sovellusliittymät ja pilvirajapinnat

Miten ne tapahtuvat:

Haavoittuvat sovellusliittymät ja vajavaisesti suojatut pilvirajapinnat mahdollistavat hyväksikäytön, mikä voi johtaa tietovuotoon ja tietomurtoihin.

Ennaltaehkäisy:

API-suojauskäytännöt ja -työkalut, suorita säännöllinen haavoittuvuustestaus ja valvo tiukkaa (zero trust) pääsynvalvontaa.

Tilin kaappaus

Miten se tapahtuu:

Hyökkääjät hankkivat laittoman pääsyn käyttämällä varastettuja käyttäjätunnuksia, jotka voivat johtaa luvattomaan tilien ja tietojen käyttöön tai tietojen tahalliseen muuttamiseen.

Ennaltaehkäisy:

Edellytä monitekijätodennusta (MFA), kouluta käyttäjiä salasanasuojauksesta ja tarkkaile säännöllisesti tilejä epäilyttävän toiminnan varalta.

Riittämätön lokitus ja seuranta

Miten se tapahtuu:

Ilman riittävää lokitusta ja valvontaa tietoturvahäiriöiden havaitseminen reaaliajassa muuttuu vaikeaksi. Tälle pilviympäristö on herkkä.

Ennaltaehkäisy:

Aktivoi pilvilokitukset (kaikki) ja käytä SIEM-järjestelmiä verkon ja järjestelmän ***toiminnan jatkuvaan seurantaan***.

DDoS-hyökkäykset

Miten ne tapahtuvat:

Hajautetut palvelunestohyökkäykset (DDoS) ylikuormittavat pilven ja verkkojärjestelmät, keskeyttävät pääsyn ja laukaisevat palveluhäiriöitä.

Ennaltaehkäisy:

DDoS-hyökkäyksiä voidaan estää ja vähentää käyttämällä DDoS-suojauspalveluita, asentamalla liikenteen suodatusta ja ottamalla käyttöön sisällönjakeluverkkoja (CDN) ylimääräisen liikenteen käsittelemiseksi.

Tietojen menetys

Miten se tapahtuu:	Ennaltaehkäisy:
Tietojen tahaton poistaminen, korruptio tai varkaus voi johtaa peruuttamattomaan tietojen menettämiseen, toiminnan häiriintymiseen ja arkaluonteisten tietojen paljastamiseen, jotka voivat myös rikkoa tietosuojasääntöjä.	Varmuuskopioi tiedot säännöllisesti, kehitä tietojen luokittelu- ja säilytyskäytäntöjä, käytä versiointiominaisuuksia, käytä Data Loss Prevention (DLP) -työkaluja ja opeta työntekijöille tietojen hallintaa ja käytäntöjen noudattamista.

Esimerkki miten Julkisia pilviympäristöjä suojataan

Toteuta seuraavia menetelmiä parantaaksesi turvallisuutta julkisessa pilviasetuksessa:

• Käytä vahvaa todennusta: Lisää käyttäjien sisäänkirjautumisen turvallisuutta käyttämällä monitekijätodennusta (MFA), joka lisää varmennusastetta laittoman käytön estämiseksi.

• Säännölliset päivitykset ja korjaukset: Suojaa pilviympäristöäsi päivittämällä ja korjaamalla ohjelmistoja ja sovelluksia säännöllisesti estääksesi tunnettuja haavoittuvuuksia.

• Jatkuva seuranta: Ota käyttöön pilviresurssien jatkuva seuranta havaitaksesi epäilyttävät toiminnot reaaliajassa. Määritä hälytykset ilmoittamaan sinulle mahdollisista tietoturvaloukkauksista heti, kun ne tapahtuvat.

• Turvallisuusohjeet ja -menettelyt: Kehitä ja ota käyttöön kattavat tietoturvakäytännöt ja -prosessit, jotka ohjaavat organisaatiosi pilvikäyttöä ja takaavat johdonmukaisuuden ja vaatimustenmukaisuuden.

• Tietojen luokittelu: Luokittele tiedot niiden herkkyyden mukaan ja käytä asianmukaisia turvatoimia. Tämä räätälöity menetelmä takaa, että tiedot suojataan asianmukaisesti niiden merkityksen mukaisesti.

• Henkilöstön koulutus: Kouluta työntekijöitä pilviturvallisuuden parhaista käytännöistä ja pilven käyttöön liittyvistä mahdollisista riskeistä.

Ensimmäinen puolustuslinjasi uhkia vastaan on hyvin perillä oleva henkilökunta.

No, entä riskit muissa pilvipalveluversioissa ja yhdistelmissä??

….Yllättäen niillä on myös edellämainitut vaarat olemassa …

..Suljettu pilvi ; Hybridipilvi ; Multipilvi…

….On prem ja muut passiiviset tietovarastot….

….Ja sitten vielä eri pilvipalveluversioihin ja aliversioihin kytkettyjä lisä-vaaroja..

En lähde niitä tässä erittelemään, koska toivon, että pointtini on käynyt jo selväksi?

Erilaisia pilvipalvelualustoja

Microsoft Azure:
Microsoft Azuressa tarjotaan monia erilaisia pilvipalveluita, kuten tietokantoja, laskentaresursseja ja tallennustilaa. Sitä käytetään usein yritysten sovellusten kehittämiseen ja käyttöönottoon.

Amazon Web Services (AWS):
AWS on suosittu pilvipalvelualusta, joka tarjoaa laajan valikoiman palveluita, kuten tietokantoja, tallennustilaa ja tekoälypalveluita. Sitä käytetään usein verkkosivustojen ja sovellusten isännöintiin.

Google Cloud Platform (GCP):
GCP tarjoaa pilvipalveluita, kuten tietokantoja, laskentaresursseja ja tekoälypalveluita. Sitä käytetään usein datan analysointiin, koneoppimiseen ja sovellusten kehittämiseen.

Dropbox:
Dropbox on pilvipalvelu, joka tarjoaa tallennustilaa tiedostojen jakamiseen ja synkronointiin eri laitteiden välillä. Sitä käytetään usein tiedostojen varmuuskopiointiin ja yhteistyöhön.

OneDrive:
OneDrive on Microsoftin tarjoama pilvitallennuspalvelu, joka mahdollistaa tiedostojen tallentamisen ja jakamisen eri laitteiden välillä. Sitä käytetään usein henkilökohtaiseen tiedostojen varmuuskopiointiin ja saatavuuteen.

VMware
rakentaa täydet pilvipalvelut Azure; AWS; alustojen päälle. Hallitsee OSI-ISO tasoilla 2-7 toiminnat.

Oletteko harkinneet siirtää tietojen käsittelyn pilveen?

- Edellä kuvatut asiat on tällöin oltava varmassa hallinnassa…!

- Samalla kannattaa uusia koko tiedonhallintasuunnitelma

- Kannattaa ottaa nyt heti käyttöön NIS2 (iso 27000 + ISMS)

- Mikä tulee olemaan AI:n ja ML:n osuus uudessa konseptissa?

- Mitä vielä ??? Ideoidaan !!!

Kun nyt sitten kuitenkin olette siirtämässä tietojenkäsittelyn pilveen niin kerrataan…

1 - Huomasitte kai, että pilven käytön suunnittelu lähti liikkeelle siirrettävän datan olemuksesta ja sen käytettävyydestä?

2 - Sama pilvikokonaisuus voidaan tavoittaa natiivisti, sekä C/S versioineen että Edge computing protokollilla (APP).

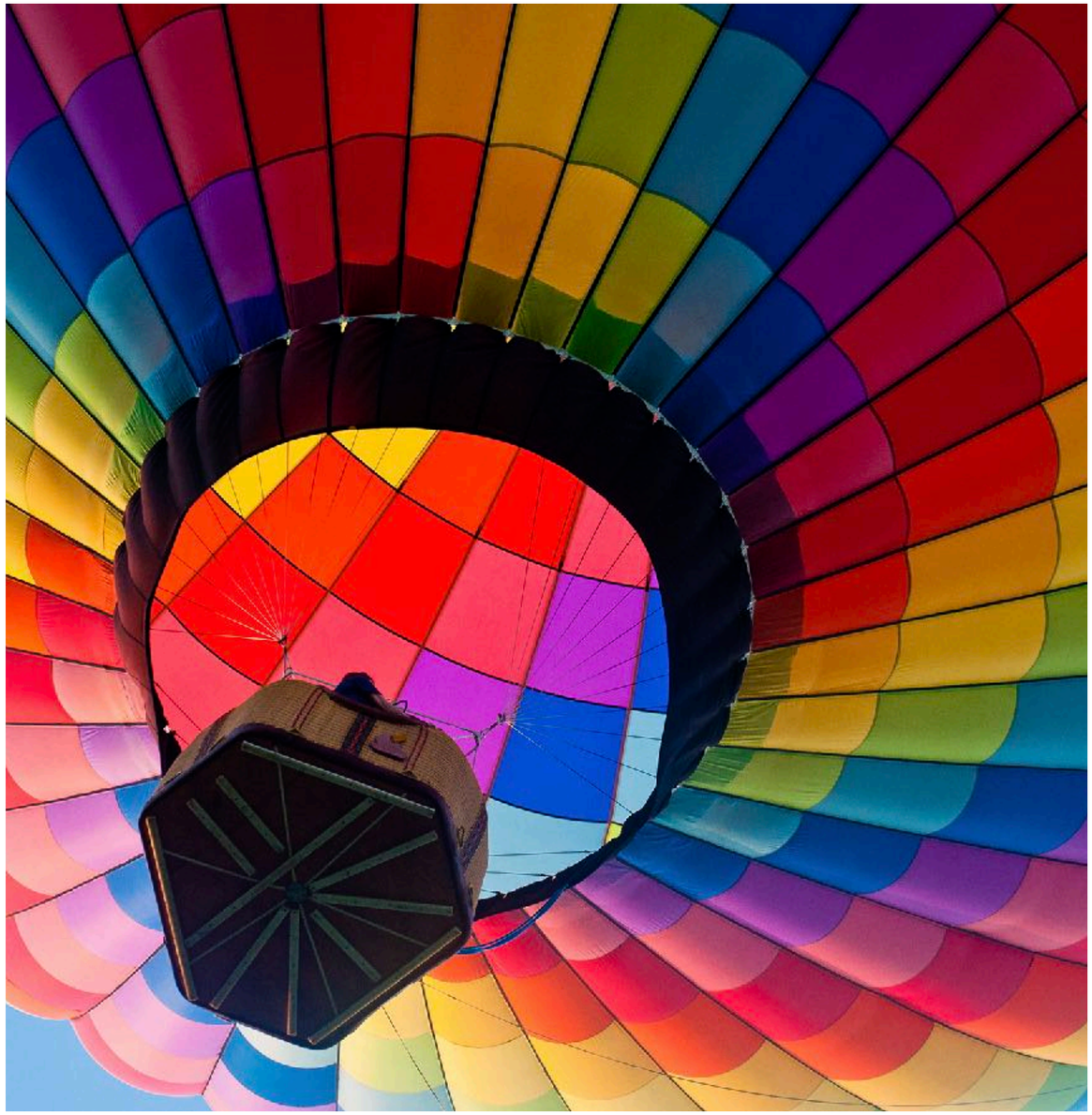
3 - Pilvipalvelukokonaisuuksia voidaan käynnistää ja sulkea tarpeen mukaan, ja poistaa käytöstä tarpeen poistuttua.

4 - Pilvipalvelu vaatii 24/7 automaattivalvonnan (AI)

5 - Mutta ennen kaikkea pilviteknologia *vaatii* uuden tavan hahmottaa oman yrityksen / viraston tietojenkäsittelyn tarpeet

Loppukaneetti

Pilvipalvelukonseptilla ja tekoälyllä on yllättävän samanaikainen ”lentoonlähtö” eli 2010 eteenpäin. Molemmat todennäköisesti tarvitsevat toisensa onnistuakseen.



Lähteet

Parin viime vuoden ajalta

- Techrepublic
- Technopedia
- Microsoft
- AWS
- Google cloud
- The hacker News
- Cloud Native Now
- Wileys kirjallisuus aiheesta
- Mercury magazines kirjallisuus
- CISA pilviturvallisuus julkaisut

Ilmoitus:

Jatkoa seuraa.....

Tämän sarjan viimeinen osa valmistumassa …