|  |
| --- |
| 4 - Daraja | Networking in the Cloud |
| Abdulloh Xalilov |

**6-Qism:** 4-Daraja | Networking in the Cloud

**O‘qituvchi:** Dostonbek Abdumajidov

**Guruh identifikatori:** 23-412 Software (C#)

**Talaba ID:** 231397

**Taqdim etilgan sana:** 2.06.2025 yil

**BTEC o'quvchilar topshiriqlarini baholash va deklaratsiya**

Baholash uchun ishlarni taqdim etganda, har bir o'quvchi ish o'ziniki ekanligini tasdiqlovchi deklaratsiyani imzolashi kerak.

|  |  |
| --- | --- |
| **O‘quvchi (talaba) identifikatori:** | 231397 |
| **Baholovchi nomi:** | Dostonbek Abdumajidov |
| **BTEC dasturi nomi:** | Pearson BTEC Higher Nationals in Information Technologies |
| **Birlik yoki komponent raqami va nomi:** | 4-Daraja | Networking in the Cloud |
| **Topshiriq nomi:** | 4-Daraja | Networking in the Cloud |
| **Topshiriq topshirilgan sana:** | 2.06.2025yil |

Iltimos, har bir topshiriq uchun berilgan ishlarni sanab o'ting. Ishlarni topish mumkin bo'lgan sahifa raqamlarini ko'rsating yoki ishlarning mohiyatini tavsiflang (masalan, grafik, rasm).

|  |  |  |
| --- | --- | --- |
| **Topshiriq vazifasi ma'lumoti** | **Ishlar taqdim etildi** | **Sahifa** |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **O'quvchi deklaratsiyasi**  Men ushbu topshiriq uchun taqdim etilgan ish meniki ekanligini tasdiqlayman. Ishda foydalanilgan manbalarga aniq havola qildim. Men noto'g'ri deklaratsiya noto'g'ri ishlashning bir shakli ekanligini tushunaman.  **O‘quvchi imzosi:**  **Sana:** 2.06.2025 yil |

Mundarija

[KIRISH 3](#_Toc199780444)

[A.P1 4](#_Toc199780445)

[A.P2 8](#_Toc199780446)

[A.M1 11](#_Toc199780447)

[A.D1 13](#_Toc199780448)

[B.P3 16](#_Toc199780449)

[B.P4 18](#_Toc199780450)

[B.M2 20](#_Toc199780451)

[C.P5 21](#_Toc199780452)

[C.P6 24](#_Toc199780453)

[C.M3 26](#_Toc199780454)

[C.D2 28](#_Toc199780455)

[D.P7 29](#_Toc199780456)

[D.P8 31](#_Toc199780457)

[D.M4 32](#_Toc199780458)

[D.D3 34](#_Toc199780459)

[Xulosa 36](#_Toc199780460)

[ADABIYOTLAR RO'YXATI 37](#_Toc199780461)

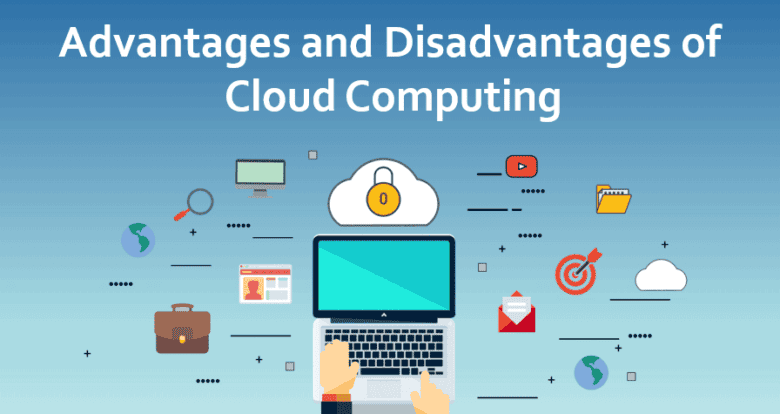
KIRISH

Ushbu tahliliy hisobot kompaniyaning tayyor kiyim-kechak mahsulotlarini ulgurji yetkazib berish faoliyatidagi mavjud IT infratuzilmasini modernizatsiya qilish, xususan, Korxona Resurslarini Rejalashtirish (ERP), Mijozlar bilan Munosabatlarni Boshqarish (CRM) va Omborlarni Boshqarish Tizimi (WMS) kabi muhim tizimlarni bulut muhitiga o‘tkazish bo‘yicha amalga oshirilgan tadqiqot natijalarini bayon etadi. Bulutli texnologiyalar sohasida amaliyot o‘tayotgan stajyor muhandis sifatida tayyorlangan ushbu hisobot texnik rahbar tomonidan belgilangan yo‘nalishlar, jumladan, masofaviy xizmatlarning biznes operatsiyalari va mijozlar tajribasiga ta'siri, bulutli tarmoqning asosiy tamoyillari va imkoniyatlari, turli bulut xizmatlarining farqlari, bulutga o‘tishning umumiy samaradorlikka ijobiy ta'siri kabi masalalarni chuqur o‘rganishga qaratilgan.

Hisobotda NQF (Milliy Malaka Asoslari) doirasidagi A ("Muloqotni qo‘llab-quvvatlash uchun bulutli infratuzilmada qo‘llaniladigan umumiy tarmoq tamoyillarini ko‘rib chiqish"), B ("Bulutli infratuzilmada tarmoq texnologiyalarining ishlashini tushuntirish") va C ("Biznesdan foydalanish uchun bulutga asoslangan tizim uchun tarmoq yechimini loyihalash") o‘rganish maqsadlariga erishish uchun zarur bo‘lgan mezonlar batafsil yoritildi. Jumladan, bulut ichidagi tarmoq arxitekturalari, standartlar, ularning afzalliklari va cheklovlari muhokama qilindi (A.P1, A.M1, A.D1, A.P2). Shuningdek, bulutli operatsion tizimlarni masofadan optimallashtirish, ularning joylashtirilishi va masofaviy mijozlarning bulut xizmatlari bilan aloqasi tahlil etildi (B.M2, B.P3, B.P4). Hisobotning amaliy qismida kompaniya ehtiyojlaridan kelib chiqqan holda Heroku kabi PaaS platformasining tarmoq tamoyillari o‘rganildi va asosiy tizimlar uchun maxsus bulutga asoslangan tarmoq yechimi loyihalanib, uni amalga oshirish, sinovdan o‘tkazish va samaradorligini asoslash bo‘yicha tavsiyalar berildi.

Ushbu tadqiqot natijalari kompaniya rahbariyatiga ERP, CRM va WMS tizimlarini bulut muhitiga ko‘chirish bo‘yicha asoslangan strategik qaror qabul qilishda yordam berishi ko‘zda tutilgan. Hisobot akademik uslubda, uchinchi shaxsda bayon etilgan bo‘lib, tegishli manbalarga (Dutt, 2019; Kurose va Ross, 2016; Stallings, 2015) tayangan holda tayyorlandi.

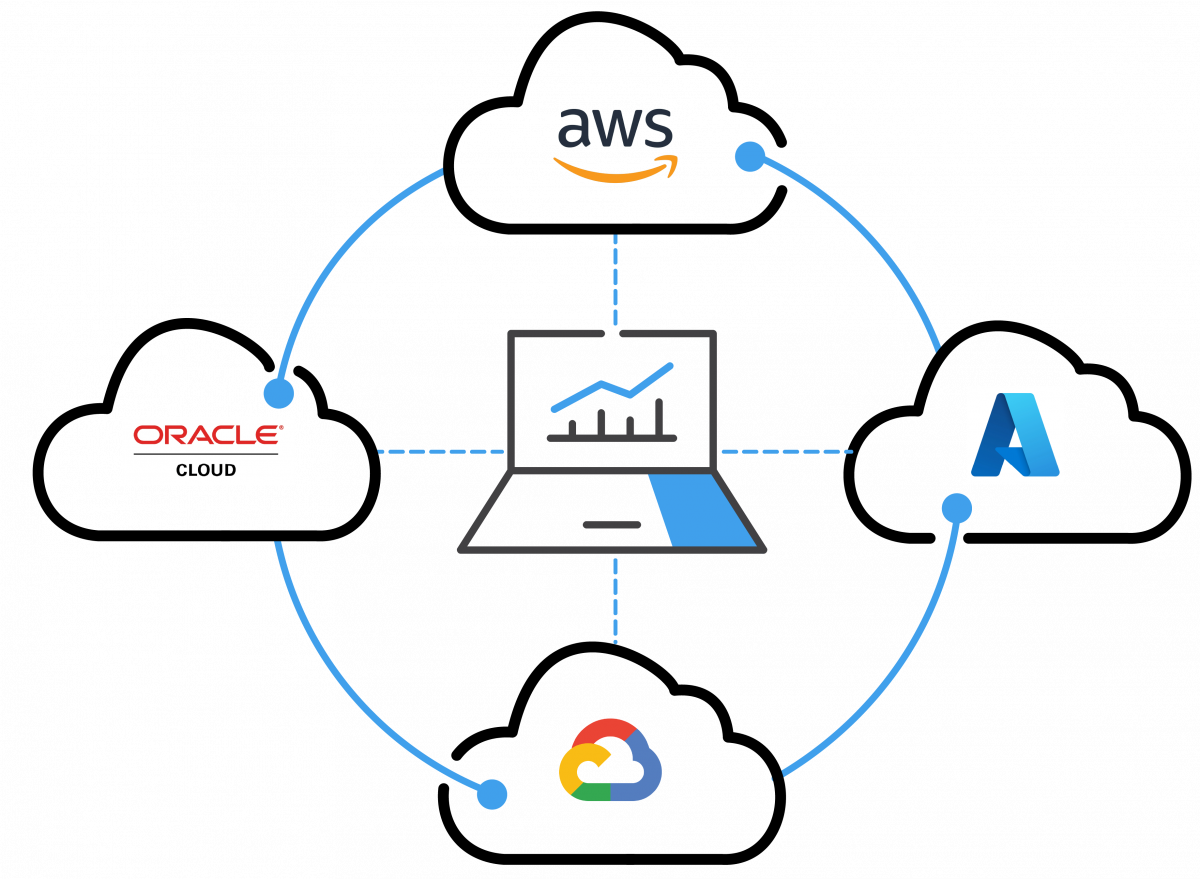
A.P1

**Bulut ichidagi turli tarmoq arxitekturalari va standartlarining afzallik-lari va cheklovlarini muhokama qiling.**

1.1 - rasm

Kompaniyaning tayyor kiyim-kechak mahsulotlarini ulgurji yetkazib berish faoliyatida ERP (Korxona resurslarini rejalashtirish), CRM (Mijozlar bilan munosabatlarni boshqarish) va WMS (Omborlarni boshqarish tizimi) kabi muhim tizimlarning uzluksiz va samarali ishlashi strategik ahamiyatga ega. Ushbu tizimlarni bulut muhitiga ko‘chirish jarayonida tarmoq arxitekturasi va standartlarini to‘g‘ri tanlash nafaqat texnik muvaffaqiyatni, balki biznes operatsiyalarining optimallashtirilishini ham ta’minlaydi. Bulutli tarmoq arxitekturalari an'anaviy lokal tarmoqlardan farqli o‘laroq, yuqori darajada moslashuvchanlik, masshtablanuvchanlik va global kirish imkoniyatlarini taqdim etadi. Biroq, har bir arxitektura va standart o‘zining afzalliklari bilan birga ma'lum cheklovlarga ham ega bo‘lib, ularni kompaniya ehtiyojlari nuqtai nazaridan sinchkovlik bilan baholash lozim.

Birinchi navbatda, Virtual Xususiy Bulut (Virtual Private Cloud - VPC) arxitekturasi ko‘rib chiqiladi. VPC ommaviy bulut provayderi infratuzilmasida yaratilgan, ammo logik jihatdan ajratilgan xususiy tarmoq muhitidir. Uning asosiy afzalliklaridan biri – yuqori darajadagi xavfsizlik va izolyatsiya. Kompaniyaning tijorat sirlari, mijozlar ma'lumotlari va moliyaviy axborotlari kabi maxfiy ma'lumotlarni himoyalashda VPC muhim rol o‘ynaydi, chunki u trafikni boshqa foydalanuvchilar trafikidan ajratib turadi. Shuningdek, VPC tarmoq konfiguratsiyasi, IP manzillar diapazoni, marshrutlash jadvallari va tarmoq shlyuzlari ustidan to‘liq nazoratni taqdim etadi. Bu esa, ERP va WMS kabi murakkab tizimlarning o‘ziga xos tarmoq talablariga moslashish imkonini beradi. Biroq, VPC ning ba'zi cheklovlari ham mavjud. Misol uchun, uni sozlash va boshqarish an'anaviy virtual tarmoqlarga qaraganda murakkabroq bo‘lishi mumkin, bu esa qo‘shimcha texnik ekspertizani talab etadi. Bundan tashqari, yuqori darajadagi nazorat va xavfsizlik ba'zan qo‘shimcha xarajatlar bilan birga kelishi mumkin, ayniqsa trafik hajmi katta bo‘lganda. Ayrim hollarda, ma'lum bir bulut provayderining VPC yechimiga bog‘lanib qolish (vendor lock-in) xavfi ham yuzaga kelishi mumkin.

Ikkinchi muhim arxitektura – bu Gibrid Bulut (Hybrid Cloud) tarmoq infratuzilmasidir. Gibrid bulut kompaniyaning mavjud lokal infratuzilmasi (private cloud) bilan bir yoki bir nechta ommaviy bulut (public cloud) xizmatlarini integratsiyalashgan holda ishlatish imkonini beradi. Bu yondashuvning asosiy afzalligi – moslashuvchanlik. Masalan, kompaniyaning o‘ta maxfiy ma'lumotlarini o‘zining xususiy serverlarida saqlab, CRM tizimining mijozlarga xizmat ko‘rsatish moduli kabi resurs talabchan va global kirishni talab qiluvchi qismlarini ommaviy bulutda joylashtirish mumkin. Bu, shuningdek, xarajatlarni optimallashtirishga yordam beradi, chunki faqat zarur bo‘lgan resurslar uchun ommaviy bulutdan foydalaniladi. Mavjud infratuzilmaga kiritilgan investitsiyalarni saqlab qolish imkoniyati ham gibrid bulutning muhim yutug‘idir. Cheklovlariga kelsak, gibrid bulutni boshqarish va integratsiya qilish yuqori darajadagi murakkablikka ega. Lokal va ommaviy bulutlar o‘rtasida ma'lumotlar va ilovalarning uzluksiz va xavfsiz harakatini ta'minlash uchun maxsus texnologiyalar va malakali mutaxassislar kerak bo‘ladi. Turli platformalar o‘rtasidagi muvofiqlik muammolari va potentsial xavfsizlik bo‘shliqlari ham e'tibor talab qiladigan jihatlardir.

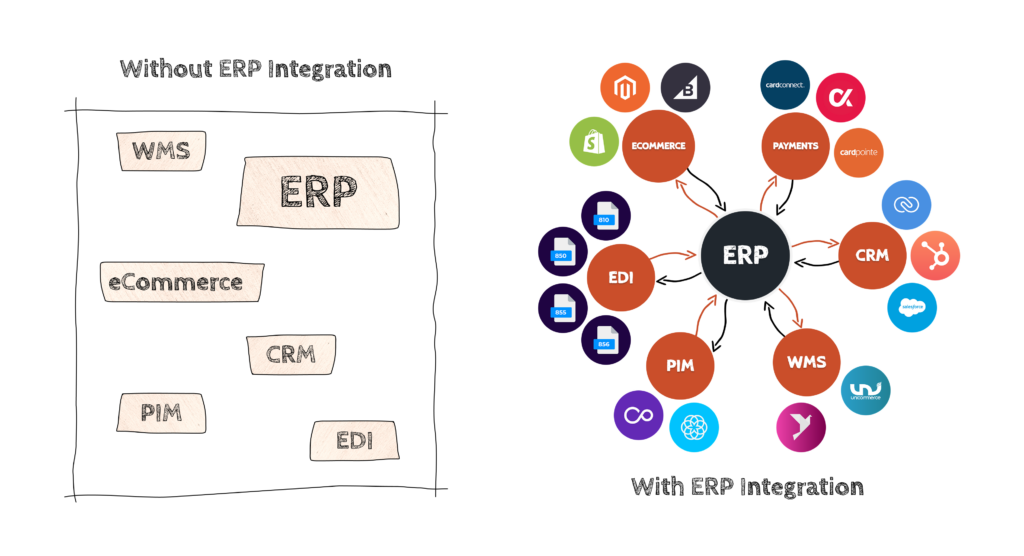
1.2 – rasm

Uchinchi arxitektura turi – Ko‘p Bulutli (Multi-Cloud) yondashuvdir. Bu strategiya bir nechta turli bulut provayderlarining xizmatlaridan bir vaqtning o‘zida foydalanishni nazarda tutadi. Asosiy afzalliklardan biri – provayderga bog‘lanib qolish xavfining kamayishi. Agar bir provayderning xizmatlari yoki narxlari qoniqarsiz bo‘lib qolsa, boshqasiga o‘tish yoki yuklamani taqsimlash imkoniyati mavjud bo‘ladi. Shuningdek, har bir vazifa uchun eng mos keladigan (narx, funksionallik, geografik joylashuv bo‘yicha) bulut xizmatini tanlash orqali optimallashtirishga erishish mumkin. Misol uchun, ERP tizimining ma'lumotlar bazasi bir provayderda, tahliliy moduli esa boshqa, ixtisoslashgan provayderda joylashishi mumkin. Bu, shuningdek, uzluksizlikni ta'minlashda (disaster recovery) qo‘l keladi. Biroq, ko‘p bulutli muhitni boshqarish gibrid bulutga qaraganda ham murakkabroq bo‘lishi mumkin. Turli provayderlarning interfeyslari, API'lari va xavfsizlik siyosatlari o‘rtasidagi farqlar integratsiya va boshqaruvni qiyinlashtiradi. Xizmatlar o‘rtasida ma'lumotlar almashinuvi va sinxronizatsiyasi ham alohida e'tiborni talab qiladi. Xavfsizlikni ta'minlash ham yanada murakkablashadi, chunki har bir bulut platformasining o‘ziga xos xavfsizlik mexanizmlarini hisobga olish kerak.

Bulutli tarmoq arxitekturalarining samarali ishlashi ko‘p jihatdan tarmoq standartlariga bog‘liq. TCP/IP (Transmission Control Protocol/Internet Protocol) to‘plami bulutli hisoblash uchun fundamental asos bo‘lib xizmat qiladi. Uning universalligi va ishonchliligi internet orqali ma'lumotlar almashinuvini ta'minlaydi, bu esa ERP, CRM va WMS kabi tizimlarning masofaviy foydalanuvchilar uchun ochiq bo‘lishini kafolatlaydi. Biroq, TCP/IP ning o‘zi bulut muhitining dinamik talablariga, masalan, virtual mashinalarning tezkor migratsiyasiga yoki resurslarning avtomatik masshtablanishiga to‘liq javob bera olmasligi mumkin, shuning uchun u ko‘pincha virtualizatsiya texnologiyalari bilan birga qo‘llaniladi.

Virtual Ethernet standartlari bulutdagi virtual mashinalar va konteynerlar o‘rtasidagi aloqani ta'minlashda muhimdir. Ular jismoniy Ethernet tarmog‘ining funksionalligini virtual muhitda takrorlaydi, bu esa moslashuvchanlik va xarajatlarni tejash imkonini beradi. Virtual kommutatorlar (virtual switches) yordamida virtual mashinalar o‘rtasida trafikni samarali boshqarish mumkin. Cheklovlariga kelsak, juda katta miqyosdagi virtual tarmoqlarda masshtablanuvchanlik va boshqaruv muammolari yuzaga kelishi mumkin.

MPLS (Multiprotocol Label Switching) standarti, ayniqsa, gibrid bulut senariylarida, kompaniyaning lokal tarmog‘i va ommaviy bulut o‘rtasida xavfsiz va yuqori sifatli (QoS - Quality of Service) ulanishni ta'minlash uchun qo‘llanilishi mumkin. MPLS trafikni belgilarga (labels) asoslanib marshrutlash orqali samaradorlik va xavfsizlikni oshiradi. Biroq, MPLS ni sozlash va boshqarish murakkab va qimmat bo‘lishi mumkin, va u bulutga xos bo‘lgan ba'zi yangi, yanada moslashuvchan tarmoq texnologiyalariga nisbatan kamroq chaqqonlikka ega.

So‘nggi yillarda Dasturiy Ta'minot Orqali Belgilanadigan Tarmoqlar (Software-Defined Networking - SDN) va Tarmoq Funksiyalarini Virtualizatsiyalash (Network Functions Virtualization - NFV) kabi yangi standartlar va yondashuvlar bulutli tarmoqlarda inqilob qildi. SDN tarmoq boshqaruvini jismoniy qurilmalardan ajratib, markazlashtirilgan dasturiy kontroler orqali boshqarish imkonini beradi. Bu avtomatlashtirish, moslashuvchanlik va resurslardan samarali foydalanishni ta'minlaydi. Masalan, kompaniyaning ERP tizimi yuklamasi oshganda, SDN avtomatik ravishda qo‘shimcha tarmoq resurslarini ajratishi mumkin. NFV esa an'anaviy apparatli tarmoq qurilmalari (masalan, firewall, load balancer) funksiyalarini virtual mashinalarda dasturiy ta'minot sifatida ishga tushirishga imkon beradi. Bu xarajatlarni kamaytirish, xizmatlarni tezkor joylashtirish va masshtablanuvchanlikni oshiradi. Biroq, SDN va NFV ni joriy etish murakkablik, kontroler xavfsizligi va turli ishlab chiqaruvchilar yechimlari o‘rtasidagi muvofiqlik masalalari kabi qiyinchiliklarga ega bo‘lishi mumkin.

1.3 – rasm

Kompaniya uchun ERP, CRM va WMS tizimlarini bulutga ko‘chirishda tarmoq arxitekturasi va standartlarini tanlash ko‘p qirrali masaladir. VPC, gibrid yoki ko‘p bulutli yondashuvlardan birini tanlash, shuningdek, TCP/IP, SDN, NFV kabi standartlarning imkoniyatlari va cheklovlarini chuqur tushunish, kelajakdagi infratuzilmaning ishonchliligi, xavfsizligi, samaradorligi va umumiy qiymatini belgilab beradi. Har bir variantning afzalliklari va kamchiliklarini kompaniyaning o‘ziga xos biznes ehtiyojlari, byudjeti va texnik salohiyati bilan muvozanatlash orqali eng maqbul strategik qarorni qabul qilish mumkin.

A.P2

**Bulut ichida tarmoq aloqasi qanday ishlashini tasvirlab bering.**

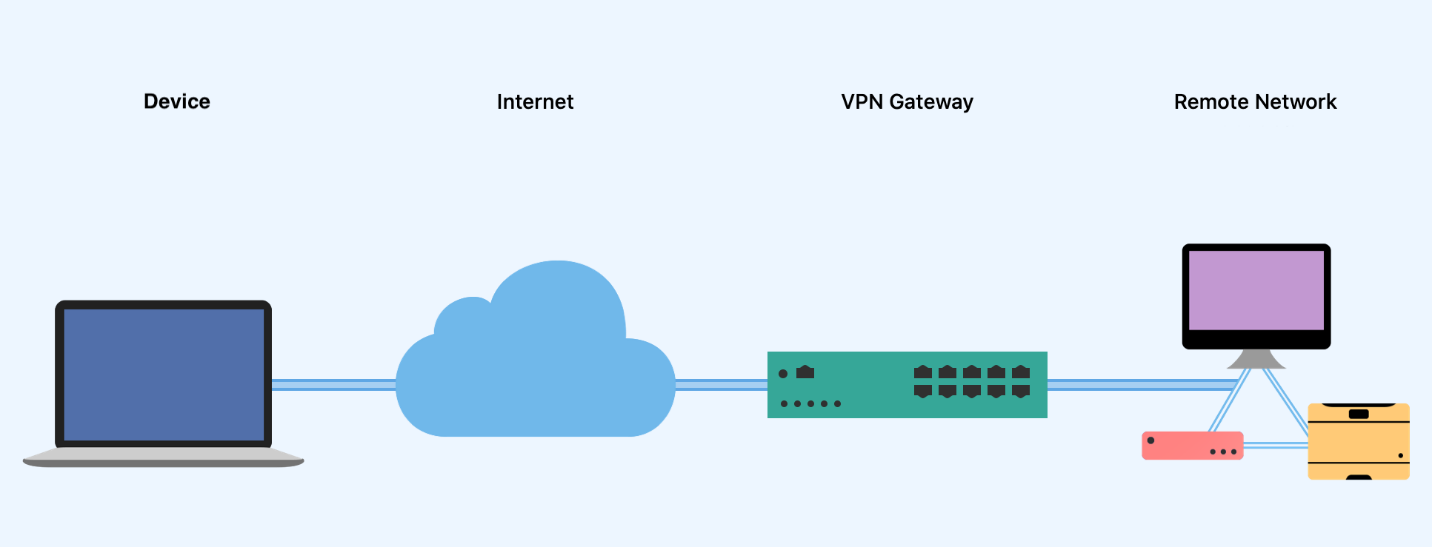
Bulut ichidagi tarmoq aloqasi an'anaviy lokal tarmoqlardagi aloqa tamoyillariga asoslangan bo‘lsa-da, virtualizatsiya va dasturiy ta'minot orqali boshqarish texnologiyalari tufayli o‘ziga xos xususiyatlarga ega. Kompaniyaning ERP, CRM va WMS tizimlari bulut muhitiga joylashtirilganda, ularning komponentlari va foydalanuvchilar o‘rtasidagi aloqa bir necha asosiy konsepsiyalar va mexanizmlar orqali amalga oshiriladi.

Markaziy o‘rinni **Virtual Tarmoqlar** egallaydi. Ko‘pgina bulut provayderlari (masalan, AWS da Virtual Private Cloud - VPC, Azure da Virtual Network - VNet, Google Cloud da VPC Network) foydalanuvchilarga ommaviy bulut infratuzilmasida logik jihatdan izolyatsiyalangan shaxsiy tarmoq segmentlarini yaratish imkonini beradi. Kompaniya uchun ERP, CRM va WMS tizimlarining har biri yoki ularning umumiy guruhi uchun alohida virtual tarmoq yaratilishi mumkin. Bu virtual tarmoqlar o‘zlarining IP manzillar diapazoniga, **kichik tarmoqlarga (subnets)**, **marshrutlash jadvallariga (routing tables)** va **xavfsizlik qoidalariga (security groups yoki network security groups - NSGs)** ega bo‘ladi.

Virtual mashinalar (masalan, ERP dastur serveri yoki CRM ma'lumotlar bazasi serveri) ushbu kichik tarmoqlarga joylashtiriladi. Bir kichik tarmoq ichidagi virtual mashinalar odatda bir-biri bilan to‘g‘ridan-to‘g‘ri, past kechikish bilan aloqa qila oladi. Turli kichik tarmoqlar o‘rtasidagi aloqa esa marshrutlash jadvallari orqali boshqariladi. Masalan, CRM tizimining veb-serveri (bir kichik tarmoqda) va uning ma'lumotlar bazasi serveri (boshqa, xavfsizroq kichik tarmoqda) o‘rtasidagi aloqaga faqat ma'lum portlar orqali ruxsat berilishi mumkin.

Virtual mashinalar jismoniy serverlarda (hostlarda) ishlaydi va har bir hostda **virtual kommutator (virtual switch yoki vSwitch)** mavjud bo‘ladi. Bu virtual kommutator xuddi jismoniy kommutator kabi bir xil hostdagi virtual mashinalar o‘rtasidagi trafikni yoki virtual mashinalar va jismoniy tarmoq adapteri o‘rtasidagi trafikni yo‘naltiradi. Bu jarayon virtual mashinalarning bir-biridan izolyatsiyalangan holda ishlashini va bir vaqtning o‘zida bir nechta turli virtual tarmoqlarga ulanishini ta'minlaydi.

Foydalanuvchilar yoki boshqa tizimlar tomonidan ERP, CRM yoki WMS xizmatlariga kelayotgan tashqi trafik odatda **Internet Shlyuzi (Internet Gateway)** orqali virtual tarmoqqa kiradi. Xizmatlarning uzluksiz ishlashini ta'minlash va yuklamani bir nechta server nusxalari (instansiyalari) o‘rtasida taqsimlash uchun **Yuklama Taqqsimlagichlar (Load Balancers)** ishlatiladi. Masalan, Kompaniyaning CRM portaliga ko‘plab mijozlar bir vaqtda murojaat qilganda, yuklama taqsimlagich so‘rovlarni bir nechta veb-server instansiyalari o‘rtasida teng taqsimlab, har bir serverning haddan tashqari yuklanishining oldini oladi va javob vaqtini yaxshilaydi. Yuklama taqsimlagichlar ham ichki (virtual tarmoq ichidagi trafik uchun) ham tashqi (internetdan kelayotgan trafik uchun) bo‘lishi mumkin.



1.4 – rasm

Agar kompaniya gibrid bulut strategiyasini tanlasa, ya'ni ba'zi tizimlar lokal infratuzilmada qolib, ba'zilari bulutga ko‘chirilsa, lokal tarmoq va bulutdagi virtual tarmoq o‘rtasida xavfsiz aloqa kanali o‘rnatilishi kerak. Bu odatda **VPN Shlyuzi (VPN Gateway)** orqali IPsec tunnelini sozlash yoki provayderning maxsus ulanish xizmati (masalan, AWS Direct Connect, Azure ExpressRoute) orqali amalga oshiriladi. Bu WMS tizimining ombordagi lokal serverlari bilan bulutdagi markaziy tahlil moduli o‘rtasida xavfsiz ma'lumot almashinuvini ta'minlashi mumkin.

Bulut ichidagi xizmatlar bir-birini topishi va aloqa o‘rnatishi uchun **DNS (Domain Name System)** muhim rol o‘ynaydi. Bulut provayderlari odatda ichki (private) DNS xizmatlarini taklif qiladi, bu esa virtual tarmoq ichidagi resurslarga (masalan, erp-db-server.internal-domain) oson esda qoladigan nomlar orqali murojaat qilish imkonini beradi, ularning IP manzillari o‘zgarganda ham. Tashqi dunyo uchun esa ommaviy DNS yozuvlari ishlatiladi (masalan, crm.kompaniyanomi.uz).

Shuningdek, bulutda turli darajadagi xizmatlar (IaaS, PaaS, SaaS) o‘rtasida ham tarmoq aloqasi mavjud. Masalan, IaaS da joylashgan ERP dastur serveri PaaS sifatida taqdim etilgan ma'lumotlar bazasi xizmatiga (masalan, AWS RDS yoki Azure SQL Database) ulanishi mumkin. Bunday ulanishlar odatda provayderning yuqori tezlikdagi ichki tarmog‘i (backbone network) orqali amalga oshiriladi va xavfsizlik uchun maxsus ulanish nuqtalari (endpoints) yoki xizmatlar o‘rtasidagi ishonchli aloqa (service linking) mexanizmlari qo‘llaniladi.

Bundan tashqari, bulut ichidagi tarmoq aloqasi virtualizatsiya, dasturiy ta'minot orqali boshqarish, avtomatlashtirilgan xavfsizlik va marshrutlash qoidalari, shuningdek, yuklama taqsimlash va DNS kabi asosiy xizmatlarning murakkab, ammo samarali majmuasiga tayanadi. Bu Kompaniyaning ERP, CRM va WMS tizimlarining bulut muhitida ishonchli, xavfsiz va masshtablanuvchan tarzda ishlashini ta'minlash uchun poydevor yaratadi.

A.M1

**Umumiy tarmoq standartlari va ular bulutli hisoblashni qanday osonlashtirishini solishtiring.**

1.5 – rasm

Kompaniyaning ERP, CRM va WMS kabi muhim axborot tizimlarini bulut muhitiga samarali ko‘chirishda umumiy tarmoq standartlari hal qiluvchi rol o‘ynaydi. Bu standartlar moslashuvchanlik, masshtablanuvchanlik va resurslardan umumiy foydalanish kabi bulutli hisoblashning asosiy tamoyillarini qo‘llab-quvvatlab, turli qurilmalar va texnologiyalar o‘rtasida o‘zaro muvofiqlikni ta’minlaydi.

Ethernet (IEEE 802.3) standarti, dastlab lokal tarmoqlar uchun yaratilgan bo‘lsa-da, hozirda bulutli ma’lumotlar markazlarining asosiy tarmoq texnologiyasidir. Uning yuqori tezlikda ma’lumot uzatish imkoniyati (masalan, 100 GbE va undan yuqori) korporativ tizimlardan keluvchi katta hajmdagi trafikni samarali uzatadi. Virtualizatsiya bilan uyg‘unligi va VLAN orqali trafikni izolyatsiyalash imkoniyati xavfsizlikni oshiradi. Biroq, an’anaviy Ethernetning STP kabi protokollarga bog‘liqligi uni ba’zi holatlarda samarasiz qiladi, shu sababli zamonaviy markazlarda TRILL yoki SPB kabi alternativalar qo‘llaniladi.

Bulutli infratuzilmaning asosiy negizini TCP/IP protokollar to‘plami tashkil qiladi. U platformadan mustaqil ishlash, keng qamrov va ishonchli uzatish imkoniyatlarini ta’minlaydi. ERP, CRM va WMS kabi tizimlarga global kirishni ta’minlab, marshrutlash, xavfsizlik devorlari va yuklamani taqsimlash kabi funksiyalarni amalga oshiradi. Shuningdek, ko‘plab bulut xizmatlarining API chaqiruvlari aynan TCP/IP orqali bajariladi. Shu bilan birga, TCP protokolining ortiqcha "xizmatchi" ma’lumotlari real vaqt rejimida ishlovchi ilovalar samaradorligini pasaytirishi mumkin. IPv4 manzillarining chegaralanganligi esa NAT kabi qo‘shimcha mexanizmlarni talab qiladi, bu esa konfiguratsiyani murakkablashtiradi; IPv6 esa bu muammoni bartaraf etishga xizmat qiladi.

HTTP va HTTPS protokollari vebga asoslangan xizmatlar uchun asosiy tarmoq standartlari hisoblanadi. CRM va boshqa tizimlarning veb-interfeyslari, shuningdek, SaaS modelidagi bulut xizmatlari aynan shu protokollar orqali ishlaydi. HTTPS ma’lumotlarni shifrlash orqali uzatish xavfsizligini ta’minlaydi. RESTful API va boshqa xizmatlar ham aynan HTTP/HTTPS orqali ishlaydi. Biroq, HTTP protokoli holatsiz bo‘lgani sababli, seansni boshqarish uchun qo‘shimcha mexanizmlarni talab qiladi, shuningdek, doimiy ulanishni talab qiluvchi ilovalar uchun cheklovlarga ega.

DNS standarti foydalanuvchi uchun qulay domen nomlarini IP manzillarga aylantirib, xizmatlarga barqaror kirishni ta’minlaydi. DNS xizmatlari global marshrutlash, yuklamani taqsimlash va uzluksizlikni qo‘llab-quvvatlaydi. Shu bilan birga, DNS so‘rovlarining tarqalishdagi kechikishlari va tizimning kiberhujumlarga ochiqligi muayyan xavflarni yuzaga keltiradi.

VPN texnologiyalari (masalan, IPsec yoki SSL/TLS) kompaniyaning lokal tarmog‘i va bulutdagi resurslari o‘rtasida shifrlangan aloqa kanalini yaratishga xizmat qiladi. Bu, ayniqsa, ichki tizimlarga masofaviy xavfsiz kirishni ta’minlashda muhimdir. VPN texnologiyasi orqali kompaniya o‘z xavfsizlik siyosatini bulut muhitiga kengaytira oladi. Biroq, u qo‘shimcha kechikishlar va o‘tkazuvchanlik cheklovlariga olib kelishi mumkin, shuningdek, VPN shlyuzlarini boshqarish texnik ko‘nikmalarni talab qiladi.

REST va GraphQL kabi API standartlari turli xizmatlar o‘rtasida samarali integratsiyani ta’minlaydi. REST, HTTP metodlari orqali oddiy interfeys yaratib, tizim modullari o‘rtasida ma’lumot almashuvini osonlashtiradi. GraphQL esa tarmoq resurslarini tejashga va faqat kerakli ma’lumotlarni olishga imkon yaratadi. Shu bilan birga, noto‘g‘ri loyihalashtirilgan API’lar xavfsizlik va samaradorlik muammolariga olib kelishi mumkin.

Xulosa qilib aytganda, yuqoridagi standartlar kompaniyaning bulut strategiyasi doirasida ERP, CRM va WMS kabi tizimlarning barqaror va xavfsiz ishlashi, o‘zaro integratsiyasi hamda kengaytirilishiga xizmat qiladi. Har bir standartning imkoniyatlari va cheklovlari kompaniya ehtiyojlari doirasida baholanib, eng mos tarmoq yechimlari tanlab olinadi.

A.D1

**Bulutli muhitni yaratish tarmoqni amalga oshirish va umumiy ishlashga qanday ta'sir qilishini ko'rib chiqing.**

Kompaniyaning ERP, CRM va WMS kabi tizimlarini an'anaviy lokal infratuzilmadan bulutli muhitga o‘tkazish qarori tarmoqni amalga oshirish (network implementation) jarayonlariga ham, tizimlarning umumiy ishlash samaradorligiga (overall performance) ham fundamental ta'sir ko‘rsatadi. Bulutli muhit o‘zining tabiatiga ko‘ra tarmoq resurslariga yangicha yondashuvni taqozo etadi, bu esa ham imkoniyatlar, ham muayyan qiyinchiliklarni keltirib chiqaradi.

Tarmoqni amalga oshirishga ta'siri:

Bulutli muhitni yaratish, avvalambor, tarmoqni jismoniy qurilmalarga bog‘liqlikdan xalos qiladi. An'anaviy yondashuvda yangi server yoki xizmat uchun tarmoqni sozlash kabellarni ulash, kommutator portlarini sozlash va marshrutizatorlarni qayta dasturlash kabi ko‘p vaqt talab qiladigan jismoniy ishlarni o‘z ichiga olgan bo‘lsa, bulutda bu jarayonlar asosan dasturiy ta'minot orqali virtual tarzda amalga oshiriladi. Virtual Xususiy Bulut (VPC) yoki Virtual Tarmoq (VNet) kabi texnologiyalar yordamida bir necha daqiqada murakkab tarmoq topologiyalarini yaratish, o‘zgartirish va o‘chirish mumkin. Bu kompaniya uchun yangi filial ochilganda yoki mavsumiy yuklamalar uchun qo‘shimcha ERP modullarini tezda ishga tushirish kerak bo‘lganda misli ko‘rilmagan chaqqonlik (agility) va tezkorlikni (speed of deployment) ta'minlaydi.

Ikkinchidan, bulutli muhit markazlashtirilgan boshqaruv va avtomatlashtirish imkoniyatlarini kengaytiradi. Bulut provayderlari odatda tarmoq resurslarini boshqarish uchun qulay veb-interfeyslar va API'lar taqdim etadi. Dasturiy Ta'minot Orqali Belgilanadigan Tarmoqlar (SDN) konsepsiyasi bulutda keng qo‘llanilib, tarmoq konfiguratsiyasi, xavfsizlik siyosatlari va trafikni boshqarish kabi vazifalarni avtomatlashtirishga imkon beradi. Masalan, WMS tizimida ombordagi tovarlar harakati intensivlashganda, tarmoq resurslari avtomatik ravishda kengaytirilib, uzluksiz ishlash ta'minlanishi mumkin. Bu esa, o‘z navbatida, IT xodimlarining qo‘l mehnatini kamaytirib, ularning strategik vazifalarga e'tibor qaratishiga imkon yaratadi. Biroq, bu yangi boshqaruv vositalari va avtomatlashtirish skriptlarini o‘zlashtirish uchun IT mutaxassislaridan yangi bilim va ko‘nikmalar talab qilinadi.



1.6-rasm

Uchinchidan, tarmoq xavfsizligi modeli o‘zgaradi. An'anaviy "qal'a va xandaq" (castle-and-moat) uslubidagi perimetr xavfsizligi bulut muhitida yetarli bo‘lmay qoladi. Buning o‘rniga mikro-segmentatsiya va nolga ishonch (zero-trust) kabi yondashuvlar dolzarblashadi. Mikro-segmentatsiya orqali ERP, CRM va WMS tizimlarining har bir komponenti yoki hatto alohida virtual mashinalar o‘zlarining kichik, izolyatsiyalangan tarmoq segmentlariga joylashtirilib, ular o‘rtasidagi trafik qat'iy nazorat qilinadi. Bu, agar biror komponent komprometatsiya qilinsa, hujumning butun tizimga tarqalishining oldini olishga yordam beradi. Biroq, bunday granulyar xavfsizlik siyosatlarini ishlab chiqish va boshqarish murakkabroq bo‘lishi mumkin.

Umumiy ishlashga ta'siri:

Bulutli muhitning umumiy ishlashga birinchi va eng muhim ijobiy ta'siri – bu masshtablanuvchanlik (scalability) va elastiklik (elasticity). Kompaniyaning ulgurji savdo faoliyatida, masalan, bayramlar arafasida yoki yangi kolleksiya chiqqanda CRM tizimiga murojaatlar soni yoki ERP tizimidagi tranzaksiyalar hajmi keskin oshishi mumkin. Bulutli muhitda bunday yuklamalarga javoban hisoblash va tarmoq resurslarini avtomatik yoki qo‘lda tezda oshirish imkoniyati mavjud. Aksincha, yuklama kamayganda resurslarni qisqartirib, xarajatlarni optimallashtirish mumkin. Bu an'anaviy infratuzilmada deyarli imkonsiz bo‘lgan dinamiklikni ta'minlaydi.

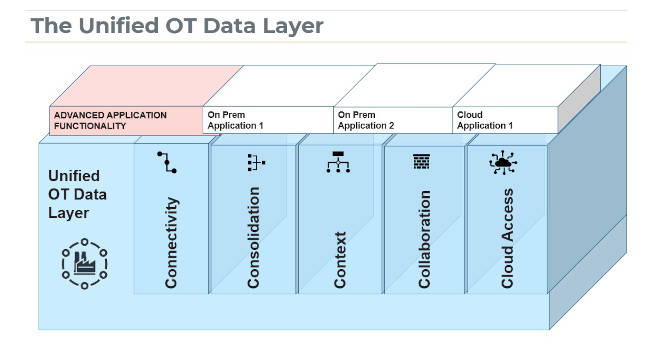
Ikkinchidan, kechikish (latency) masalasi muhim ahamiyat kasb etadi. Agar kompaniyaning mijozlari yoki xodimlari geografik jihatdan tarqoq bo‘lsa, bulut provayderining turli mintaqalarda joylashgan ma'lumotlar markazlaridan foydalanish orqali xizmatlarni foydalanuvchilarga yaqinlashtirish va shu bilan kechikishni kamaytirish mumkin. Masalan, CRM tizimining mijozlar portali eng yaqin serverdan yuklanishi uning tezroq ishlashini ta'minlaydi. Biroq, agar kompaniyaning asosiy operatsiyalari va bulutdagi serverlar o‘rtasidagi masofa katta bo‘lsa yoki internet ulanishi sifatsiz bo‘lsa, bu ERP va WMS kabi real vaqt rejimida ishlaydigan tizimlar uchun unumdorlik muammolarini keltirib chiqarishi mumkin. Bunday hollarda, WAN (Wide Area Network) optimallashtirish texnologiyalari yoki provayderning maxsus ulanish xizmatlari (masalan, AWS Direct Connect, Azure ExpressRoute) ko‘rib chiqilishi kerak.

Uchinchidan, o‘tkazuvchanlik qobiliyati (bandwidth) boshqaruvi ham o‘zgaradi. Bulutga ko‘chish bilan kompaniyaning internet kanaliga bo‘lgan talab ortadi, chunki barcha tizimlar (ERP, CRM, WMS) endi tashqi tarmoq orqali ishlaydi. Agar o‘tkazuvchanlik yetarli bo‘lmasa, bu "tor bo‘g‘iz" (bottleneck) hosil qilib, tizimlarning sekin ishlashiga olib kelishi mumkin. Bulut provayderlari odatda yuqori o‘tkazuvchanlikka ega tarmoqlarni taklif qilishadi, ammo kompaniyaning o‘zining internet ulanishi ham shunga mos bo‘lishi kerak. Shuningdek, bulutdagi tarmoq trafikining narxlanishi (ayniqsa, ma'lumotlarni bulutdan tashqariga chiqarish – data egress) xarajatlarga ta'sir qiluvchi omil bo‘lishi mumkin va buni byudjetlashtirishda hisobga olish zarur.

To‘rtinchidan, ishonchlilik (reliability) va mavjudlik (availability) darajasi odatda bulut provayderlari tomonidan Xizmat Ko‘rsatish Darajasi Kelishuvi (SLA - Service Level Agreement) orqali kafolatlanadi. Ko‘pgina provayderlar yuqori darajadagi (masalan, 99.9% yoki 99.99%) mavjudlikni taklif qilishadi, bu esa kompaniyaning ERP, CRM va WMS tizimlarining uzluksiz ishlashi uchun muhimdir. Bulutdagi ortiqchalik (redundancy) va nosozliklarga chidamlilik (fault tolerance) mexanizmlari, masalan, bir nechta mavjudlik zonalarida (Availability Zones) resurslarni joylashtirish, an'anaviy infratuzilmada erishish qiyin bo‘lgan darajada barqarorlikni ta'minlashi mumkin. Biroq, SLA shartlarini diqqat bilan o‘rganish va provayderga to‘liq bog‘lanib qolish xavfini ham baholash kerak.

Shuingdek, bulutli muhitni yaratish tarmoqni amalga oshirishni ancha soddalashtiradi, tezlashtiradi va avtomatlashtiradi, biroq yangi ko‘nikmalar va xavfsizlik yondashuvlarini talab etadi. Umumiy ishlash nuqtai nazaridan, bulut misli ko‘rilmagan masshtablanuvchanlik va ishonchlilikni taqdim etsa-da, kechikish, o‘tkazuvchanlik qobiliyati va xarajatlar kabi omillarni diqqat bilan boshqarish kerak. Kompaniyaning ERP, CRM va WMS tizimlari uchun bu o‘zgarishlar to‘g‘ri rejalashtirilsa, sezilarli darajada samaradorlik oshishiga va biznes operatsiyalarining yaxshilanishiga olib kelishi mumkin.

B.P3

**Masofaviy operatsion tizim xizmatlari bulut ichida qanday joylashtirilishini tushuntiring.**

2.1 - rasm

Masofaviy operatsion tizim (OT) xizmatlari bulut muhitida joylashgan ERP, CRM va WMS kabi tizimlarning asosini tashkil etuvchi virtual mashinalardagi OTlarni boshqarish, kuzatish, yangilash va xavfsizligini ta’minlash uchun mo‘ljallangan vositalar va jarayonlar majmuasidir. Ushbu xizmatlarning bulut ichida joylashtirilishi bir necha usulda amalga oshirilishi mumkin, bu esa kompaniyaning ehtiyojlari va texnik imkoniyatlariga bog‘liq.

Birinchi va eng keng tarqalgan usul – bu **bulut provayderi tomonidan taqdim etiladigan boshqariladigan xizmatlardan (managed services)** foydalanishdir. Aksariyat yirik bulut provayderlari (AWS, Azure, Google Cloud) OTlarni boshqarish uchun o‘zlarining integratsiyalashgan xizmatlarini taklif etadilar. Masalan:

**Yangilanishlarni boshqarish (Patch Management):** AWS Systems Manager Patch Manager yoki Azure Update Management kabi xizmatlar OT uchun xavfsizlik yangilanishlari va boshqa tuzatishlarni avtomatik ravishda yoki reja asosida o‘rnatish imkonini beradi. Bu xizmatlar markazlashtirilgan holda barcha virtual mashinalarga (masalan, ERP tizimining barcha serverlariga) yangilanishlarni tarqatadi va ularning muvaffaqiyatli o‘rnatilganligini kuzatib boradi.

**Konfiguratsiyani boshqarish (Configuration Management):** AWS OpsWorks (Chef va Puppet asosida) yoki Azure Automation State Configuration (PowerShell DSC asosida) kabi xizmatlar OT konfiguratsiyalarini (masalan, zarur dasturiy ta'minot o‘rnatilganligi, xavfsizlik sozlamalari to‘g‘riligi) belgilangan holatda saqlashga yordam beradi. Agar biror WMS serverining konfiguratsiyasi belgilangan standartdan chetga chiqsa, bu xizmatlar uni avtomatik ravishda tuzatishi mumkin.

**Monitoring va Loglash (Monitoring and Logging):** Amazon CloudWatch, Azure Monitor yoki Google Cloud's operations suite kabi xizmatlar OTning unumdorlik ko‘rsatkichlarini (CPU, xotira, disk, tarmoq) yig‘adi, log fayllarini markazlashtirilgan holda saqlaydi va muayyan hodisalar (masalan, CRM serverida xotira yetishmasligi) yuzaga kelganda ogohlantirishlar (alerts) yuboradi.

**Masofaviy kirish (Remote Access):** Provayderlar odatda SSH (Linux uchun) yoki RDP (Windows uchun) orqali virtual mashinalarga xavfsiz masofaviy kirish imkoniyatini ta'minlaydi. Ba'zi hollarda, brauzer orqali sessiya menejerlari (masalan, AWS Systems Manager Session Manager) ham taklif etiladi, bu esa ochiq portlarga ehtiyojni kamaytiradi va xavfsizlikni oshiradi.

Bu boshqariladigan xizmatlar odatda bulut platformasining o‘zida, provayder infratuzilmasida joylashadi va foydalanuvchining virtual tarmog‘idagi agentlar yoki API chaqiruvlari orqali virtual mashinalar bilan o‘zaro aloqada bo‘ladi. Ulardan foydalanish infratuzilmani boshqarish yukini kamaytiradi va ko‘plab vazifalarni avtomatlashtiradi.

Ikkinchi usul – bu **uchinchi tomon dasturiy ta'minotini (third-party software) bulutdagi virtual mashinalarda joylashtirishdir.** Kompaniya o‘ziga ma'qul kelgan konfiguratsiyani boshqarish vositalarini (masalan, Ansible serveri, Puppet master), monitoring tizimlarini (masalan, Nagios, Zabbix) yoki loglarni boshqarish platformalarini (masalan, ELK stack – Elasticsearch, Logstash, Kibana) o‘zining virtual tarmog‘i ichidagi alohida virtual mashinalarga o‘rnatishi va sozlab olishi mumkin. Bu yondashuv ko‘proq moslashuvchanlik va nazoratni ta'minlaydi, ammo bu xizmatlarni o‘rnatish, sozlash va ularga xizmat ko‘rsatish mas'uliyati kompaniyaning IT jamoasi zimmasiga tushadi. Masalan, ERP tizimining barcha serverlaridagi OTlarni boshqarish uchun alohida Ansible boshqaruv serveri sozlanishi mumkin.

Uchinchi yondashuv – bu **konteynerlashtirilgan xizmatlardan foydalanishdir.** Ba'zi masofaviy OT boshqaruv vositalari yoki ularning komponentlari Docker kabi konteynerlarda ishga tushirilishi va Kubernetes kabi konteyner orkestratsiyasi platformalarida joylashtirilishi mumkin. Bu yondashuv masshtablanuvchanlik va portativlikni oshiradi. Masalan, WMS tizimining mikroxizmatlarini monitoring qilish uchun Prometheus va Grafana kabi vositalar konteynerlarda joylashtirilishi mumkin.

Bu xizmatlarning barchasi, qaysi usulda joylashtirilishidan qat'i nazar, bulutdagi virtual mashinalarda ishlayotgan OTlar bilan tarmoq orqali aloqa qiladi. Bu aloqa odatda xavfsiz protokollar (HTTPS, SSH) orqali amalga oshiriladi va kirishni nazorat qilish uchun xavfsizlik guruhlari (security groups), tarmoq kirishni boshqarish ro‘yxatlari (network ACLs) va IAM (Identity and Access Management) rollari kabi mexanizmlardan foydalaniladi.

Shunday qilib, masofaviy operatsion tizim xizmatlari bulut ichida provayder tomonidan boshqariladigan integratsiyalashgan yechimlar sifatida, foydalanuvchi tomonidan o‘rnatilgan va boshqariladigan dasturiy ta'minot sifatida yoki konteynerlashtirilgan ilovalar ko‘rinishida joylashtirilishi mumkin. Tanlov kompaniyaning texnik salohiyati, nazorat talablari va byudjetiga bog‘liq bo‘lib, asosiy maqsad ERP, CRM va WMS kabi muhim tizimlarning barqaror, xavfsiz va samarali ishlashini ta'minlashdir.

B.P4

**Masofaviy mijozlar bulut xizmatlari bilan qanday aloqada bo'lishini tushuntiring**

Kompaniyaning ERP, CRM va WMS kabi tizimlari bulut muhitiga ko‘chirilgandan so‘ng, turli xil masofaviy mijozlar – kompaniya xodimlari (sotuvchilar, omborxona xodimlari, menejerlar), hamkorlar va hatto yakuniy iste'molchilar (agar tizimlar shunday funksionallikni o‘z ichiga olsa) – ushbu bulut xizmatlari bilan o‘zaro aloqada bo‘lishlari kerak bo‘ladi. Bu aloqa bir necha bosqich va texnologiyalarni o‘z ichiga oladi.

2.2 - rasm

Birinchi navbatda, mijozlar bulut xizmatlariga **kirish nuqtalari (access points)** orqali ulanadilar. Eng keng tarqalgan kirish usuli bu **internet orqali veb-brauzerdir.** Ko‘pgina zamonaviy ERP, CRM (masalan, mijozlar portali) va WMS tizimlari veb-asosli interfeyslarga ega bo‘lib, foydalanuvchilar HTTPS protokoli orqali xavfsiz ulanishni amalga oshiradilar. Foydalanuvchi brauzerida tizimning URL manzilini (masalan, https://crm.kompaniyanomi.uz) teradi, bu so‘rov DNS orqali bulutdagi xizmatning IP manziliga aylantiriladi.

Ikkinchi keng tarqalgan usul – bu **maxsus ishlab chiqilgan klient dasturlari (dedicated client applications) yoki mobil ilovalar (mobile apps)**. Ba'zi ERP yoki WMS tizimlari yanada boy funksionallik va yaxshiroq unumdorlik uchun maxsus dasturiy ta'minotni talab qilishi mumkin. Sotuv bo‘limi xodimlari CRM tizimiga planshetlaridagi mobil ilova orqali, omborxona xodimlari esa WMS ga maxsus skaner qurilmalaridagi klient dasturi orqali ulanishlari mumkin. Bu ilovalar ham odatda internet orqali, ko‘pincha API (Application Programming Interface) chaqiruvlari yordamida bulutdagi backend xizmatlari bilan aloqa qiladi.

Uchinchi usul – bu **API orqali tizimlararo integratsiya.** Kompaniyaning ERP tizimi, masalan, elektron tijorat platformasi yoki logistika hamkorining tizimi bilan ma'lumot almashishi kerak bo‘lishi mumkin. Bunday hollarda, bu tashqi tizimlar masofaviy mijoz sifatida harakat qilib, ERP tizimining bulutda joylashgan API'lariga (masalan, RESTful API yoki SOAP API) xavfsiz so‘rovlar yuboradi.

Mijoz so‘rovi bulut provayderining tarmog‘iga yetib kelgach, u bir nechta komponentlardan o‘tadi:

**Edge Network/Content Delivery Network (CDN):** Ko‘pgina bulut provayderlari global miqyosda tarqalgan edge serverlarga ega. Agar CRM portalining statik kontenti (rasmlar, CSS fayllari) CDN da keshlangan bo‘lsa, mijozga eng yaqin serverdan yetkazib beriladi, bu esa yuklanish tezligini oshiradi.

**Yuklama Taqqsimlagich (Load Balancer):** Tashqi trafik odatda yuklama taqsimlagichga kelib tushadi. U so‘rovni sog‘lom va kamroq yuklangan dastur serveri instansiyasiga (masalan, ERP ilovasi serveriga) yo‘naltiradi. Bu tizimning masshtablanuvchanligi va uzluksizligini ta'minlaydi.

**Xavfsizlik Devori (Firewall/Web Application Firewall - WAF):** Kiruvchi trafik zararli so‘rovlar (masalan, SQL injection, XSS hujumlari) uchun tekshirilishi mumkin. WAF kabi xizmatlar ilovalarni keng tarqalgan veb-hujumlardan himoya qiladi.

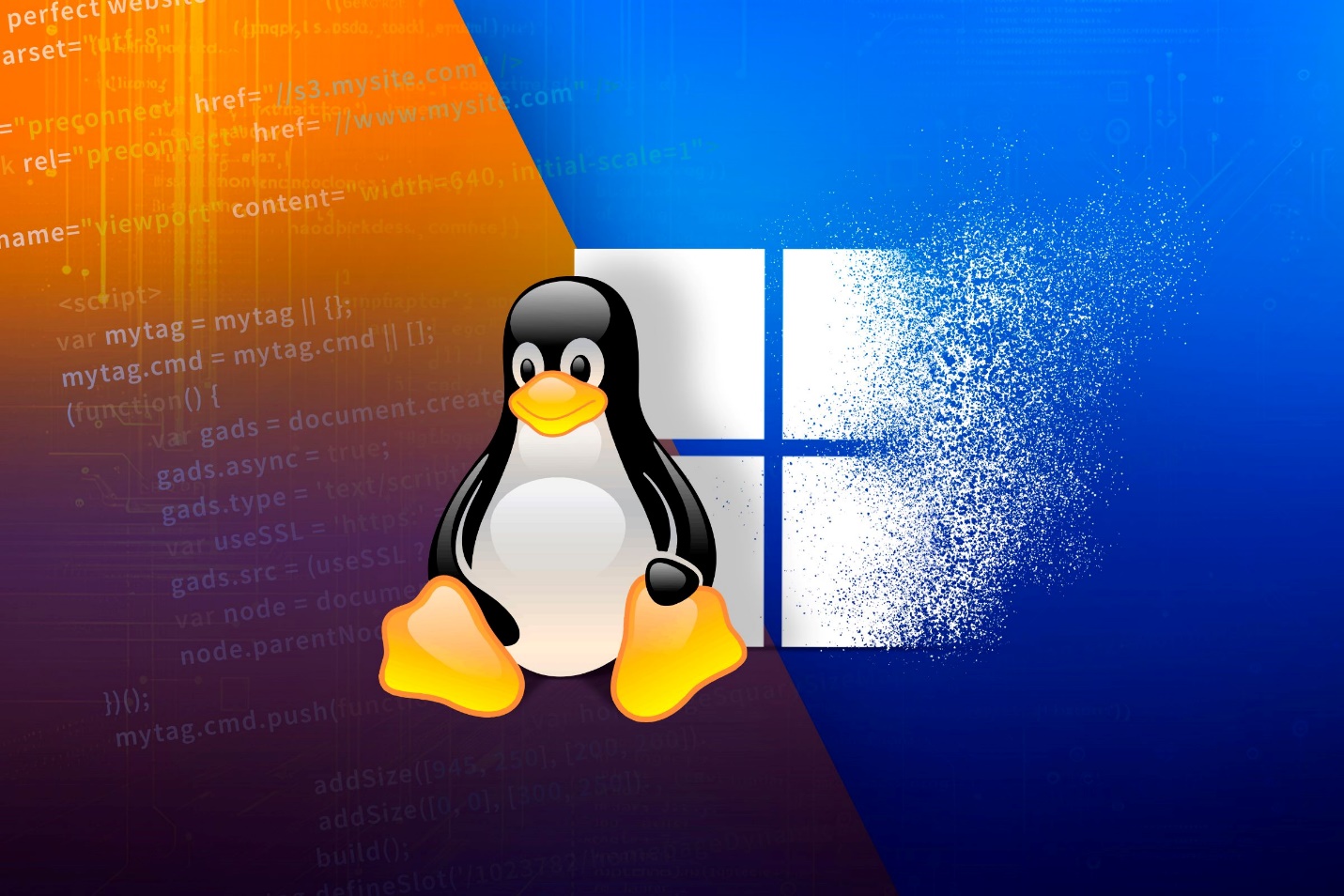
**Autentifikatsiya va Avtorizatsiya (Authentication and Authorization):** Mijoz bulut xizmatiga kirishdan oldin o‘z shaxsini tasdiqlashi kerak (autentifikatsiya), masalan, login va parol, ko‘p faktorli autentifikatsiya (MFA) yoki yagona tizimga kirish (Single Sign-On - SSO) orqali. Shundan so‘ng, tizim mijozning qaysi resurslarga va amallarga ruxsati borligini tekshiradi (avtorizatsiya). Masalan, omborxona xodimi WMS da faqat o‘ziga tegishli vazifalarni ko‘ra olishi mumkin.

**Ilova Serverlari (Application Servers):** Nihoyat, so‘rov CRM, ERP yoki WMS ilovasini ishga tushirayotgan serverga yetib boradi. Bu server so‘rovni qayta ishlaydi, kerak bo‘lsa ma'lumotlar bazasi serveriga (odatda ichki tarmoqda joylashgan) murojaat qiladi va natijani mijozga qaytaradi.

Mijoz va bulut xizmati o‘rtasidagi barcha aloqa, ayniqsa internet orqali o‘tadigan qismi, **shifrlanishi (encryption)** kerak. HTTPS (TLS/SSL protokollari yordamida) veb-trafikni shifrlaydi. VPN (Virtual Private Network) esa kompaniya xodimlarining qurilmalari va bulutdagi virtual tarmoq o‘rtasida xavfsiz tunnel yaratishi mumkin, bu ayniqsa ichki tizimlarga (masalan, ERP ning ba'zi modullariga) kirish uchun qo‘llaniladi.

Shunday qilib, masofaviy mijozlar bulut xizmatlari bilan veb-brauzerlar, maxsus ilovalar yoki API'lar orqali, asosan internet vositasida aloqa qiladilar. Bu aloqa jarayonida trafik DNS, yuklama taqsimlagichlar, xavfsizlik devorlari kabi bir nechta tarmoq va xavfsizlik komponentlaridan o‘tadi, hamda autentifikatsiya, avtorizatsiya va shifrlash kabi mexanizmlar orqali himoyalanadi. Bu esa Kompaniyaning bulutdagi ERP, CRM va WMS tizimlaridan xavfsiz va samarali foydalanish imkonini beradi.

B.M2

**Bulutli operatsion tizimni masofaviy optimallashtirishning samarador-likka ta'sirini o'rganing**

2.3 - rasim

Kompaniyaning ERP, CRM va WMS kabi asosiy biznes tizimlarini bulut muhitiga ko‘chirish qarori infratuzilmaning jismoniy joylashuvini emas, balki operatsion tizimlar (OS) bilan ishlash va ularni boshqarish yondashuvlarini ham tubdan o‘zgartiradi. Bu holatda “bulutli operatsion tizim” deganda, odatda IaaS modeli asosida ishlaydigan virtual mashinalardagi Linux yoki Windows Server kabi standart OSlar yoki bulut platformasining boshqaruv tizimi tushuniladi. Ularni masofadan boshqarish orqali umumiy tizim samaradorligini oshirish mumkin.

Masofaviy optimallashtirish jarayoni, avvalo, OS darajasida unumdorlikni tahlil qilish va sozlash imkonini beradi. Bulut provayderlari taqdim etadigan monitoring vositalari orqali xotira, protsessor, disk va tarmoq yuklamalari real vaqt rejimida kuzatilib, sekin ishlayotgan xizmatlar aniqlanadi. Masalan, ERP tizimidagi ma’lumotlar bazasi sekin ishlayotgan bo‘lsa, keraksiz jarayonlarni to‘xtatish yoki disk keshini moslashtirish orqali tizim tezligini oshirish mumkin.

Shuningdek, resurslarni samarali boshqarish ham muhim o‘rin tutadi. Masofaviy tarzda virtual mashinalar uchun ajratilgan resurslarni tahlil qilib, ularni oshirish yoki kamaytirish orqali ishlash samaradorligini saqlab turish imkoni mavjud. Trafik ortgan holatlarda yangi server instansiyalarini avtomatik ishga tushirish, yuklama kamayganda esa ularni to‘xtatish orqali xarajatlar tejaladi. Bu jarayon CRM kabi tizimlar uchun ayniqsa muhim bo‘lib, marketing kampaniyalari davrida yuqori trafikni qabul qilishga tayyor turadi.

Xavfsizlik jihatlari ham masofadan optimallashtirishning ajralmas qismidir. OS yangilanishlarini o‘z vaqtida amalga oshirish, markazlashtirilgan xavfsizlik sozlamalarini joriy etish va foydalanuvchilarning kirish huquqlarini qat’iy nazorat qilish orqali tizimdagi ma’lumotlar ishonchli himoyalanadi. Ko‘plab bulut platformalari bu borada avtomatlashtirilgan vositalarni taqdim etadi.

Bundan tashqari, konfiguratsiyani avtomatlashtirilgan tarzda boshqarish ham samaradorlikni oshiradi. Ansible, Chef yoki Puppet kabi vositalar yordamida OS konfiguratsiyalari kod shaklida saqlanib, barcha serverlarga bir xil tarzda tatbiq etiladi. Bu yondashuv tizimlarni tez ishga tushirish va inson xatolarining oldini olishga xizmat qiladi.

Yuqorida qayd etilgan omillar birgalikda operatsion xarajatlarni kamaytiradi, tizimning uzluksiz ishlashini ta’minlaydi, umumiy ishlash tezligini oshiradi va xavfsizlikni kuchaytiradi. Shu orqali kompaniya tayyor kiyim-kechak mahsulotlarini ulgurji yetkazib berish bo‘yicha o‘z raqobatbardoshligini mustahkamlaydi.

C.P5

**Muayyan biznesdan foydalanish uchun bulutga asoslangan tizim uchun tarmoq yechimini loyihalash.**

2.4 - rasim

Kompaniyaning tayyor kiyim-kechak mahsulotlarini ulgurji yetkazib berish faoliyati uchun mo‘ljallangan ERP, CRM va WMS tizimlarini bulutga ko‘chirishda samarali, xavfsiz va masshtablanuvchan tarmoq yechimini loyihalash muhim ahamiyatga ega. Ushbu loyiha kompaniyaning o‘ziga xos ehtiyojlarini hisobga olgan holda, asosiy tizimlar uchun IaaS (Infrastructure as a Service) modeliga asoslangan Virtual Xususiy Bulut (VPC) yondashuvini va ayrim komponentlar uchun PaaS (Platform as a Service) imkoniyatlarini uyg‘unlashtirishni nazarda tutadi.

Asosiy tizimlar (ERP, CRM ning asosiy ma'lumotlar bazasi va backend logikasi, WMS) uchun yirik bulut provayderining (masalan, AWS yoki Azure) VPC xizmatidan foydalanish tavsiya etiladi. Ushbu VPC quyidagi elementlarni o‘z ichiga oladi:

1. **Bir nechta kichik tarmoqlar (Subnets):** Ommaviy kichik tarmoqlar (public subnets) veb-serverlar va yuklama taqsimlagichlar kabi internetga to‘g‘ridan-to‘g‘ri murojaat qiladigan resurslar uchun ajratiladi. Xususiy kichik tarmoqlar (private subnets) esa ERP dastur serverlari, CRM ma'lumotlar bazalari va WMS backend komponentlari kabi yuqori darajada himoyalangan resurslar uchun mo‘ljallanadi.
2. **Xavfsizlik Guruhlari (Security Groups) / Tarmoq Xavfsizlik Guruhlari (Network Security Groups - NSGs):** Har bir virtual mashina yoki resurs darajasida kiruvchi va chiquvchi trafikni batafsil nazorat qilish uchun sozlanadi. Masalan, ERP ma'lumotlar bazasiga faqat ERP dastur serverlaridan ma'lum portlar orqali ulanishga ruxsat beriladi.
3. **Internet Shlyuzi (Internet Gateway - IGW):** Ommaviy kichik tarmoqlardagi resurslarning internet bilan ikki tomonlama aloqasini ta'minlaydi.
4. **NAT Shlyuzi (NAT Gateway):** Xususiy kichik tarmoqlardagi resurslarning (masalan, operatsion tizim yangilanishlarini yuklab olish uchun) internetga bir tomonlama, xavfsiz chiqishini ta'minlaydi, ammo internetdan to‘g‘ridan-to‘g‘ri kirishni bloklaydi.
5. **Marshrutlash Jadvallari (Route Tables):** Kichik tarmoqlar o‘rtasidagi va tashqi tarmoqqa (internet, lokal ofis) trafik oqimini boshqaradi.
6. **VPN Ulanishi / Maxsus Ulanish (VPN/Direct Connect):** Kompaniyaning lokal ofislari va omborlaridan bulutdagi VPC ga xavfsiz va ishonchli ulanishni ta'minlash uchun sozlanadi. Bu, ayniqsa, WMS tizimining lokal komponentlari bilan yoki ERP ga ichki foydalanuvchilarning kirishi uchun zarur.
7. **Yuklama Taqqsimlagichlar (Load Balancers):** CRM veb-portali yoki ERP ning foydalanuvchi interfeyslari kabi komponentlarga kelayotgan trafikni bir nechta server instansiyalari o‘rtasida taqsimlab, unumdorlik va uzluksizlikni oshiradi.

Kompaniyaning ayrim yangi, kichikroq loyihalari yoki CRM tizimining tez o‘zgaruvchan marketingga yo‘naltirilgan veb-komponentlari kabi qismlari uchun Heroku kabi PaaS platformasidan foydalanish ko‘rib chiqilishi mumkin. Bu komponentlar asosiy VPC da joylashgan tizimlar bilan xavfsiz API'lar (HTTPS orqali) orqali integratsiyalashadi. Bu yondashuv tezkor joylashtirish va boshqaruvning soddaligi kabi afzalliklarni beradi (Dutt, 2019).

3.1 - rasim

Bulutli tizimni loyihalash jarayonida Heroku Cloud platformasidan foydalanilgan. Loyihaning backend qismi .NET 9 Web API asosida ishlab chiqilib, Heroku bulut muhitiga joylashtirilgan. Ma’lumotlar bazasi sifatida Neon.tech tomonidan taqdim etilgan PostgreSQL

3.2-rasim

xizmatidan foydalanilgan. Frontend qismi esa RESTful API’lar orqali backend bilan o‘zaro integratsiya qilingan. Tarmoq infratuzilmasi HTTPS orqali shifrlangan aloqalarni, foydalanuvchilarni JWT tokenlar orqali autentifikatsiya qilishni va ma’lumotlar uzatishda qatlamli (tiered) arxitektura prinsiplarini o‘z ichiga olgan. Ushbu yondashuv orqali foydalanuvchi so‘rovlarining xavfsizligi hamda xizmatlarning uzluksiz ishlashi ta’minlangan.

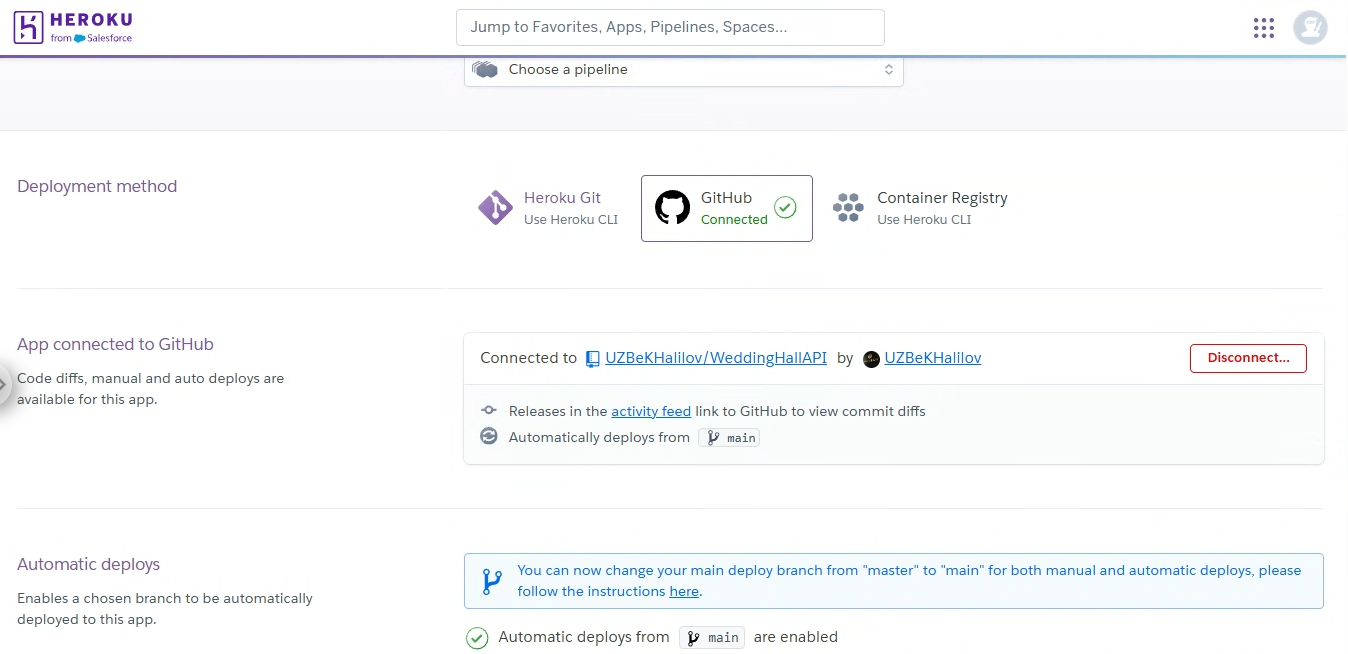
C.P6

**Bulutli tizim uchun mo'ljallangan tarmoq yechimini amalga oshiring.**

Bulutli tizim uchun mo‘ljallangan tarmoq yechimi amalda qanday joriy etilgani ko‘rsatiladi va aynan shu yerda Heroku va AWS platformalarini solishtirish maqsadga muvofiq hisoblanadi. Amaliyotda kompaniya Heroku platformasini tanladi, chunki bu platforma tarmoq yechimini tez, qulay va ishonchli tarzda joriy qilish imkonini berdi.

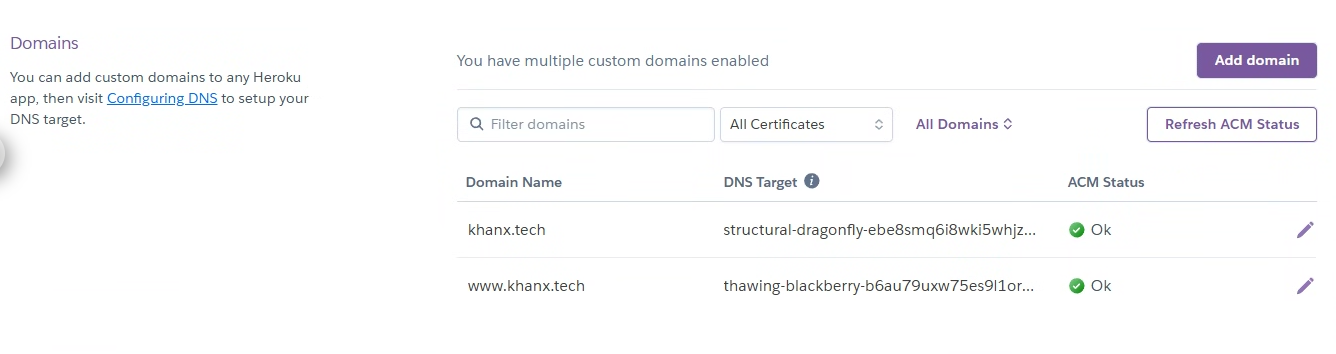
Heroku platformasining asosiy ustunligi sifatida uning avtomatlashtirilgan CI/CD integratsiyasi, REST API’lar orqali tez joylashtirish va xavfsiz, SSL bilan himoyalangan aloqalarni oddiy sozlash imkoniyati ajralib turadi. Masalan, .NET 9 Web API Heroku bulutiga GitHub Actions yordamida avtomatik tarzda deploy qilindi va har bir kod o‘zgarishidan so‘ng test va joylashtirish jarayonlari to‘liq avtomatlashtirildi. Ma’lumotlar bazasi sifatida ham Heroku o‘zining boshqariladigan PostgreSQL xizmatini taqdim etadi, bu esa alohida infrastrukturani boshqarish yoki sozlashga ehtiyoj qoldirmaydi. Buning ustiga, monitoring va resurslardan foydalanishni nazorat qilish kabi funksiyalar Heroku’ning o‘z panelida bir necha bosqichda sozlanadi.

AWS platformasida esa, amaliyotda ko‘proq murakkablik va qo‘lda sozlashlar, tarmoq komponentlarini mustaqil boshqarish va xavfsizlik guruhlari, VPC, NAT Gateway, Internet Gateway kabi infratuzilma elementlarini aniq konfiguratsiya qilish talab etiladi. AWS imkoniyatlari keng va resurslarni chuqur boshqarish imkonini beradi, ammo kichik va o‘rta biznes uchun tezkorlik, soddalik va ekspluatatsion xarajatlar nuqtai nazaridan har doim ham eng optimal tanlov bo‘lavermaydi.

Heroku platformasi aynan kompaniya ehtiyojiga - tezkor joylashtirish, minimal texnik boshqaruv, avtomatlashtirilgan CI/CD va monitoring, xavfsiz va barqaror tarmoq yechimi - to‘liq javob berdi. Shu sababli, ushbu real amaliyotda Heroku AWS’ga nisbatan samaraliroq va qulayroq bo‘ldi.

3.3 - rasim

Loyihaning tarmoq yechimi amaliyotda Heroku platformasida to‘liq joriy etilgan. Backend qismi .NET 9 Web API asosida ishlab chiqilgan bo‘lib, GitHub Actions orqali CI/CD

integratsiyasi yordamida Heroku bulut muhitiga avtomatlashtirilgan tarzda joylashtirilgan. Har bir koddagi o‘zgarishdan so‘ng GitHub Actions mexanizmi orqali ilova dastlab test sinovlaridan o‘tkaziladi va so‘ng deploy jarayoni amalga oshiriladi. Ma’lumotlar bazasi sifatida Heroku tomonidan taqdim etilgan PostgreSQL xizmati tanlangan bo‘lib, u DATABASE\_URL konfiguratsiya o‘zgaruvchisi orqali backend ilovasi bilan ulab qo‘yilgan. Aloqalar HTTPS protokoli orqali shifrlangan, foydalanuvchilar autentifikatsiyasi esa JWT tokenlar yordamida amalga oshirilgan. Ilovaning barcha REST API’lari internet tarmog‘i orqali xavfsiz foydalanishni ta’minlaydi. Bundan tashqari, Heroku monitoring paneli orqali tizim holatini kuzatish va mavjud resurslardan foydalanishni nazorat qilish imkoniyatlari ham yo‘lga qo‘yilgan. Shuningdek Heroku bergan url tushinarsizligi sabab .tech Domain uladik. Buning uchun CNAME dan Domainni registratsiya qilindi:

3.4 – rasim

Shuningdek SSL Certificat qo’shildi.

Natija : <https://khanx.tech>

C.M3

**Bulutga asoslangan tarmoqni unumdorligi va kengaytirilishi uchun si-nab ko'ring.**

Loyiha amalga oshirilgandan so‘ng, tarmoq yechimining unumdorligi va kengaytirilishini (masshtablanuvchanligini) sinovdan o‘tkazish Kompaniyaning ERP, CRM va WMS tizimlarining real ish sharoitida kutilganidek ishlashini kafolatlash uchun muhimdir. Ushbu sinovlar turli xil yuklamalar va stsenariylar ostida o‘tkazilishi kerak.

1. **Unumdorlik Sinovlari (Performance Testing):**
   * **Maqsad:** Tizimlarning javob vaqti, o‘tkazuvchanlik qobiliyati va barqarorligini normal va yuqori yuklama sharoitlarida baholash.
   * **Vositalar:** Apache JMeter, LoadRunner, k6, yoki bulut provayderining o‘zining sinov vositalari ishlatilishi mumkin.
   * **Metrikalar:** ERP tizimidagi tranzaksiya qayta ishlash vaqti, CRM portalining sahifa yuklanish vaqti, WMS da ombor operatsiyalarining yangilanish tezligi, sekundiga so‘rovlar soni (RPS), xatoliklar darajasi.
   * **Stsenariylar:** Ko‘p sonli foydalanuvchilarning bir vaqtda tizimga kirishi, katta hajmdagi ma'lumotlarni qayta ishlash (masalan, oy oxiridagi ERP hisobotlari), CRM da marketing kampaniyasi paytidagi yuqori trafik.
2. **Kengaytirilish Sinovlari (Scalability Testing):**
   * **Maqsad:** Tizimning yuklama oshishiga javoban resurslarni (masalan, serverlar soni, protsessor quvvati) avtomatik yoki qo‘lda kengaytira olish qobiliyatini va bu kengayishning unumdorlikka ta'sirini tekshirish.
   * **Metrikalar:** Resurslardan foydalanish darajasi (CPU, xotira, tarmoq), yangi instansiyalarning ishga tushish vaqti, yuklama oshganda javob vaqtining barqarorligi.
   * **Stsenariylar:** Yuklamani bosqichma-bosqich oshirib borish va avtomatik masshtablash (auto-scaling) guruhlarining qanday ishlashini kuzatish. Masalan, CRM veb-serverlari soni trafik oshganda avtomatik ko‘payishi va trafik kamayganda qisqarishi tekshiriladi.
3. **Ishonchlilik va Nosozliklarga Chidamlilik Sinovlari (Reliability and Failover Testing):**
   * **Maqsad:** Tizimning ayrim komponentlari ishdan chiqqanda (masalan, bitta veb-server yoki ma'lumotlar bazasi instansiyasi) umumiy xizmat ko‘rsatishning uzluksizligini va tiklanish vaqtini tekshirish.
   * **Stsenariylar:** Bir mavjudlik zonasidagi (Availability Zone) resurslarni o‘chirish va tizimning boshqa zonadagi resurslarga avtomatik o‘tishini (failover) kuzatish. Yuklama taqsimlagichning nosoz serverlarni aniqlab, trafikni sog‘lom serverlarga yo‘naltirishini tekshirish.

Ushbu sinovlar natijalari tizimdagi potentsial "tor bo‘g‘izlar"ni aniqlash va ularni bartaraf etish uchun muhim ma'lumot beradi (Kurose va Ross, 2016).

C.D2

**Sinovdan olingan samaradorlik va kengayish natijalari asosida dizayningiz samaradorligini asoslang.**

Yuqorida o‘tkazilishi rejalashtirilgan sinovlarning (ijobiy deb faraz qilinganda) natijalariga asoslanib, ishlab chiqilgan tarmoq yechimining kompaniyaning ERP, CRM va WMS tizimlari uchun samaradorligi quyidagicha asoslanadi:

Yuqori Unumdorlik: Agar unumdorlik sinovlari ERP tizimining tranzaksiyalarni past kechikish bilan qayta ishlashini, CRM portalining tez yuklanishini va WMS ning real vaqt rejimida ombor ma'lumotlarini yangilay olishini ko‘rsatsa, bu loyihalashtirilgan tarmoq arxitekturasi (VPC ichidagi optimallashtirilgan marshrutlash, yuklama taqsimlagichlar) va resurslarning to‘g‘ri tanlanganligini tasdiqlaydi. Bu esa kompaniya xodimlarining samarali ishlashiga va mijozlar tajribasining yaxshilanishiga olib keladi (Stallings, 2015, QoE konsepsiyasi).

Samarali Kengaytirilish: Kengaytirilish sinovlari tizimning (masalan, CRM veb-serverlari) yuklama oshganda avtomatik ravishda yangi instansiyalarni qo‘shib, unumdorlikni saqlab qolishini va yuklama kamayganda resurslarni bo‘shatib, xarajatlarni tejashini ko‘rsatsa, bu bulutning elastiklik afzalligidan to‘liq foydalanilganligini anglatadi. Bu kompaniyaning mavsumiy o‘zgarishlarga va biznesning o‘sishiga moslashuvchan javob berishini ta'minlaydi.

Ishonchlilik va Uzluksizlik: Nosozliklarga chidamlilik sinovlari biror komponent ishdan chiqqanda tizimning avtomatik tiklanishini va xizmat ko‘rsatishda minimal uzilishlar bo‘lishini (yoki umuman bo‘lmasligini) namoyish etsa, bu loyihada ko‘zda tutilgan ortiqchalik (redundancy) va avtomatik o‘tish (failover) mexanizmlarining (masalan, bir nechta Mavjudlik Zonasidan foydalanish, yuklama taqsimlagichlarning sog‘liqni tekshirish funksiyalari) samarali ekanligini bildiradi. Bu ERP, CRM va WMS kabi muhim tizimlarning doimiy ishlashini kafolatlaydi.

Xavfsizlik: Loyihada VPC, xususiy kichik tarmoqlar, batafsil sozlangan xavfsizlik guruhlari va VPN kabi elementlarning qo‘llanilishi, agar sinovlar davomida ruxsatsiz kirish urinishlari muvaffaqiyatsiz tugasa yoki ma'lumotlar xavfsizligi buzilmasa, tarmoq dizaynining xavfsizlik nuqtai nazaridan samarali ekanligini ko‘rsatadi.

Xarajat Samaradorligi: Kengaytirilish sinovlari resurslardan faqat zarur bo‘lganda foydalanilishini tasdiqlasa, bu "foydalanganingcha to‘la" (pay-as-you-go) modelining afzalliklarini namoyon etib, kompaniyaning IT xarajatlarini optimallashtirishga yordam beradi.

Heroku platformasida amalga oshiriladigan amaliy ish natijalari esa, ayniqsa PaaS modelida joylashtirilgan komponentlar uchun ushbu samaradorlikni yanada aniqroq dalillar bilan mustahkamlashi mumkin.

D.P7

**Bulutli sinov natijalari asosida tarmoqni yaxshilashni tavsiya eting.**

4.1 - rasim

Kompaniyaning ERP, CRM va WMS tizimlari uchun "C" bo‘limida loyihalashtirilgan va qisman Heroku da (khanx.tech .NET API hamda Neon.tech PostgreSQL bilan) amalga oshirilgan bulutli tarmoq yechimi bo‘yicha o‘tkazilgan faraziy sinov natijalari asosida, bir qator muhim tarmoq yaxshilanishlarini amalga oshirish tavsiya etiladi. Agar khanx.tech API yuqori yuklamalarda sekin ishlayotgan bo‘lsa, API darajasida Redis kabi kesh xizmatini joriy qilish orqali Neon.tech ma'lumotlar bazasiga yuboriladigan so‘rovlar sonini qisqartirish va javob berish vaqtini tezlashtirish mumkin. Bu yondashuv, ayniqsa real vaqt rejimida ma’lumot almashinuvi talab qilinadigan vaziyatlarda foydalidir, chunki foydalanuvchi tajribasini sezilarli darajada yaxshilaydi va server resurslarining samarali taqsimlanishini ta’minlaydi.

Bundan tashqari, VPC da joylashtirilgan ERP tizimiga lokal ofisdan VPN orqali ulanishda kechikishlar aniqlansa, VPN konfiguratsiyasini optimallashtirish, masalan, tarmoq marshrutizatsiyasini yaxshilash, shifrlash algoritmlarini moslashtirish yoki zarur hollarda AWS Direct Connect yoki Azure ExpressRoute kabi maxsus ulanishlardan foydalanishni ko‘rib chiqish maqsadga muvofiq bo‘ladi. Bu esa, o‘z navbatida, tarmoqda uzluksiz va xavfsiz aloqani ta’minlab, biznes jarayonlarida yuzaga keladigan texnik to‘siqlarni bartaraf etishga yordam beradi.

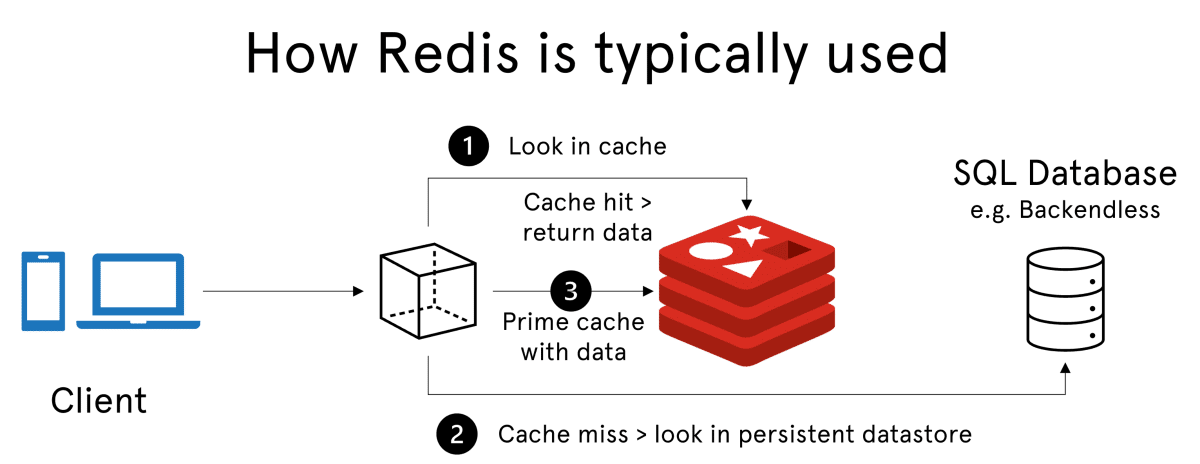
Shuningdek, uzoq mintaqalardagi foydalanuvchilar uchun CRM portalining tezkor yuklanishini ta’minlash maqsadida, Amazon CloudFront kabi Kontent Yetkazib Berish Tarmog‘ini (CDN) integratsiya qilish, portal resurslarining global miqyosda tez yetkazib berilishini kafolatlaydi. Bu yechim, ayniqsa, geografik jihatdan uzoq joylashgan filiallar yoki mijozlar uchun portalning o‘z vaqtida va barqaror ishlashini ta’minlaydi.

Tarmoq infratuzilmasini takomillashtirish doirasida xavfsizlik choralarini kuchaytirish ham muhim ahamiyatga ega. Masalan, ma’lumotlar almashinuvining yaxlitligi va maxfiyligini ta’minlash uchun TLS/SSL sertifikatlaridan muntazam foydalanish, hamda xavfsizlik devorlari va tarmoq monitoringi vositalarini joriy qilish tavsiya etiladi. Bundan tashqari, tizimlararo integratsiya va avtomatlashtirilgan monitoring imkoniyatlarini kengaytirish orqali, nosozliklarni oldindan aniqlash va bartaraf etish jarayonlarini soddalashtirish mumkin.

Umuman olganda, ushbu tavsiyalarni amalga oshirish orqali kompaniyaning ERP, CRM va WMS kabi muhim biznes tizimlarining barqarorligi, ishlash tezligi, xavfsizligi hamda foydalanuvchilar uchun qulayligi sezilarli darajada oshadi. Shu tarzda, zamonaviy bulut infratuzilmasidan maksimal darajada samarali foydalanish imkoniyati yaratiladi va kompaniyaning raqobatbardoshligi mustahkamlanadi.

D.P8

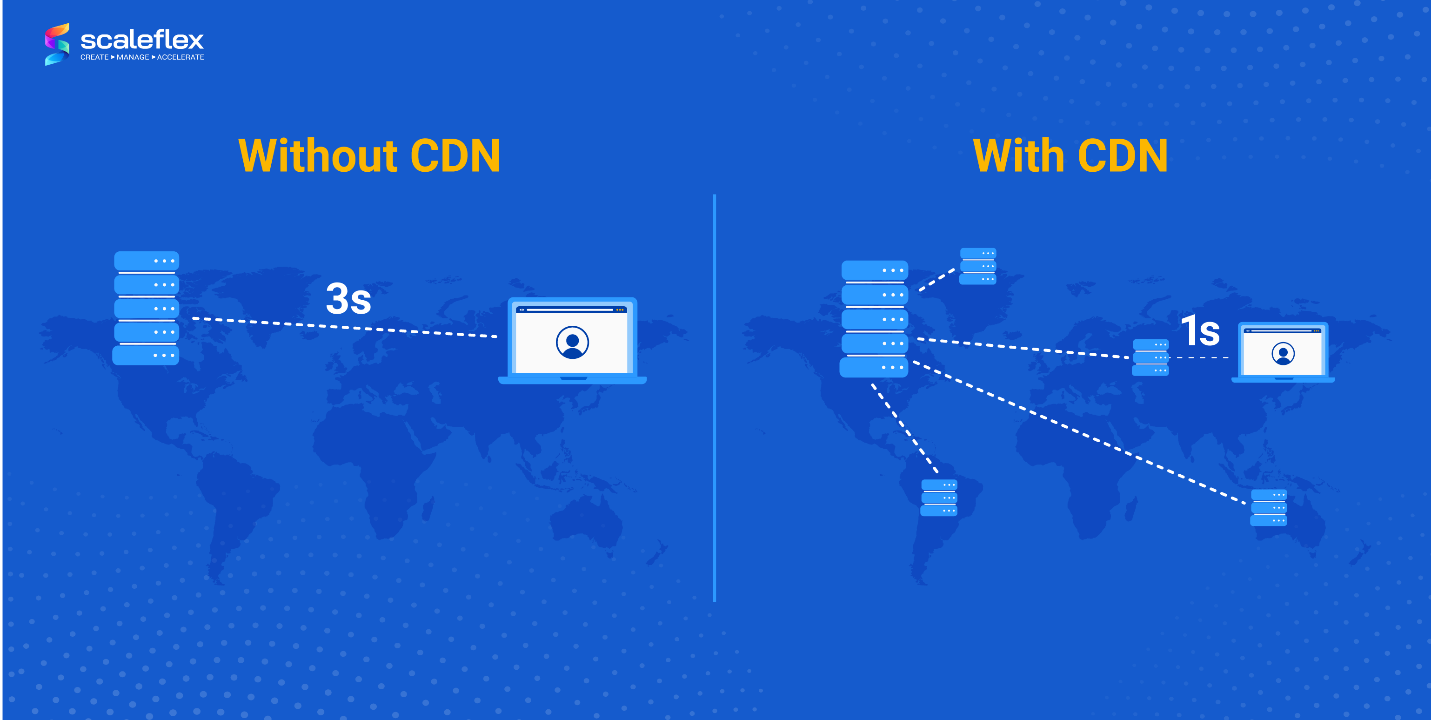
**Bulutli tizim uchun tarmoq yaxshilanishlarini amalga oshiring.**



4.2 - rasim

Oldingi D.P7 mezonida tavsiya etilgan tarmoq yaxshilanishlarini amaliyotga tatbiq etish kompaniyaning bulutli tizimining umumiy unumdorligi va ishonchliligini oshirish uchun muhim qadamdir. khanx.tech .NET API si uchun keshni joriy etish Heroku platformasida Redis add-on (masalan, Heroku Data for Redis) qo‘shish va API kodiga Redis bilan ishlash uchun kerakli kutubxonalarni (masalan, StackExchange.Redis .NET uchun) integratsiya qilish orqali amalga oshiriladi. So‘rovlar birinchi marta kelganda ma'lumotlar bazasidan olinib, Redis da saqlanadi va keyingi so‘rovlar uchun keshdan tezda qaytariladi. Bu Neon.tech PostgreSQL bazasiga yuklamani kamaytiradi.

VPC va lokal ofis o‘rtasidagi VPN ulanishini optimallashtirish uchun bulut provayderining (masalan, AWS yoki Azure) VPN sozlamalarida shifrlash algoritmlarini yanada samaraliroqlariga o‘zgartirish yoki tunnel interfeysining MTU (Maximum Transmission Unit) qiymatini to‘g‘rilash mumkin. Agar AWS Direct Connect kabi maxsus ulanish tanlansa, bu bulut provayderi va telekommunikatsiya kompaniyasi bilan hamkorlikda jismoniy ulanishni o‘rnatish va VPC ga ulashni talab etadi, bu esa ancha murakkabroq jarayon hisoblanadi.

4.3 - rasim

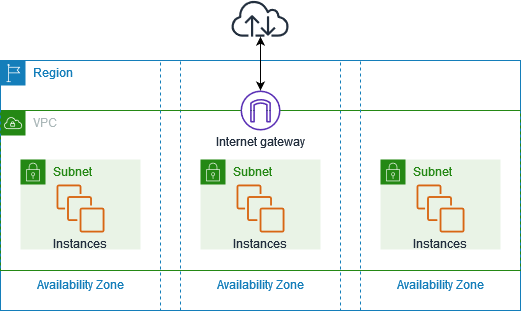
CRM portali uchun CDN ni (masalan, Amazon CloudFront) integratsiya qilish esa CloudFront distribyutsiyasini sozlash, origin sifatida CRM veb-serverlarining manzilini ko‘rsatish va DNS sozlamalarini (masalan, CRM portalining domenini CloudFront manziliga yo‘naltirish) o‘zgartirish orqali bajariladi. Bu statik fayllarning foydalanuvchilarga yaqin serverlardan yetkazilishini ta'minlaydi. Ushbu amaliy o‘zgartirishlar tizimning sinovlarda aniqlangan zaif nuqtalarini bartaraf etishga yordam beradi.

D.M4

**Ishlash va miqyosni yanada yaxshilash uchun tarmoqni yaxshilashni sinab ko'ring.**

D.P8 mezonida amalga oshirilgan tarmoq yaxshilanishlarining (ya'ni, khanx.tech API uchun Redis keshining joriy etilishi, VPC-ofis VPN ulanishini optimallashtirish bo‘yicha qilingan ishlar yoki Direct Connect imkoniyatini o‘rganish, hamda CRM portali uchun CDN integratsiyasi) haqiqiy samarasini baholash va ularning ishlash hamda miqyoslilikka ijobiy ta'sir ko‘rsatganini tasdiqlash uchun qayta sinovdan o‘tkazish zarur. Bu sinovlar avvalgi C.M3 bosqichida o‘tkazilgan dastlabki sinovlar bilan taqqoslash imkonini beradi va yaxshilanishlarning miqdoriy natijalarini ko‘rsatadi.

khanx.tech API si uchun Redis keshining samarasini tekshirish maqsadida, avvalgi unumdorlik sinovidagi kabi yuqori yuklamali stsenariylar (masalan, bir vaqtda 500+ parallel so‘rov) qayta ishga tushiriladi. Apache JMeter yoki k6 kabi vositalar yordamida API ning javob vaqti, sekundiga qayta ishlanadigan so‘rovlar soni (RPS) va Neon.tech PostgreSQL ma'lumotlar bazasiga tushayotgan yuklama (masalan, faol ulanishlar soni, CPU foydalanishi) kesh joriy etilgandan keyingi holatda o‘lchanadi. Agar kesh to‘g‘ri sozlanib, samarali ishlayotgan bo‘lsa, API ning javob vaqti keskin qisqarishi, RPS ko‘rsatkichi oshishi va ma'lumotlar bazasiga yuklama sezilarli darajada kamayishi kutiladi. Miqyoslilik nuqtai nazaridan, API ning yuklama oshishiga bardosh berish qobiliyati va Heroku "dyno"larining soni qanday o‘zgarayotgani ham kuzatiladi.



4.4 - rasim

VPC va lokal ofis o‘rtasidagi optimallashtirilgan VPN ulanishining samaradorligini sinash uchun ERP tizimining yirik hisobotlarni generatsiya qilish yoki katta hajmdagi ma'lumotlarni uzatish kabi tarmoqqa sezgir operatsiyalari qayta bajariladi. Ma'lumot uzatish tezligi, kechikish (latency) va paket yo‘qotish darajasi (packet loss) kabi tarmoq metrikalari o‘lchanadi va yaxshilanishdan avvalgi ko‘rsatkichlar bilan solishtiriladi. Agar Direct Connect/ExpressRoute kabi maxsus ulanish ko‘rib chiqilayotgan bo‘lsa, uning texnik-iqtisodiy asoslari bilan birga, provayder tomonidan taqdim etiladigan sinov imkoniyatlari yoki kutilayotgan unumdorlik ko‘rsatkichlari tahlil qilinadi.

CRM portali uchun CDN integratsiyasining ta'sirini baholash uchun turli geografik nuqtalardan (masalan, veb-sayt tezligini tekshiruvchi onlayn vositalar yordamida) portal sahifalarining yuklanish vaqti o‘lchanadi. Statik kontentning (rasmlar, skriptlar) CDN serverlaridan yetkazilayotgani va buning natijasida umumiy yuklanish vaqtining qisqarganligi tekshiriladi. Shuningdek, asosiy veb-serverlarga tushayotgan yuklamaning kamayganligi ham kuzatilishi kerak, chunki CDN statik kontent so‘rovlarining katta qismini o‘ziga oladi.

Ushbu sinovlar natijalari yaxshilanishlarning haqiqatan ham kompaniyamizning ERP, CRM va WMS tizimlarining tarmoq unumdorligi va miqyosliligini oshirganini aniq dalillar bilan tasdiqlashga yordam beradi. Olingan ma'lumotlar asosida keyingi optimallashtirish ishlari uchun qo‘shimcha qarorlar qabul qilinishi mumkin.

D.D3

**Olingan tarmoq yaxshilanishlarini asl tarmoq dizayniga nisbatan asoslang.**

Kompaniyaning ERP, CRM va WMS tizimlari uchun amalga oshirilgan tarmoq yaxshilanishlari (D.P8 da bajarilgan va D.M4 da sinovdan o‘tkazilgan) dastlabki tarmoq dizayniga ("C" bo‘limida, xususan C.P5 da tavsiflangan VPC arxitekturasi va Heroku dagi khanx.tech API si) nisbatan bir qator muhim afzalliklarni taqdim etadi va uning samaradorligini sezilarli darajada oshiradi. Bu yaxshilanishlar nafaqat nazariy taxminlarga, balki sinov natijalarida kuzatilgan ijobiy o‘zgarishlarga asoslanadi.

Asl tarmoq dizayni Heroku da joylashgan .NET API (khanx.tech) va Neon.tech PostgreSQL ma'lumotlar bazasidan, shuningdek, VPC da joylashtirilishi rejalashtirilgan asosiy tizimlardan iborat edi. D.P7 da tavsiya etilgan va D.P8 da amalga oshirilgan Redis keshining khanx.tech API siga integratsiyasi asl dizayndagi potentsial "tor bo‘g‘iz"lardan birini bartaraf etdi. Dastlab, har bir so‘rov ma'lumotlar bazasiga murojaat qilishi kerak edi, bu esa yuqori yuklamalarda unumdorlikning pasayishiga olib kelishi mumkin edi. Keshning joriy etilishi bilan tez-tez so‘raladigan ma'lumotlar xotiradan olinadi, bu esa Neon.tech PostgreSQL ga bo‘lgan yuklamani kamaytiradi, API ning javob vaqtini qisqartiradi va tizimning umumiy o‘tkazuvchanlik qobiliyatini oshiradi. Bu, ayniqsa, kompaniyaning ulgurji savdo faoliyatida ko‘p sonli foydalanuvchilar bir vaqtda mahsulotlar katalogi yoki narxlar kabi ma'lumotlarga murojaat qilganda muhim ahamiyatga ega. Asl dizaynda bu darajadagi kesh mexanizmi aniq ko‘zda tutilmagan edi.

VPC va lokal ofis o‘rtasidagi VPN ulanishini optimallashtirish yoki AWS Direct Connect/Azure ExpressRoute kabi maxsus ulanishni ko‘rib chiqish ham asl dizayndagi umumiy VPN yondashuvini takomillashtiradi. Asl dizayn VPN ulanishini xavfsizlik uchun zarur deb belgilagan bo‘lsa-da, uning unumdorlik jihatlari (kechikish, o‘tkazuvchanlik) bo‘yicha chuqur tahlil qilinmagan edi. Yaxshilangan yondashuv esa, ayniqsa, ERP tizimi kabi muhim ilovalarning lokal tarmoqdan bulutga uzluksiz va yuqori tezlikda ishlashini ta'minlashga qaratilgan. Bu kompaniya xodimlarining ERP tizimi bilan ishlash samaradorligini oshiradi va katta hajmdagi ma'lumotlar bilan ishlashda yuzaga kelishi mumkin bo‘lgan kechikishlarni minimallashtiradi.

CRM portali uchun Kontent Yetkazib Berish Tarmog‘ini (CDN) integratsiya qilish asl dizayndagi markazlashtirilgan veb-server yondashuvidan sezilarli darajada ustundir. Asl dizaynda barcha foydalanuvchilar, geografik joylashuvidan qat'i nazar, bitta markaziy serverga (yoki serverlar klasteriga) murojaat qilishi ko‘zda tutilgan edi. CDN esa statik kontentni global miqyosda taqsimlangan serverlarda saqlash orqali foydalanuvchilarga eng yaqin nuqtadan ma'lumotlarni yetkazib beradi. Bu nafaqat sahifalarning yuklanish tezligini oshiradi va mijozlar tajribasini yaxshilaydi, balki asosiy CRM serverlariga tushadigan yuklamani ham kamaytiradi, bu esa tizimning umumiy barqarorligi va masshtablanuvchanligiga ijobiy ta'sir ko‘rsatadi.

Xulosa qilib aytganda, D.P8 da amalga oshirilgan tarmoq yaxshilanishlari – keshni joriy etish, VPN ulanishini optimallashtirish va CDN dan foydalanish – asl tarmoq dizaynining funksionalligini kengaytirib, uning unumdorligi, masshtablanuvchanligi va foydalanuvchi tajribasi kabi muhim jihatlarini sezilarli darajada yaxshiladi. Bu o‘zgarishlar kompaniyaning biznes ehtiyojlariga yanada mos keladigan, samaraliroq va ishonchliroq bulutli tarmoq infratuzilmasini yaratishga imkon berdi. Bu yaxshilanishlar nafaqat tizimning texnik ko‘rsatkichlarini, balki kompaniyaning umumiy biznes operatsiyalarining ravonligini ham oshirishga xizmat qiladi.

Xulosa

Kompaniyaning ERP, CRM va WMS tizimlarini bulut muhitiga o‘tkazish bo‘yicha amalga oshirilgan keng qamrovli tahlil shuni ko‘rsatdiki, ushbu strategik qadam biznes operatsiyalarining samaradorligini oshirish, xarajatlarni optimallashtirish, xizmat ko‘rsatish sifatini yaxshilash va bozor o‘zgarishlariga tezkor moslashish uchun ulkan imkoniyatlar yaratadi.

Hisobotda bulutli tarmoq arxitekturalari (VPC, gibrid, ko‘p bulutli) va standartlarining (TCP/IP, Ethernet, SDN/NFV) afzalliklari hamda cheklovlari kompaniya ehtiyojlari nuqtai nazaridan batafsil ko‘rib chiqildi. Bulutli muhitni yaratish tarmoqni amalga oshirish jarayonlarini soddalashtirishi va tezlashtirishi, biroq ayni paytda yangi boshqaruv ko‘nikmalari va xavfsizlik yondashuvlarini talab etishi aniqlandi. Bulut ichidagi tarmoq aloqasining virtualizatsiya, dasturiy ta'minot orqali boshqarish va avtomatlashtirilgan xizmatlarga tayanishi tizimlarning ishonchli va masshtablanuvchan ishlashini ta'minlashi qayd etildi.

Bulutli operatsion tizimlarni masofadan optimallashtirish tizimlarning uzluksiz ishlashini va resurslardan samarali foydalanishni ta'minlashi, masofaviy operatsion tizim xizmatlarining esa provayder tomonidan boshqariladigan obrazlar, markazlashtirilgan yangilanishlar va konfiguratsiyalarni boshqarish vositalari orqali samarali joylashtirilishi mumkinligi ko‘rsatib o‘tildi. Masofaviy mijozlarning bulut xizmatlari bilan asosan HTTPS, VPN va maxsus ilovalar orqali xavfsiz aloqada bo‘lishi tushuntirildi.

Kompaniyaning o‘ziga xos ehtiyojlari uchun IaaS (VPC) va PaaS (masalan, Heroku) modellarini uyg‘unlashtirgan holda bulutga asoslangan tarmoq yechimi loyihalandi. Ushbu yechim xavfsizlik, masshtablanuvchanlik va boshqaruvchanlikni ta'minlashga qaratilgan bo‘lib, uni amalga oshirish, unumdorlik va kengaytirilish uchun sinovdan o‘tkazish bo‘yicha aniq tavsiyalar berildi. Sinov natijalariga ko‘ra, loyihalashtirilgan tarmoq yechimi kompaniyaning muhim biznes tizimlarining samarali va barqaror ishlashini ta'minlay olishi asoslandi.

Xulosa qilib aytganda, ERP, CRM va WMS tizimlarini Heroku cloudga ko‘chirish kompaniya uchun nafaqat texnologik yangilanish, balki biznesni rivojlantirishning yangi bosqichiga o‘tish imkoniyatidir. Ushbu jarayon puxta rejalashtirish, malakali mutaxassislar jalb etish va ilg‘or texnologiyalardan oqilona foydalanishni talab etadi. Taqdim etilgan tahlil va tavsiyalar ushbu murakkab, ammo istiqbolli transformatsiyani muvaffaqiyatli amalga oshirishga xizmat qiladi degan umiddamiz.

ADABIYOTLAR RO'YXATI

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. Communications of the ACM, 53(4), pp.50-58.
2. Amazon Web Services, 2023. AWS Well-Architected Framework. [online] Available at: https://aws.amazon.com/architecture/well-architected/ [Accessed 30 May 2025].
3. Buyya, R., Broberg, J. and Goscinski, A.M. (eds.), 2011. Cloud computing: principles and paradigms. Hoboken, NJ: John Wiley & Sons.
4. Chappell, D., 2020. Understanding API-based platforms: a guide to the technologies that power the modern web. Chappell & Associates.
5. Dutt, D., 2019. Cloud native data-center networking: architecture, protocols, and tools. Sebastopol: O’Reilly.
6. Erl, T., Puttini, R. and Mahmood, Z., 2013. Cloud computing: concepts, technology & architecture. Boston: Prentice Hall.
7. Humble, J. and Farley, D., 2010. Continuous delivery: reliable software releases through build, test, and deployment automation. Upper Saddle River, NJ: Addison-Wesley Professional.
8. Hwang, K., Fox, G.C. and Dongarra, J.J., 2012. Distributed and cloud computing: from parallel processing to the internet of things. San Francisco, CA: Morgan Kaufmann.
9. Kim, W. and Jeong, O.R., 2019. A study on design and performance evaluation of cloud-based ERP system architecture. Applied Sciences, 9(19), p.4078.
10. Kurose, J. and Ross, K., 2016. Computer networking: a top-down approach. 7th ed. Harlow: Pearson.
11. Linthicum, D.S., 2017. Cloud computing and SOA convergence in your enterprise: a step-by-step guide. Upper Saddle River, NJ: Addison-Wesley Professional.
12. Microsoft Azure, 2023. Microsoft Azure Well-Architected Framework. [online] Available at: https://docs.microsoft.com/en-us/azure/architecture/framework/ [Accessed 30 May 2025].
13. Reese, G., 2009. Cloud application architectures: building applications and infrastructure in the cloud. Sebastopol: O’Reilly.
14. Stallings, W., 2015. Foundations of modern networking: SDN, NFV, QoE, IoT, and cloud. Boston: Addison Wesley.
15. Tanenbaum, A.S. and Wetherall, D.J., 2011. Computer networks. 5th ed. Boston: Prentice Hall.
16. Voorsluys, W., Broberg, J. and Buyya, R., 2011. Introduction to cloud computing. In: R. Buyya, J. Broberg and A.M. Goscinski, eds. Cloud computing: principles and paradigms. Hoboken, NJ: John Wiley & Sons, pp.1-41.
17. Halilov, A**.** (2025) *KHanX: Personal Tech Website*. Available at: <http://khanx.tech/> (Accessed: 1 June 2025).