|  |
| --- |
| 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:** 29.05.2025 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:** | 27.05.2025yil |

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:** 27.05.2025 yil |

Mundarija

[KIRISH 3](#_Toc199348577)

[A.P1 3](#_Toc199348578)

[A.P2 3](#_Toc199348579)

[A.M1 3](#_Toc199348580)

[A.D1 3](#_Toc199348581)

[B.P3 3](#_Toc199348582)

[B.P4 6](#_Toc199348583)

[B.M2 9](#_Toc199348584)

[C.P5 12](#_Toc199348585)

[C.P6 12](#_Toc199348586)

[C.M3 12](#_Toc199348587)

[C.D2 13](#_Toc199348588)

[Xulosa 13](#_Toc199348589)

[ADABIYOTLAR RO'YXATI 13](#_Toc199348590)

KIRISH

Aa

A.P1

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

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.

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.

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. Kompaniyamizning 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. Kompaniyamiz 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, kompaniyamizning 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.

Agar kompaniyamiz 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 kompaniyamizning 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.**

Kompaniyaning ERP, CRM va WMS kabi muhim tizimlarini bulut muhitiga muvaffaqiyatli ko‘chirish va ularning samarali ishlashini ta’minlash uchun umumiy tarmoq standartlarining roli beqiyosdir. Ushbu standartlar turli xil texnologiyalar va qurilmalarning o‘zaro muvofiqligini (interoperability) ta’minlab, bulutli hisoblashning asosiy tamoyillari bo‘lgan moslashuvchanlik, masshtablanuvchanlik va resurslardan umumiy foydalanish (resource pooling) imkoniyatlarini ro‘yobga chiqarishga xizmat qiladi. Quyida asosiy umumiy tarmoq standartlari va ularning bulutli hisoblashni osonlashtirishdagi o‘rni solishtirma tarzda ko‘rib chiqiladi.

Birinchi navbatda, **Ethernet (IEEE 802.3)** standartini ta'kidlash lozim. Dastlab lokal tarmoqlar (LAN) uchun ishlab chiqilgan bo‘lsa-da, Ethernet bugungi kunda bulutli ma'lumotlar markazlarining (data centers) asosiy tarmoq texnologiyasiga aylangan. Uning **yuqori o‘tkazuvchanlik qobiliyati** (masalan, 10 GbE, 40 GbE, 100 GbE va undan yuqori tezliklar) katta hajmdagi ma'lumotlarni, jumladan, ERP tizimining tranzaksiyalari, CRM ma'lumotlar bazalari va WMS operatsiyalaridan kelib chiqadigan trafikni samarali uzatish imkonini beradi. Ethernetning **arzonligi va keng tarqalganligi** ham bulut provayderlari uchun jozibador bo‘lib, xizmat narxlarining nisbatan past bo‘lishiga olib keladi. Bulutli hisoblashni osonlashtirish nuqtai nazaridan, Ethernet virtualizatsiya texnologiyalari bilan birgalikda virtual mashinalar va konteynerlar o‘rtasida tezkor va ishonchli aloqani ta’minlaydi. Virtual LAN (VLAN) kabi mexanizmlar orqali trafikni segmentatsiyalash va izolyatsiyalash imkoniyati ham xavfsizlikni oshiradi. Biroq, an'anaviy Ethernetning o‘zi bulut muhitining dinamik talablariga, masalan, virtual mashinalarning keng miqyosli va tezkor migratsiyasiga (live migration) to‘liq mos kelmasligi mumkin, bu esa **Spanning Tree Protocol (STP)** kabi eskirgan protokollar bilan bog‘liq cheklovlardan kelib chiqadi. Shu sababli, ma'lumotlar markazlarida ko‘pincha TRILL (Transparent Interconnection of Lots of Links) yoki SPB (Shortest Path Bridging) kabi yanada zamonaviy texnologiyalar qo‘llaniladi.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** protokollar to‘plami internetning asosini tashkil etgani kabi, bulutli hisoblashning ham poydevoridir. Uning **platformadan mustaqilligi va global qamrovi** kompaniyamizning ERP, CRM va WMS tizimlariga dunyoning istalgan nuqtasidan, turli xil qurilmalar orqali kirish imkoniyatini yaratadi. TCP ishonchli ma'lumotlar uzatishni kafolatlasa, IP manzillash va marshrutlashni ta'minlaydi. Bulutli hisoblashda TCP/IP virtual tarmoqlarni yaratish, yuklamani taqsimlash (load balancing), xavfsizlik devorlarini (firewalls) sozlash va boshqa ko‘plab tarmoq funksiyalarini amalga oshirish uchun asos bo‘lib xizmat qiladi. API (Application Programming Interface) chaqiruvlari, ma'lumotlar bazasiga ulanishlar va veb-xizmatlar asosan TCP/IP orqali amalga oshiriladi. Cheklov sifatida, ba'zan TCP ning "overhead"i (qo‘shimcha xizmatchi ma'lumotlar) real vaqt rejimida ishlaydigan yoki kechikishlarga o‘ta sezgir bo‘lgan ilovalar uchun muammo tug‘dirishi mumkin. Shuningdek, IP manzillarining (ayniqsa IPv4) cheklanganligi bulut provayderlari uchun NAT (Network Address Translation) kabi qo‘shimcha mexanizmlarni qo‘llashni taqozo etadi, bu esa ba'zan konfiguratsiyani murakkablashtirishi mumkin. IPv6 esa bu muammoni hal qilishga qaratilgan.

**HTTP/HTTPS (Hypertext Transfer Protocol/Secure HTTP)** standartlari veb-asosidagi ilovalar va xizmatlar uchun asosiy protokollardir. Kompaniyamizning CRM tizimi, shuningdek, ERP va WMS tizimlarining veb-interfeyslari asosan HTTP/HTTPS orqali ishlaydi. Bulutli xizmatlarning aksariyati (masalan, SaaS – Software as a Service) veb-brauzer orqali taqdim etiladi, bu esa HTTP/HTTPS ning muhimligini yanada oshiradi. HTTPS **ma'lumotlarni shifrlash** orqali uzatish xavfsizligini ta'minlaydi, bu esa mijozlar ma'lumotlari va tijorat sirlarini himoyalashda juda muhimdir. RESTful API'lar, keng tarqalgan bulut integratsiyasi usuli ham HTTP/HTTPS ga tayanadi. Bu standartlar bulutli hisoblashni **foydalanuvchilar uchun qulay va oson kirish mumkin** bo‘lishini ta'minlaydi. Cheklov sifatida, HTTP holatsiz (stateless) protokol bo‘lgani uchun, seanslarni boshqarish (session management) uchun qo‘shimcha mexanizmlar (masalan, cookies) talab etiladi. Katta hajmdagi fayllarni uzatishda yoki doimiy ulanishni talab qiluvchi ilovalarda HTTP ning samaradorligi cheklangan bo‘lishi mumkin, bu holatlarda WebSocket kabi texnologiyalar afzalroqdir.

**DNS (Domain Name System)** standartining bulutli hisoblashdagi ahamiyati shundaki, u foydalanuvchiga tushunarli domen nomlarini (masalan, crm.kompaniyanomi.uz) bulutdagi serverlarning IP manzillariga aylantirib beradi. Bu **xizmatlarga oson kirish**ni ta'minlaydi va IP manzillar o‘zgarganda ham (masalan, server masshtablanganda yoki boshqa joyga ko‘chirilganda) uzluksizlikni saqlashga yordam beradi. Bulut provayderlari ko‘pincha o‘zlarining boshqariladigan DNS xizmatlarini taklif qilishadi, bu esa **global yuklamani taqsimlash, geografik marshrutlash va uzluksizlikni ta'minlash (failover)** kabi ilg‘or funksiyalarni amalga oshirish imkonini beradi. Masalan, CRM tizimiga kelayotgan so‘rovlar foydalanuvchining geografik joylashuviga qarab eng yaqin ma'lumotlar markaziga yo‘naltirilishi mumkin. Cheklov sifatida, DNS so‘rovlarining o‘zi kechikishlarga sabab bo‘lishi mumkin (DNS propagation delays) va DNS tizimining o‘zi hujumlarga (masalan, DDoS) nishon bo‘lishi mumkin, bu esa xizmatlarning ishdan chiqishiga olib kelishi mumkin.

**VPN (Virtual Private Network)** texnologiyalari va ular bilan bog‘liq standartlar (masalan, IPsec, SSL/TLS) kompaniyaning lokal tarmog‘i va bulutdagi resurslari o‘rtasida yoki turli bulut muhitlari o‘rtasida **xavfsiz va shifrlangan ulanish kanalini** yaratish uchun keng qo‘llaniladi. Bu, ayniqsa, ERP va WMS kabi ichki tizimlarga masofadan xavfsiz kirishni ta'minlashda yoki gibrid bulut arxitekturalarida muhimdir. VPNlar ma'lumotlarning maxfiyligi va yaxlitligini himoya qiladi. Bulutli hisoblashni osonlashtirish nuqtai nazaridan, VPNlar kompaniyalarga o‘zlarining mavjud xavfsizlik siyosatlarini bulut muhitiga kengaytirish imkonini beradi. Cheklovlariga kelsak, VPN ulanishlari ba'zan **qo‘shimcha kechikishlar**ga olib kelishi va o‘tkazuvchanlik qobiliyatini cheklashi mumkin. VPN shlyuzlarini sozlash va boshqarish ham ma'lum texnik malakani talab qiladi.

**API standartlari**, xususan, **REST (Representational State Transfer)** va tobora ommalashib borayotgan **GraphQL**, bulutli xizmatlarning o‘zaro aloqasi va integratsiyasi uchun hal qiluvchi ahamiyatga ega. Kompaniyamizning ERP, CRM va WMS tizimlari turli modullardan iborat bo‘lishi va boshqa tashqi xizmatlar bilan integratsiyalashishi mumkin. RESTful API'lar HTTP metodlaridan (GET, POST, PUT, DELETE) foydalangan holda resurslarga kirishning sodda va standartlashtirilgan usulini taqdim etadi. Bu **xizmatlarning bir-biri bilan osongina "gaplashishi"** va ma'lumot almashishini ta'minlaydi, bu esa bulutdagi ilovalarning moslashuvchanligi va kengaytiriluvchanligini oshiradi. GraphQL esa mijozga faqat o‘zi so‘ragan ma'lumotlarni olish imkonini berib, ortiqcha ma'lumotlar uzatilishining (over-fetching/under-fetching) oldini oladi, bu esa mobil ilovalar va tarmoq o‘tkazuvchanligi cheklangan sharoitlarda afzalliklarga ega. Cheklov sifatida, yomon loyihalashtirilgan API'lar xavfsizlik bo‘shliqlariga yoki unumdorlik muammolariga olib kelishi mumkin. API versiyalarini boshqarish va orqaga qarab muvofiqlikni ta'minlash ham murakkab vazifa bo‘lishi mumkin.

Shuningdek, yuqorida sanab o‘tilgan umumiy tarmoq standartlari bulutli hisoblashning texnologik asosini tashkil etadi. Ular turli komponentlarning birgalikda ishlashini ta'minlab, kompaniyamizning ERP, CRM va WMS kabi tizimlarini bulutga muvaffaqiyatli ko‘chirish, ulardan samarali foydalanish va kelajakda kengaytirish uchun zarur shart-sharoitlarni yaratadi. Har bir standart o‘zining afzalliklari va cheklovlariga ega bo‘lib, ularni kompaniyaning o‘ziga xos talablari va bulut strategiyasi bilan birgalikda ko‘rib chiqish orqali eng maqbul tarmoq yechimlarini tanlash mumkin bo‘ladi.

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.

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.**

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**

Kompaniyamizning 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.

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.** Kompaniyamizning 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 kompaniyamizning 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**

Kompaniyaning ERP, CRM va WMS kabi muhim biznes tizimlarini bulut muhitiga o‘tkazish qarori nafaqat infratuzilmaning jismoniy joylashuvini o‘zgartiradi, balki operatsion tizimlarni (OT) boshqarish va optimallashtirish yondashuvlarini ham tubdan o‘zgartiradi. "Bulutli operatsion tizim" deganda, bu yerda asosan IaaS (Infrastructure as a Service) modelida virtual mashinalarda ishlaydigan standart server OTlari (masalan, Linux yoki Windows Server) yoki bulut platformasining o‘zining boshqaruv qatlami nazarda tutiladi. Ushbu OTlarni **masofadan turib optimallashtirish** kompaniyaning umumiy samaradorligiga sezilarli ijobiy ta'sir ko‘rsatishi mumkin.

Masofaviy optimallashtirish bir nechta asosiy jihatlarni o‘z ichiga oladi. Birinchidan, bu **unumdorlikni sozlash (performance tuning)**. Bulut provayderlari OT darajasida monitoring vositalarini taqdim etadi, bu esa protsessor yuklamasi, xotira ishlatilishi, disk operatsiyalari va tarmoq trafigi kabi ko‘rsatkichlarni real vaqt rejimida kuzatish imkonini beradi. Masalan, ERP tizimining ma'lumotlar bazasi serveri OTsi sekin ishlayotgan bo‘lsa, masofadan turib keraksiz jarayonlarni to‘xtatish, yadro parametrlarini (kernel parameters) moslashtirish yoki disk keshini optimallashtirish orqali unumdorlik oshirilishi mumkin. Bu, o‘z navbatida, hisobotlarning tezroq shakllanishiga va tranzaksiyalarning tezroq qayta ishlanishiga olib keladi, bu esa kompaniyaning kiyim-kechak ulgurji savdosi operatsiyalarini tezlashtiradi.

Ikkinchidan, **resurslarni boshqarish (resource management)** samaradorlikka bevosita ta'sir qiladi. Bulutli OTlarni masofadan optimallashtirish orqali resurslardan foydalanishni tahlil qilish va kerak bo‘lganda virtual mashinalarning hajmini (masalan, CPU soni, RAM miqdori) dinamik ravishda o‘zgartirish mumkin (vertical scaling). Shuningdek, yuklama oshganda yangi instansiyalarni avtomatik qo‘shish (horizontal scaling) va yuklama kamayganda ularni o‘chirish orqali xarajatlar tejaladi va tizimning doimiy yuqori unumdorligi ta'minlanadi. Misol uchun, CRM tizimi yangi marketing kampaniyasi davrida ko‘proq trafikni qabul qilsa, uning OTlari uchun ajratilgan resurslar masofadan turib avtomatik kengaytirilishi, kampaniya tugagach esa asl holiga qaytarilishi mumkin. Bu esa resurslarning behuda sarflanishining oldini oladi va tizimning javob qaytarish vaqtini (response time) optimallashtiradi.

Uchinchidan, **xavfsizlikni mustahkamlash (security hardening)** masofaviy optimallashtirishning muhim qismidir. OTlarni muntazam ravishda yangilab turish (patch management), xavfsizlik konfiguratsiyalarini markazlashtirilgan holda qo‘llash, kirish huquqlarini (access controls) qat'iy nazorat qilish va zararli dasturlardan himoya vositalarini masofadan boshqarish orqali ERP, CRM va WMS tizimlaridagi maxfiy ma'lumotlar himoyasi kuchaytiriladi. Bulut provayderlari ko‘pincha bu vazifalarni avtomatlashtirish uchun maxsus xizmatlar (masalan, AWS Systems Manager Patch Manager, Azure Update Management) taklif qiladi. Xavfsizlikning proaktiv tarzda boshqarilishi potentsial buzilishlarning oldini oladi, bu esa kompaniyaning obro‘siga va moliyaviy holatiga zarar yetkazilishining oldini oladi.

To‘rtinchidan, **avtomatlashtirilgan konfiguratsiya boshqaruvi (automated configuration management)** samaradorlikni oshirishda katta rol o‘ynaydi. Ansible, Chef, Puppet kabi vositalar yordamida OT konfiguratsiyalarini kod sifatida belgilash (Infrastructure as Code) va ularni barcha serverlarga (masalan, WMS ilovasi serverlariga) bir xilda va avtomatik tarzda qo‘llash mumkin. Bu nafaqat vaqtni tejaydi, balki inson xatosi tufayli yuzaga keladigan nomuvofiqliklarning ham oldini oladi, tizimlarning barqaror va bashorat qilinadigan tarzda ishlashini ta'minlaydi. Yangi serverni ishga tushirish kerak bo‘lganda, oldindan belgilangan konfiguratsiya avtomatik ravishda qo‘llanilishi, tizimni tezda foydalanishga topshirish imkonini beradi.

Masofaviy optimallashtirishning samaradorlikka ta'siri quyidagilarda namoyon bo‘ladi:

**Operatsion xarajatlarning kamayishi:** Resurslardan samarali foydalanish, avtomatlashtirish va IT xodimlarining qo‘l mehnatining qisqarishi tufayli xarajatlar tejaladi.

**Tizimning ish vaqtining (uptime) oshishi:** Proaktiv monitoring, tezkor muammolarni bartaraf etish va avtomatlashtirilgan tiklash jarayonlari tizimlarning uzluksiz ishlashini ta'minlaydi.

**Unumdorlikning yaxshilanishi:** OT darajasidagi optimallashtirishlar ERP, CRM va WMS tizimlarining tezroq va samaraliroq ishlashiga olib keladi.

**Chaqqonlikning (agility) ortishi:** Biznes ehtiyojlari o‘zgarganda resurslarni va konfiguratsiyalarni tezda moslashtirish imkoniyati kompaniyaning bozor o‘zgarishlariga tezkor javob berishiga yordam beradi.

**Xavfsizlik darajasining oshishi:** Markazlashtirilgan va avtomatlashtirilgan xavfsizlik boshqaruvi ma'lumotlar xavfsizligini kuchaytiradi.

Xulosa qilib aytganda, bulutli operatsion tizimlarni masofadan turib optimallashtirish kompaniyamizning IT infratuzilmasini boshqarishda muhim strategik yondashuv bo‘lib, u nafaqat texnik samaradorlikni oshiradi, balki biznes jarayonlarining uzluksizligi, xavfsizligi va iqtisodiy samaradorligiga ham bevosita ijobiy ta'sir ko‘rsatadi. Bu esa, o‘z navbatida, tayyor kiyim-kechak mahsulotlarini ulgurji yetkazib berish faoliyatining umumiy raqobatbardoshligini oshirishga xizmat qiladi.

C.P5

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

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).

C.P6

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

Yuqorida loyihalashtirilgan tarmoq yechimini amalga oshirish quyidagi asosiy bosqichlarni o‘z ichiga oladi. Bu yerda VPC asosidagi yechimning umumiy amalga oshirilishi tasvirlanadi, Heroku platformasidagi amaliy yuklash jarayonlarini esa siz o‘z ishingizda batafsil yoritishingiz mumkin bo‘ladi.

1. **Bulut Provayderi va Mintaqa Tanlash:** Kompaniyaning ehtiyojlari, narxlar va geografik joylashuviga qarab mos bulut provayderi (masalan, AWS, Azure) va asosiy mintaqa tanlanadi.
2. **VPC Yaratish:** Tanlangan provayderning boshqaruv konsoli yoki buyruqlar qatori interfeysi (CLI) orqali IP manzillar diapazoni (CIDR bloki) belgilanib, yangi VPC yaratiladi.
3. **Kichik Tarmoqlar, Shlyuzlar va Marshrutlash Jadvallarini Sozlash:** Loyihaga muvofiq ommaviy va xususiy kichik tarmoqlar yaratiladi. Internet Shlyuzi va NAT Shlyuzi (kerak bo‘lsa) sozlanib, marshrutlash jadvallari trafikni to‘g‘ri yo‘naltirish uchun konfiguratsiya qilinadi.
4. **Xavfsizlik Guruhlarini Konfiguratsiya Qilish:** Har bir xizmat (ERP, CRM, WMS) va komponent uchun minimal imtiyoz tamoyiliga (principle of least privilege) asoslangan holda batafsil xavfsizlik guruhlari qoidalari yaratiladi.
5. **Virtual Mashinalarni Joylashtirish:** ERP, CRM va WMS tizimlarining serverlari uchun mos o‘lchamdagi virtual mashinalar tanlangan kichik tarmoqlarga joylashtirilib, operatsion tizimlar va kerakli dasturiy ta'minot o‘rnatiladi.
6. **VPN/Maxsus Ulanishni O‘rnatish:** Kompaniyaning lokal tarmog‘i va bulutdagi VPC o‘rtasida xavfsiz ulanish kanali (VPN tunnel yoki maxsus ulanish) sozlanadi.
7. **Yuklama Taqqsimlagichlarni Sozlash:** Ommaviy kichik tarmoqlarda yuklama taqsimlagichlar o‘rnatilib, ular tegishli backend serverlariga (masalan, CRM veb-serverlari) trafikni yo‘naltirish uchun konfiguratsiya qilinadi.
8. **DNS Yozuvlarini Konfiguratsiya Qilish:** Xizmatlar uchun (masalan, erp.kompaniyanomi.uz, crm.kompaniyanomi.uz) ommaviy va (kerak bo‘lsa) xususiy DNS yozuvlari yaratiladi.

Heroku platformasida joylashtiriladigan komponentlar uchun amalga oshirish jarayoni odatda quyidagilarni o‘z ichiga oladi (buni siz amaliy ishingizda kengroq yoritasiz):

* Heroku da yangi ilova yaratish.
* Dastur kodini Heroku ga yuklash (masalan, Git orqali).
* Kerakli qo‘shimcha xizmatlarni (add-ons, masalan, ma'lumotlar bazasi, kesh) sozlash.
* Maxsus domen nomlarini (custom domains) bog‘lash va SSL sertifikatlarini sozlash.

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 kompaniyamizning 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

Aa

Xulosa

Aa

ADABIYOTLAR RO'YXATI

1. Aguinis, H., & Kraiger, K. (2009). Benefits of training and development for individuals and teams, organizations, and society. *Annual Review of Psychology*, *60*(1), 451-474. [https://www.annualreviews.org/doi/abs/10.1146/annurev.psych.60.110707.163505](https://www.google.com/url?sa=E&source=gmail&q=https://www.annualreviews.org/doi/abs/10.1146/annurev.psych.60.110707.163505)