

11-Mavzu.Ma'lumotlar bazasi xavfsizligi qismtizimining arxitekturasi va ishlash prinsipi

“S2” xavfsizlik sinfi

Ma'lumotlar bazasini boshqarish tizimlari, ayniqsa relyatsion MBBTlari, axborotning katta massivlarini saqlashda ustun instrument bo'lib qoldi. Bir qadar rivojlangan ilovalar operatsion tizimning fayl strukturalariga emas, balki mijoz/server texnologiyasida bajarilgan ko'pchilik foydalanuvchi MBBTga ishonadi. Shu sababli MBBTning, birinchi navbatda uning server komponentlarining, axborot xavfsizligini ta'minlash butun tashkilot xavfsizligi uchun hal qiluvchi ahamiyatga ega.

Yuqorida aytib o'tilganidek, MBBT uchun axborot xavfsizligining uchta asosiy jihatlari - konfidensiallik, yaxlitlik va foydalanuvchanlik muhim hisoblanadi.

Ma'lumotlar bazasini himoyalashning umumiy g'oyasi "Ishonchli kompyuter tizimlarini baholash mezonlari"da S2 xavfsizlik sinfi uchun ta'riflangan tavsiyalarga rioya qilishdan iborat. Umuman, ba'zi MBBTlar VI sinfiga xos qo'shimchalar taklif etadi, ammo bunday qo'shimchalarni amalda qo'llash faqat tashkilot axborot strukturasi barcha komponentlari xavfsizlikning V kategoriyasiga ega bo'lgandagina ma'no kasb etadi. Bunga erishish texnik va moliya nuqtayi nazaridan murakkab.

Undan tashqari quyidagi ikkita jihatni hisobga olish kerak. Birinchidan, aksariyat tijoriy tashkilotlar uchun xavfsizlikning S2 sinfi yetarli. Ikkinchidan, yaxshi himoyalangan versiyalar ma'nodorligi va imkoniyatlari bo'yicha oddiy "kasbdoshlar" idan orqada qoladi. Shuning sababli maxfiylik uchun kurashuvchilar aslida ma'naviy eskirgan (garchi sinchiklab tekshirilgan) mahsulotlardan foydalanishga majburlar.

Identifikatsiya va foydalanuvchilarning haqiqiylikni tekshirish.

Odatda, MBBTda foydalanuvchilarni identifikatsiyalash va ularni haqiqiylikni tekshirish uchun operatsion tizimning mos mexanizmlari, yoki SQL-CONNECT operatori qo'llaniladi.

Masalan, *ORACLE* MBBT holida CONNECT operatori quyidagi ko'rinishga ega bo'ladi:

```
CONNECT foydalanuvchi [parol] [@ma'lumotlar_bazasi].
```

Har holda, ma'lumotlar bazasi serveri bilan ishlash seansining boshlanishi onida foydalanuvchi o'zining nomi bilan identifikatsiyalanadi, autentifikatsiya vositasi sifatida esa parol ishlatiladi. Ushbu jarayonning tafsilotlari ilovaning mijoz qismining amalga oshirilishi orqali aniqlanadi.

UNIX kabi ba'zi operatsion tizimlar dastur ishga tushirilishi vaqtida amaldagi foydalanuvchi identifikatorini o'zgartirishga imkon beradi. Ma'lumotlar bazasi bilan ishlovchi ilova odatda, oddiy foydalanuvchilar imtiyozlariga nisbatan ancha ortiqcha imtiyozlarga ega. Tabiiyki, bunda ilova puxtalik bilan o'ylangan, qat'iy

belgilangan imkoniyatlar naborini taqdim etadi. Agar foydalanuvchi u yoki bu usul yordamida ilovani nihoyasiga yetkaza olsa, ammo ma'lumotlar bazasining serverga ulanishini asray olsa, u ma'lumotlar bilan har qanday harakatlarni bajarishi mumkin.

Foydalanishni boshqarish

Foydalanishni boshqarish bilan bog'liq masalalarni oydinlashtirish uchun *INGRES* MBBT ishlatiladi. Odatda MBBTda foydalanishni ixtiyoriy boshqarish qo'llaniladi. Bunda obyekt egasi undan foydalanish huquqini (ko'pincha imtiyozini deb yuritishadi) o'z ixtiyoricha beradi. Imtiyozlar subyektlarga (alohida foydalanuvchilarga), guruhlariga, rol larga yoki barcha foydalanuvchilarga berilishi mumkin.

Rollar imtiyozlari foydalanuvchilar va guruhlar imtiyozlaridan ustun turadi.

Boshqacha aytganda, subyekt sifatidagi foydalanuvchining ma'lum rolli ilovalar ishlov beruvchi obyektlardan foydalanish huquqiga ega bo'lishi shart emas.

Ta'kidlash lozimki, *ORACLE* MBBTda rol deganda imtiyozlar nabori tushuniladi. Bunday roller imtiyozlarni strukturalash vositasi sifatida xizmat qiladi va ularning modifikatsiyalanishini osonlashtiradi.

PUBLIC

Barcha foydalanuvchilar majmui PUBLIC deb ataladi.

PUBLICga imtiyozlar berilishi - foydalanishning ko'zda tutilgan huquqlarini berishning qulay usuli. Turli foydalanuvchilar zimmasiga turli ma'lumotlar bazasini ma'murlashru yuklash ma'noga ega bo'ladi, qachonki ushbu bazalar mustaqil va ularga nisbatan imtiyozlarni ajratishning kelishilgan siyosatini yoki rezervli nusxalashni o'tkazishga to'g'ri kelmasa. Bu holda har bir ma'mur qancha zarur bo'lsa, shuncha biladi.

Bir tomondan *INGRES* foydalanuvchisi va ma'lumot bazasi, ikkinchi tomondan operatsion tizim superfoydalanuvchi (OS UNIX holda root) va xizmatchi foydalanuvchilar (OS UNEXda bu-bin, Ip, UUCP va h. bo'lishi mumkin) orasidagi o'xshashlikni kuzatish mumkin. Xizmatchi foydalanuvchilarning kiritilishi superfoydalanuvchi imtiyozlarini olmasdan funktsional qismlarni ma'murlashga imkon beradi.

Xuddi shu tarzda serverda saqlanuvchi ma'lumotlarni bo'lmalarga ajratish mumkin. Bitta bo'lma ma'murining obro'sizlantirilishi, albatta boshqa bo'lma ma'murining obro'sizlantirilishi degani emas.

Imtiyoz turlari

MBBTda imtiyozlarni ikkita kategoriyaga ajratish mumkin: xavfsizlik imtiyozlari va foydalanish imtiyozlari.

Xavfsizlik imtiyozlari doim muayyan foydalanuvchiga uning yaratilishi (CREATE USER operatori yordamida) yoki xarakteristikalarini o'zgartirish (ALTER USER operatori yordamida) vaqtida ajratiladi. Bunday imtiyozlar beshta:

- security — MBBT xavfsizligini boshqarish va foydalanuvchi harakatlarini kuzatish huquqi. Foydalantuvchi ushbu imtiyoz bilan har qanday ma'lumotlar bazasiga ulanishi, foydalanuvchilar, guruhlar va rollar xarakteristikalarini yo'q qilishi va o'zgartirishi, ma'lumotlar bazasidan foydalanish huquqini boshqa foydalanuvchiga berishi, qayd qilinuvchi axborotning yozilishini boshqarishi, boshqa foydalanuvchilar so'rovini kuzatishi vanihoyat, boshqa foydalanuvchilar nomidan INGRES-komandalami ishga tushirishi mumkin. Security imtiyozi ma'lumotlar bazasi serverining ma'muriga hamda axborot xavfsizligiga shaxsan javobgar shaxsga zarur. Ushbu imtiyozni boshqa foydalanuvchilarga berish (masalan, ma'lumotlar bazasi ma'muri tomonidan) ma'lumotlar bazasi serverining himoyasidagi bo'lishi mumkin boigan zaif joylarni ko'paytiradi;

“Createdb” ma'lumotlar bazasini yaratish va yo'q qilish huquqi

Ushbu imtiyozga server ma'muridan tashqari foydalanuvchilar ega bo'lishlari lozim. Foydalanuvchilar ixtiyoriga alohida ma'lumotlar bazasining ma'murlari roli taqdim etiladi;

- operator - odatda operator ixtiyoridagi harakatlarni bajarish huquqi. Servemishga tushirish va to'xtatish, axborotni saqlash va tiklash ko'zda tutiladi. Ushbu imtiyozni server va ma'lumotlar bazasi ma'muridan tashqari operatsion tizim ma'muriga ham berish maqsadga muvofiq hisoblanadi;

- maintain locations - ma'lumotlar bazasi serveri ma'murining bazasi va operatsion tizim o'mashgan joyni boshqarish huquqi;

“Trace”

- **trace** - sozlovchi trassirovka flaglari xolatlarini o'zgartirish huquqi. Ushbu imtiyoz murakkab, tushunarsiz vaziyatlarni tahlillashda ma'lumotlar bazasi serveri ma'muriga va boshqa tajribali foydalanuvchilarga foydali. Xavfsizlik imtiyozlari ma'muriy harakatlar bajarishga imkon beradi. Foydalanish imtiyozlari, nomiga muvofiq, subyektlarning ma'lum obyektlardan foydalanish huquqini belgilaydi va foydalanuvchilarga, guruhlarga, rollarga yoki barchaga GRANT operatori yordamida ajratiladi va REVOKE operatori yordamida olib qo'yiladi.

Ushbu imtiyozlar odatda, mos obyekt egasi (ma'lumotlar bazasi ma'muri) yoki security imtiyoziga ega shaxs (odatda ma'lumotlar bazasi serveri) tomonidan beriladi.

Operatorlar

Guruhlarga va rollarga imtiyozlarni berishdan oldin ularni CREATE GROUP va CREATE ROLE operatorlari yordamida yaratish lozim.

Guruh tarkibini o'zgartirish uchun ALTER GROUP operatori xizmat qiladi. DROP GROUP operatori guruhlarni yo'q qilishga imkon beradi (faqat guruh a'zolari ro'yxati yo'q qilinganidan so'ng).

ALTER ROLE operatori rollar parollarini o'zgartirishga, DROP ROLE operatori esa rollami yo'q qilishga xizmat qiladi. Yuqorida aytib o'tilganidek, imtiyozlarning nomlangan eltuvchilarini yaratish va yo'q qilish hamda ularning xarakteristikalarini o'zgartirish, faqat security imtiyoziga ega foydalanuvchi tomonidan amalga oshirilishi mumkin. Bunday harakatlar amalga oshirilganda, tarkibida subyektlar va ularning imtiyozlari saqlanuvchi ma'lumotlar bazasiga ulanishga ega bo'lish lozim.

INGRES

Foydalanish imtiyozlarini ular taalluqli obyektlar turi bo'yicha ajratish mumkin. INGRES MBBTda bunday turlar beshta:

- jadvallar va tasavvurlar;
- muolajalar;
- ma'lumotlar bazasi;
- ma'lumotlar bazasi serveri;
- hodisalar.

GRANT operatori

Foydalanish imtiyozlarini berish GRANT operatori yordamida amalga oshiriladi. GRANT operatori umumiy ko'rinishda quyidagi formatga ega:

- GRANT imtiyozlar;
- ON obyektlar;
- TO kimga.

Jadvallar va tasavvurlarga muvofiq quyidagi foydalanish huquqlarini boshqarish mumkin:

SELECT - ma'lumotlarni tanlash huquqi;
INSERT - ma'lumotlarni qo'shish huquqi;
DELETE - ma'lumotlarni yo'q qilish huquqi;
UPDATE - ma'lumotlarni yangilash huquqi (yangilanishga ruxsat bo'lgan ma'lum ustunlarni ko'rsatish mumkin);

REFERENCES

REFERENCES - berilgan jadvalga (ma'lum ustunlarni ko'rsatish mumkin) havola qiluvchi tashqi kalitlardan foydalanish huquqi. Odatda, foydalanuvchi jadvallardan va tasavvurlardan foydalanishning hech qanday huquqiga ega emas. Bu huquqlarni GRANT operatorlari yordamida berish mumkin.

Muolajalarga nisbatan bajarish huquqi berilishi mumkin. Bunda muolajalar ishlov beruvchi obyektlardan foydalanish huquqlarining ajratilishi xususida o'ylash kerak emas, ularning mavjudligi shart emas. Shunday qilib, ma'lumotlar bazasi muolajalari ma'lumotlar ustida qat'iy belgilangan harakatlarni bajarish uchun nazoratni foydalanisirni taqdim etishning qulay vositasi hisoblanadi.

Ma'lumotlar bazasidan foydalanish huquqlarini uning ma'muri yoki security imtiyoziga ega foydalanuvchi taqdim etishi mumkin.

Ushbu “huquqlar” aslida ma’lumotlar bazasidan foydalanishga qator cheklashlar o‘rnatadi, ya’ni mohiyatan taqiqlovchi hisoblanadi. Kiritish/chiqarish amallar soniga yoki bitta so‘rov bilan qaytariluvchi qator soniga cheklash, jadvallar va muolajalar yaratish huquqiga cheklash ko‘zda tutiladi. Odatda foydalanuvchi miqdoriy limitlar bilan qoniqmaydi va bazada obyektlar yaratish huquqini oladi.

Ta’kidlash lozimki, ma’lumotlar bazasini yaratishda uning maqomi (umumiy yoki shaxsiy) ko‘rsatiladi. Bu bazadan nazarda tutilgan foydalanish huquqiga ta’sir etadi. Odatda umumiy bazaga ulanish huquqi barchaga beriladi. Shaxsiy bazaga ulanish huquqi oshkora ravishda berilishi lozim. Ulanishga huquq baza va undagi obyektlar bilan boshqa barcha amallarni bajarish uchun kerak.

Agar optimizator oldindan so‘rov kiritish/chiqarish amaliga yoki qaytariluvchi qatorga ajratilgan limit sonidan oshganini aytsa, so‘rov rad etiladi. Bu xildagi miqdoriy cheklashlarning qo‘yilishi servemning bitta mijoz tomonidan monopoliya qilinishiga to‘sqinlik qiladi va yuqori tayyorlikni madadlash instrumentining biri sifatida ishlatilishi mumkin.

Oldin berilgan imtiyozlarni (ruxsat beruvchi va taqiqlovchi) bekor qilishda REVOKE operatori xizmat qiladi.

Foydalanishni boshqarishda tasawurlardan foydalanish.

MBBT foydalanishni boshqaruvchi o‘ziga xos vosita – tasawurlarni taqdim etadi. Tasavvurlar subyektlar uchun bazaviy jadvallarning ma’lum qatorlarining ko‘rinarli bo‘lishiga (proeksiyani amalga oshirishga) yoki ma’lum qatorlarni tanlashga (seleksiyani amalga oshirishga) imkon beradi. Ma’lumotlar bazasining ma’muri subyektlarga bazaviy jadvallardan foydalanish huquqini bermasdan va munosib tasavvurlarni tuzib, jadvallarni ruxsatsiz foydalanishdan himoyalaydi va har bir foydalanuvchini o‘zining ma’lumotlar bazasiga qarashi bilan ta’minlaydi.

Quyida tarkibida dastlabki jadvalning ikkita ustuni bo‘lgan va o‘z ichiga faqat ustunlarni birining ma’lum qiymatli qatorini qamrab oluvchi tasavvurni yaratish misoli keltirilgan:

```
CREATE VIEW empview AS
```

```
SELECT name, dept
```

```
FROM employee
```

```
WHERE dept = 'shoe';
```

Ushbu tasavvurdan tanlash huquqi barchaga berilganida:

```
GRANT SELECT
```

```
ON empview
```

```
TO PUBLIC;
```

“Empview”

Empview tasavvurdan foydalanishni amalga oshiruvchi subyektlar “shoe”dan farqlanuvchi bo‘limlar xususidagi ma’lumotlarni so‘rashga intilishlari mumkin, masalan:

SELECT *

FROM empview

WHERE dept = 'toy';

ammo javob tariqasida foydalanish huquqlarining buzilganligini ko'rsatuvchi javob kodini emas, balki oddiygina nulli qatorli natijani oladilar. Bu juda muhim, chunki niyati buzuvchi bo'lmishlar ro'yxatini javob kodlarini tahlillash orqali bilvosita tarzda olish imkoniyatidan mahrum etadi.

Foydalanish huquqlarining ierarxiyasi

GRANT operatori va MBBTdan foydalanishni boshqaruvchi boshqa vositalar foydalanishning quyidagi cheklashlar turini amalga oshirishga imkon beradi:

- amaliy cheklashlar (jadvalning barcha yoki faqat ba'zi ustunlariga qo'llaniluvchi SELECT, INSERT, UPDATE, DELETE foydalanish huquqlari hisobiga);
- muhimligi bo'yicha cheklashlar (tasawurlar mexanizmi hisobiga);
- resurslarga cheklashlar (ma'lumotlar bazasidan foydalanish imtiyozlari bo'yicha).

So'rovlarni ishlashda MBBT avval obyektlardan foydalanish huquqini tekshiradi. Agar amaliy cheklashlar buzilgan bo'lsa, so'rov mos tashxis chiqarilib, rad etiladi. Muhimligi bo'yicha cheklashlarning buzilishi faqat natijaviy qatorlarning soniga ta'sir etadi, bunda hech qanday tashhis chiqarilmaydi. Nihoyat, oldingi ikkita cheklashlar hisobga olinganidan so'ng, so'rov ishlanish uchun optima qatorga beriladi.

Agar optimizator resurslarga cheklashlar oshirilganini aniqlasa, so'rov mos tashhis chiqarilib, rad etiladi. Imtiyozlar ierarxiyasiga boshqa nuqtayi nazardan qarash mumkin. Har bir foydalanuvchi o'zidan tashqari PUBLIC imtiyoziga ega. Undan tashqari, u turli guruhlarda bo'lib, ma'lum roller bilan ilovalarni ishga tushirishi mumkin. Quyida imtiyozlarning nomlangan turli eltuvchilari taqdim etgan huquqlarning o'zaro munosabati xususida so'z ketadi.

INGRES MBBT uchun avtorizatsiya ierarxiyasi quyidagi ko'rinishga ega:

- rol (yuqori ustuvorlik);
- foydalanuvchi;
- guruh;
- PUBLIC (past ustuvorlik).

Har bir foydalanuvchi obyekt uchun INGRES foydalanishning so'raluvchi turiga (SELECT, EXECUTE va h.) tegishli ierarxiyadagi imtiyozni qidirishga urinadi. Masalan, yangilash maqsadida jadvaldan foydalanishga urinishda INGRES rolning, foydalanuvchining, guruhning va barcha foydalanuvchilarning imtiyozlarini tekshiradi. Agar ierarxiyaning bitta sathida UPDATE imtiyozi bo'lsa ham, so'rov keyingi ishlash uchun uzatiladi. Aks holda, so'rovni rad etishni ko'zda tutuvchi foydalanish huquqi ishlatiladi.

Xavfsizlik belgilari va foydalanishni majburiy nazoratlash

Yuqorida xavfsizlikning S sathiga xos foydalanishni ixtiyoriy boshqarish vositalari tavsiflangan edi. Ma'lumki, ular umuman aksariyat tijoriy ilovalarga yetarli.

Shunday bo'lsa-da, ular bitta juda muhim masalani - axborot uzatilishini kuzatish masalasini yechmaydi.

Foydalanishni ixtiyoriy boshqarish vositalari avtorizatsiyalangan foydalanuvchiga maxfiy axborotni qonuniy tarzda olishga va so'ngra undan boshqa avtorizatsiyalanmagan foydalanuvchilarning foydalanishlariga xalaqit bermaydi. Chunki foydalanishni ixtiyoriy boshqarishda imtiyozlar ma'lumotlardan alohida joylashadi (relyatsion MBBTlarda esa relyatsion jadvallar qatoridan alohida joylashadi).

Natijada ma'lumotlar "egasiz qoladi" va ularning kimga bo'lsa ham uzatilishiga hech nima xalaqit bermaydi (hatto MBBT vositalari ham).

Xavfsizlik sathi tizimi Bga muvofiq "Ishonchli kompyuter tizimlarini baholash mezonlari"da INGRES/Enhanced Security (xavfsizligi oshirilgan INGRES) versiyada amalga oshirilgan xavfsizlik belgilari mexanizmi tavsiflangan. Ushbu versiyani amalda qo'llash faqat operatsion tizim va xavfsizlik B sathiga ega boshqa dasturiy komponentlar bilan birgalikda amalga oshirilganida ma'noga ega bo'ladi. Shunday bo'lsa ham, INGRES MBBTda belgisi xavfsizlikning amalga oshirilishini ko'rish, bilish nuqtayi nazaridan qiziqarli, ma'lumotlarni maxflylik sathlari va foydalanish kategoriyalariga ajratishga asoslangan yondashishning o'zi esa, ko'pgina foydalanuvchilarning ma'lumotlarning katta massivlariga nisbatan imtiyozlari tizimini loyihalashda foydali bo'lishi mumkin.

INGRES/Enhanced Security

INGRES/Enhanced Security MBBTda har bir relyatsion jadvalga yashirincha jadval qatori xavfsizligi belgisi bo'lgan ustun qo'shiladi. Xavfsizlik belgisi uchta komponentdan iborat:

Maxflylik sathi. Ushbu komponentning mazmuni ilovaga bog'liq. Xususan, sathlarning an'anaviy spektri "mutlaqo maxfiy"dan "maxfiy emas" gacha bo'lishi mumkin.

Kategoriyalar. Kategoriya tushunchasi ma'lumotlarni "bo'lmalar" ga ajratishga va natijada xavfsizlik tizimi ishonchliligini oshirishga imkon beradi. Tijoriy ilovalarda kategoriya sifatida "moliyalar", "kadrlar", "moddiy boyliklar" xizmat qilishi mumkin.

Hududlar

Axborotni bo'lmalarga ajratishda qo'shimcha vosita hisoblanadi. Amalda "hudud" komponenti, haqiqatan geografik mazmunga (masalan, ma'lumot taalluqli mamlakatga) ega bo'lishi mumkin.

INGRES/Enhanced- Security MBBTning har bir foydalanuvchisi ishonchlilik darajasi orqali xarakterlanadi. Ishonchlilik darajasi foydalanuvchiga berilgan xavfsizlik belgisi orqali ham aniqlanadi. Foydalanuvchi, agar uning ishonchlilik darajasi mos xavfsizlik belgisi talablarini qondirsa, ma'lumotlardan foydalanishi mumkin, yanada aniqrog'i:

- foydalanuvchining maxfiylik sathi ma'lumotlarning maxflylik sathidan past bo'lmashligi shart;

- ma'lumotlar xavfsizligi belgisidagi kategoriyalar nabori butunlay foydalanuvchi xavfsizligi belgisida bo'lishi shart;
- foydalanuvchi xavfsizligi belgisidagi hududlar nabori butunlay ma'lumotlar xavfsizligi belgisida bo'lishi shart

“DOWNGRADE”

Maxsus imtiyoz DOWNGRADE ma'lumotlar bilan assotsiatsiyalangan xavfsizlik belgisini o'zgartirishga imkon beradi. Bunday imkoniyat, masalan, u yoki bu sabab bilan noto'g'ri bo'lib qolgan belgilarni tuzatish uchun zarur.

Tabiiyki, INGRES/Enhanced Security MBBTi reyatsion jadvallarga xavfsizlik belgisini nafaqat yashirincha, balki ochiq holda kiritishga yo'l qo'yadi. Mos taqqoslash amallarini madadlovchi ma'lumotlarning yangi turi security label paydo bo'ladi.

INGRES/Enhanced Security - xavfsizlikning V sinfiga sertifikat (attestatsiyaga ekvivalent) olgan birinchi MBBT hisoblanadi. Ehtimol, xavfsizlik belgilari asta-sekin ma'lumotlar bazasini boshqarish tizimining standart repertuariga kiradi.

MBBT da ma'lumotlar yaxlitligini madadlash

Tijoriy tashkilotlar uchun ma'lumotlar yaxlitligini ta'minlashning konfidensiallikni ta'minlashga nisbatan muhimligi kam emas. Shubhasiz, mijozlarning hisob raqamidagi mablag'ni mo'ralab ko'rish ko'ngilsiz hodisa hisoblanadi. Hisob raqamidan hisob raqamiga pul o'tkazishda mablag'ning norna'lum yo'nalishda yo'qolishi esa undan battar noxush hodisa hisoblanadi.

Ma'lumki, ma'lumotlar bazasining asosiy dushmani tashqaridagi niyati buzuvchi emas, balki uskunaning, ma'murlarning, tatbiqiy dasturlarning va foydalanuvchilarning yangilishi.

MBBTi foydalanuvchisi nuqtayi nazaridan ma'lumotlar yaxlitligini madadlashning asosiy vositalari cheklashlar va qoidalar hisoblanadi.

Cheklashlar

Cheklashlar jadvallarga yoki alohida ustunlarga taalluqli bo'lishi mumkin.

Ustunlarga cheklashlar CREATE TABLE operatorida jadvalni yaratishda beriladi.

Jadval cheklashlari ustunlar guruhiga taalluqli va jadval yaratishda, yoki kechroq, ALTER TABLE operatori yordamida berilishi mumkin.

Havolali cheklashlar jadval orasidagi aloqaning yaxlitligiga javob beradi.

Bunday cheklashning talabiga binoan bitta har bir qiymatga boshqa jadvaldagi roppa-rosa bitta qiymat mos kelishi lozim. Bunday qiymatlar relyatsion modeldagi jadval orasida havola rolini o'ynaydi.

Cheklashlarning barcha turlari jadval egasi tomonidan yuklanadi va keyingi ma'lumotlar bilan amallar natijasiga ta'sir qiladi. SQL-operatorming bajarilishi tugashidan avval mavjud cheklashlar tekshiriladi. Buzilishlar aniqlanganida MBBT nonormal tugallanish xususida xabar beradi va operator kiritgan o'zgarishlarni bekor qiladi. Ta'kidlash lozimki, havolali cheklashni yuklash uchun havola

qilinayotgan jadvalga nisbatan REFERENCES imtiyoziga ega bo'lish lozim (yuqoridagi misoldagi dept).

Cheklashlarni nafaqat yuklash, balki bekor qilish mumkin. Bunda cheklashlar orasida bog'lanishlar bo'lishi mumkin va ulardan birining bekor qilinishi boshqa (havolali) cheklashlarning yo'q qilinishini talab qilishi mumkin. INGRES MBBTda cheklashlarni nazoratlash bilan ishlash samaradorligini muvosiqa keltirishga urinishadi. Ma'lumotlarni ommaviy nusxalashda cheklashlarni nazoratlash o'chirib qo'yiladi. Bu degani, nusxalashni yaxlitlikni tekshirishning global muvosiqasini ishga tushirish bilan to'ldirish lozim.

Qoidalar

Qoidalar ma'lumotlar bazasidagi ma'lum o'zgarishlar bo'lganida berilgan harakatlarni bajarilishini chaqirishga ixlos beradi. Odatda, harakat - muvosiqasi chaqirish. Qoidalar jadvallar bilan assotsiatsiyalanadi va ushbu jadvallar o'zgarishida ishga tushadi.

Qoidalar faqat nisbatan oddiy shartlarni nazoratlash vositalari hisoblanuvchi cheklashlardan farqli holda, bazadagi ma'lumotlar elementlari orasidagi xohlaganicha murakkab o'zaro bog'lanishni tekshirishga va madadlashga imkon beradi. Cheklashlar holdagiga o'xshab qoidalarni tekshirish nusxalashning ommaviy amallarida to'xtatiladi. Ma'lumotlar bazasi ma'muri ham SETNOROLES operatoridan foydalanib, qoidalarni tekshirishni oshkora to'xtatishi mumkin. SETRULES operatori qoidalar mexanizmi ishini tiklashi mumkin. Odatda ushbu mexanizm ulangan bo'ladi.

Qoidalarni yo'q qilish DROP RULE qoida operatori orqali amalga oshiriladi. Mos jadval yo'q qilingan holda MBBT avtomatik tarzda qoidalarning yo'q qilinishini ta'minlaydi. Shu tariqa jadvallar va qoidalar yaxlitligi ta'minlanadi.

Axborot xavfsizligi nuqtayi nazaridan ta'kidlash lozimki, jadval bilan assotsiatsiyalangan qoidani mos muvosiqalarni bajarish huquqini ushbu jadval egasi yaratishi mumkin. Harakati qoidani ishlashiga sabab bo'luvchi foydalanuvchi faqat jadvaldan foydalanishning kerakli huquqlariga ega bo'lishi shart. Shu tariqa qoidalar oshkora bo'lmagan holda foydalanuvchilar imtiyozlarini kengaytiradi. Bunday kengayishlar qat'iy ma'muriy nazoratga ehtiyoj sezadi, chunki xatto qoidaning yoki assotsiatsiyalangan muvosiqaning biroz o'zgarishli ma'lumotlar himoyalanganligiga tubdan ta'sir etishi mumkin. Qoidalarning murakkab tizimidagi xatolik esa bashorat qilib bo'lmaydigan oqibatlariga sabab bo'ladi.

Tuqori tayyorlikni madadlash vositalari

Tijoriy ilovalarda apparat-dasturiy komplekslarning yuqori tayyorligi muhim omil hisoblanadi. MBBTga muvofiq yuqori tayyorlikni madadlovchi vositalar apparat, ayniqsa disklarga tegishli buzilishlarni neytrallashtirishni hamda xizmatchi xodim yoki tatbiqiy dastur xatoliklarini tiklashni ta'minlashi lozim. Bunday vositalar boshidayoq kompleks arxitekturasiga o'rnatilishi shart. Masalan, ortiqcha disk massivlarining u yoki bu turidan foydalanish kerak. Albatta, apparat-dasturiy

yechim qimmatlashadi, ammo ekspluatatsiya vaqtida bo'lishi mumkin bo'lgan zarardan asraydi.

Odatda klaster tarkibida uzellar-kompyuterlar tomonidan birgalikda ishlatiluvchi bir necha diskli qismtizim va komponentlar orasidagi ortiqcha bog'lanishlar bo'ladi.

Tashqi nuqtayi nazaridan klaster bir butun kabi ko'rinadi, bir necha uzellaming mavjudligi esa unumdorlikning va buzilishlarga barqarorlikning oshishiga sabab bo'ladi.

Ma'lumotlarni tirajlash

Axborot xavfsizligi nuqtayi nazaridan tirajlashga ma'lumotlaming foydalanuvchanligini oshirish vositasi sifatida qarash mumkin. INGRES MBBT tirajlashning rivojlangan imkoniyatini taqdim etadi. Informix OnLine-DS 7. Ida ma'lumotlami asosiy serverdan to'laligicha ikkilamchi serverga akslantirishdan iborat tirajlash modeli madadlanadi.

Tirajlashli Informix OnLine-DS serverlarining konfiguratsiyasida bitta asosiy va qator ikkilamchi serverlar ajratiladi. Asosiy serverda o'qish va ma'lumotlami yangilash amalga oshiriladi, barcha o'zgarishlar esa ikkilamchi serverlarga iizatiladi. Ikkilamchi serverlardan faqat o'qish mumkin. Asosiy server buzilganida, ikkilamchi server avtomatik ravishda yoki qo'lda o'qish va yozish rejimiga o'tkaziladi. Asosiy server buzilganida, mijozlami ochiq-oydin qayta yo'naltirish madadlanmaydi, ammo u ilovalar doirasida amalga oshirilishi mumkin.

Asosiy server tiklanganidan so'ng ushbu server ikkilamchi serverga aylanishi mumkin, endi o'qish-yozish rejimida ishlovchi avvalgi ikkilamchi serverga asosiy server maqomi beriladi va unga ulangan mijozlar ishlarini davom ettiradilar. Shu tariqa ma'lumotlardan uzluksiz foydalanish ta'minlanadi.

Tirajlash axborotni tranzaksiya jumalidan (mantiqiy jumaldan) asosiy serveming tirajlash buferiga uzatish yo'li bilan amalga oshiriladi. Undan axborot ikkilamchi serveming tirajlash buferiga o'tkaziladi. Bunday o'tkazish sinxron yoki asinxron rejimida sodir bo'lishi mumkin. Sinxron rejim ma'lumotlar bazasining to'liq muvofiqligini kafolatlaydi, ya'ni asosiy serverda qaydlangan birorta ham tranzaksiya, xatto asosiy server yanglishganida ham ikkilamchi serverda qaydlanmay qolmaydi. Asinxron rejim mutlaqo muvofiqlikni ta'minlamaydi, ammo tizimning ishchi xarakteristikalarini yaxshilaydi.

Tirajlashning qo'shimcha ijobiy samarasi - qaror qabul qilishni madadlovchi katta hajmli resursli ilovalami, asosan, ikkilamchi serverga o'tkazish imkoniyati. Bu holda ular parallel ishlash vositalaridan maksimal foydalanib, asosiy serverda to'plangan tranzaksiyalami operativ ishlovchi ilovalarga xalaqit qilmasdan, ishlanishi mumkin. Bunga ma'lumotlaming foydalanuvchanligini oshiruvchi omil sifatida ham qarash mumkin.

Server va mijozlar orasidagi kommunikatsiyalarni himoyalash

Server va mijozlar orasidagi kommunikatsiyalarni himoyalash muammosi nafaqat MBBTlarga, balki barcha taqsimlangan tizimlarga taalluqli. Tabiiyki, bu yerda, masalan, OSF konsemining taqsimlangan hisoblash muhitidagi kabi umumiy yechimlar qidiriladi. MBBT ishlab chiqaruvchilariga o‘zining dasturiy mahsulotlarini ushbu muhitga “yuklash” qoladi.

Informix-DCE/Net Informixning barcha instrumental vositalari hamda har qanday ilovalar yoki ODBC interfeysidan foydalanuvchi mustaqil ta‘minotchilardagi instrumental komplekslari uchun DCE serverlaridan foydalanishni tashkil etadi. Xavfsizlik serveri DCE muhitida mijoz-serveming o‘zaro aloqalarini amalga oshirishdagi muhim komponent hisoblanadi. Ushbu server taqdim etadigan asosiy fiinksiyalar — Kerberos vositalari amalga oshiruvchi autentifikatsiya, avtorizatsiya va shifrlash. Masalan, mijoz-serveming har bir ilovasi uchun ma‘mur himoyaning quyidagi beshta sathidan birini berishi mumkin:

- faqat mijozning server bilan ulanganligi aniqlanganidagina uzatiluvchi ma‘lumotlar himoyalaniadi;

- server ilk bor so‘rovni olganida, faqat muolajani masofadan chaqirishning boshlang‘ich bosqichida ma‘lumotlar himoyalaniadi;

- ma‘lumotlar manbaining haqiqiyiligini tasdiqlash. Serverga qabul qilinuvchi barcha ma‘lumotlaming ma‘lum mijozdan ekanligi tekshiriladi;

- ma‘lumotlar manbai, yaxlitligi va konfidensialligini tasdiqlash.

Oldingi sathda ko‘zda tutilgan tekshirishlar bajariladi va barcha jo‘natilgan ma‘lumotlar shifrlaniadi.

Informix-DCE/Net madadlagan autentifikatsiya servisi DCE taqsimlangan muhit xavfsizligi xarakteristikalarini yaxshilaydi, o‘sha vaqtda foydalanuvchilar va ma‘murlar faoliyati soddalashadi.

Ushbu muhitga joylashtirilgan har qanday ma‘lumotlar bazasiga murojaat etish uchun yagona kirish nomiga va DCE uchun parolga ega bo‘lish kifoya. Ilova ishga tushirilganda Informix-DCE/Net DCEdan foydalanuvchining autentifikatsiya axborotini so‘raydi va uni istalgan bazaga ulaydi.

Ma‘lumotlar bazasidan va ilovalardan foydalanishning kirish nomi va huquqini ma‘murlashning yagona nuqtasining mavjudligi xavfsizlikning umumiy vaziyatini tartibga solishga imkon beradi.

Ma‘lumotlar tuzilmalarini loyihalash

Ma‘lumotlar tuzilmalarini loyihalash deyilganda ularning xotirada taqdimlarini ishlab chiqish tushuniladi. Ma‘lumotlar tuzilmalarini loyihalashda hisobga olinishi zarur asosiy parametrlar quyidagilardir:

- ma‘lumotlar har bir elementlarning saqlanuvchi axboroti turi;
- ma‘lumotlar elementlarning va sarflangan tuzilmalarning aloqalari;
- tuzilma ma‘lumotlarining saqlanish vaqti (<<hayot vaqti>>);
- ma‘lumotlar elementlari, sarflangan tuzilmalar va' umuman tuzilma bilan operatsiyalar jamlanmasi.

Saqlanuvchi axborot turi

Saqlanuvchi axborot turi xotiraning tegishli tipini belgilaydi. Foydalanilayotgan dasturlarning tipiga bog‘liq ravishda ma‘lumotlar elementlari sifatida quyidagilar qaralishi mumkin:

- turli formatdagi butun va haqiqiy sonlar;
- timsollar (simvollar);
- Bull qiymatlari: true va false.

Shuningdek, ma‘lumotlarning ayrim tuzilmaviy tiplari, masalan:

- satrlar;
- yozuvlar;
- maxsus e‘lon qilingan sinflar.

Bu o‘rinda sonli maydonlar uchun mumkin bo‘lgan birliklar diapazonini, satrli ma‘lumotlar uchun esa satrning mumkin bo‘lgan maksimal uzunligini to‘g‘ri belgilash g‘oyat muhimdir.

Elementlar va ichma-ich qo‘yilgan tuzilmalar aloqalari, shuningdek ularning barqarorligi hamda elementlar va sarflangan tuzilmalar bilan operatsiyalar jamlanmasi ma‘lumotlar taqdimi uchun foydalaniluvchi xotira tuzilmalarini ham belgilaydi.

Ma‘lumotlarni statik yoki dinamik, shuningdek tashqi xotiraga joylashtirishda hayot vaqti hisobga olinadi. Ma‘lumotlar, ularning elementlari va ular o‘rtasidagi aloqalar ichki taqdimining mavjud variantlarini yanada batafsil ko‘rib chiqamiz.

Ma‘lumotlarning operativ xotiradagi taqdimi

Ma‘lumotlarni operativ xotirada tashkillashtirishning ikki tayanch tuzilmasi — vektorli va ro‘yxatli tuzilmalar farqlaniladi.

Vektorli tuzilma ma‘lumotlar maydonlarini joylashtirish uchun foydalaniladigan xotira baytlari bosqichlilikini o‘zida ifoda etadi. Ma‘lumotlarning tashkillashtirilgan tuzilmalarini bosqichlilikda joylashtirish elementlarga to‘g‘ridan-to‘g‘ri daxlni: massivlarda yoki satrlarda indeks (indekslar jamlanmasi) bo‘yicha yoki yozuvlarda yoxud obyektlarda maydon nomi bo‘yicha amalga oshirish imkonini beradi.

Biroq massivlar elementlarini joylashtirish uchun vektorli tuzilmalardan foydalanishda elementlarni qo‘shish yoki yo‘qotish operatsiyalarini bajarish elementlarning ko‘p oshirilishini talab qilish mumkin.

Ma‘lumotlar tuzilmalarini vektorli taqdimda ham statik, ham dinamik xotiraga joylashtirish mumkin. Vektorli taqdimlarning dinamik xotiradagi joylashuvi ba‘zan operativ xotiradan foydalanish samaradorligini jiddiy ravishda orttirishga imkon beradi. Dinamik xotirada oraliq natijalarni saqlovchi muvaqqat tuzilmalarni hamda o‘lchami kiritiluvchi boshlang‘ich ma‘lumotlarga kuchli bog‘liq tuzilmalarni joylashtirgan ma‘qul.

Ro‘yxatli tuzilmalar

Ro‘yxatli tuzilmalar axborot qism bilan birga yana bir yoki bir necha ko‘rsatkichlarni — elementlarning yoki shu elementlarga aloqador sarflangan tuzilmalarning manzillarini ham qamrab oluvchi maxsus elementlardan barpo

etiladi. Bunday elementlarni dinamik xotirada joylashtirgan holda turli ichki tuzilmalarni tashkillashtirish mumkin.

Biroq ro'yxatli tuzilmalardan foydalanishda quyidagilarni yodda tutish lozim:

- ko'rsatkichlarni saqlash uchun qo'shimcha xotira zarur;
- yo'nalishli ro'yxatlarda axborotni izlash bosqichma-bosqich amalga oshiriladi va shu boisdan ko'proq vaqt talab qiladi;
- ro'yxatlarni tuzish va ro'yxatlarda saqlanayotgan ma'lumotlar elementlari ustidan operatsiyalarni bajarish dasturchilarning yanada yuqori malakasini hamda ko'p ishlashni talab qiladi, tegishli dasturlar esa ko'proq xatolarga egaligi bois yanada batafsil testlashni talab etadi.

Vektorli ko'pliklar

Odatda vektorli taqdim statik ko'pliklarni, jadvallarni, masalan satrlar, yozuvlar matritsalarini, shuningdek o'rindoshlik matritsasi, insidentlik matritsasi yoki tahliliy taqdim etilgan graflarni saqlash uchun qo'llaniladi.

Ro'yxatli taqdim dinamik (o'zgaruvchan) tuzilmalarni va murakkab aloqali tuzilmalarni saqlash uchun qulay.

Eng mas'uliyatli holatlarda ichki taqdimni tanlashda ma'lumotlar tuzilmasi yoki turli variantlar uchun uning elementlari bilan eng ko'p uchraydigan operatsiyalarni bajarishning hisoblash murakkabligini belgilash maqsadga muvofiq. Shuningdek, ularning sig'imi murakkabligini ham baholash kerak.

Tashqi xotirada ma'lumotlar taqdimi

Zamonaviy operatsion tizimlar tashqi xotirada ma'lumotlarni tashkillashtirishning ikki usulini: bosqichli va bevosita daxlli usullarini quvvatlaydi.

Ma'lumotlarga bosqichli daxlda faqat ma'lumotlar elementlarini bosqichli o'qish yoki ularning bosqichli yozuvi mumkin.

Bunday variant klaviatura yoki displey tipidagi mantiqiy qurilmalar bilan ishlashda, yozuvlar formati ish jarayonida o'zgaradigan fayllarga yoki matnli fayllarga ishlov berish nazarda tutiladi.

Bevosita daxl faqat qaydlangan uzunlikdagi yozuvlar bilan axborot almashinuvi amalga oshiriluvchi diskli fayllar uchun mumkin. Bunday faylning yozuvi manzilini uning raqami bocyicha aniqlash mumkin, bu esa kerakli yozuvga bevosita murojaat qilishga imkon beradi.

Ma'lumotlar tuzilmalarini joylashtirish uchun xotira tipini tanlashda quyidagilarni nazarda tutish lozim:

- operativ xotiraga ham o'qish, ham o'zgartirish uchun tezkor ruxsatli kirish zarur ma'lumotlar joylashtiriladi;
- tashqi xotiraga dastur tugallanganidan so'ng saqlanishi shart ma'lumotlar joylashtiriladi.

Ma'lumotlar dekompozitsiyasiga asoslangan dasturiy ta'minlashni loyihalash

Dasturiy ta'minotni loyihalashning ma'lumotlar dekompozitsiyasiga asoslangan Jekson hamda Varnye—Orr metodikalari amalda bir vaqtning o'zida takjif etilganligi eslatib o'tilgan edi.

Har ikki metodika murakkab; lekin iyerarxik tashkillashtirilgan ma'lumotlar tuzilmalari bilan ishlovchi «sodda» dasturlarni ishlab chiqish uchun mo'ljallangan. Dasturiy tizimlarni ishlab chiqish zarur bo'lganda har ikki holatda ham avval tizimni dasturlarga bo'laklash, so'ngra metodika ma'lumotlaridan foydalanish nazarda tutiladi.

Jekson metodikasi

O'z metodikasini yaratishda M. Jekson boshlang'ich ma'lumotlar va natijalar tuzilmalari dastur tuzilmasini belgilashidan kelib chiqqan.

Metodika boshlang'ich ma'lumotlar va natijalar tuzilmalarining muvofiqliklarini izlashga asoslangan. Biroq uning qo'llanishida qandaydir darajada muvofiqliklar mavjud bo'lmagan vaziyatlar yuzaga kelishi mumkin. Masalan, boshlang'ich fayl yozuvlari tegishli satrlar hisobotda namoyon bo'lishi shart tartibda tartiblanmagan. Bunday vaziyatlar «to'qnashuvlar» deb nomlangan edi. Turlicha hal qilinadigan to'qnashuvlarning bir necha tiplari ajratiladi. Yozuvlarning turlicha bosqichliligida ularni ishlov berishga qadar shunchaki tartiblanadi. To'qnashuvlarni hal etish usullarida yanada batafsil bayon etilgan.

Dastur tuzilmasini metodikaga muvofiq ishlab chiqish quyidagicha yo'sinda bajariladi:

- kirish va chiqish ma'lumotlari tuzilmalarining tasviri barpo qilinadi;
- ushbu ma'lumotlar o'rtasidagi ishlov aloqalari (muvofliqliklar) identifikatsiyasi bajariladi;
- ma'lumotlar tuzilmalari va aniqlangan muvofiqliklar asosida dastur tuzilmasi shakllantiriladi;
- muvofiqliklar aniqlanilmagan elementlar ishlovi bloklari qo'shimcha qilinadi;
- nomuvofiqliklar tahlil qilinadi va ishlovdan o'tkaziladi, ya'ni «to'qnashuvlar» hal etiladi;
- zaruriy operatsiyalar (fayllarni kiritish, chiqarish, ochish/ yopish va hokazo) qo'shimcha qilinadi;
- dasturni tuzilmaviy notatsiyada yozib qo'yiladi.

Tahlil va loyihalashning tuzilmaviy metodologiyalari

Tahlil va loyihalashning tuzilmaviy metodologiyalariga asoslangan CASE texnologiyalar. Hozirgi vaqtda tegishli CASE vositalarda tuzilmaviy tahlil va loyihalashning aksariyat mashhur metodologiyalaridan muvafaqqiyatli foydalanish tajribasi to'plangan. SADT, Geyn— Sarson tuzilmaviy tizimiy tahlil, Yordan—De Marko tuzilmaviy tahlil va loyihalash, Jekson tizim rivoji, Varnye-Orr DSSD (Data Structured System Development) tuzilmaviy sxemalar rivoji, Uord—Mellor

va Xartli real vaqt tizimlari tahlili hamda loyihalanishi, Martin axborot modellashtirish metodikalari eng ko‘p joriy etilgan.

Keltirilgan statistik ma’lumotlardan ayonki, ma’lumotlar oqimlari diagrammalaridan foydalanuvchi tuzilmaviy metodikalar eng ko‘p qo‘llanilmoqda. Buning ikkita sababi bor:

- ma’lumotlar oqimlari diagrammalari funksional diagrammalarga qiyosan hozirgi paytda ko‘p sonli axborot tizimlar spetsifikasini yanada batafsil aks ettiradi: ishlanayotgan axborotning qat’iy tiplashtirilishini talab qilmaydi, ma’lumotlar saqlanishi imkoniyatini nazarda tutadi, tashqi dunyo bilan o‘zaro harakatlanishni muayyanlashtiradi, dasturiy ta’minlash kompleks modeli olinishini nazarda tutadi.
- ma’lumotlar oqimlari diagrammalari bo'yicha loyiha spetsifikatsiyalari (Jekson yoki Konstantayn tuzilmaviy xaritalari) barpo etilishining usuli ishlab chiqilgan, bu esa avtomatik ravishda shunday spetsifikatsiyalarni yaratish imkonini beradi.

Foydalanilgan adabiyotlar

1. Ramez Elmasri, Shamkant B.Navathe. Fundamentals of Database Systems (7th Edition). Pearson. USA, 2015.
2. M.T.Azimjanova, Muradova, M.Pazilova. Informatika va axborot texnologiyalari. O'quv qo'llanma. T.: "O'zbekiston faylasuflari milliy jamiyati", 2013 y.
3. Holmatov T.X., N.I.Tayloqov. Amaliy matematika, dasturlash va kompyuteming dasturiy ta'minoti. O'quv qo'llanma. T.: "Mehnat", 2000 y.
4. S.S.Qosimov Axborot texnologiyalar O'quv qo'llanma. T.: "Aloqachi", 2006 y.
5. M Aripov, B.Begalov va boshqalar. Axborot texnologiyalari. O'quv qo'llanma. T.: "Noshir", 2009 y.
6. A.Sattorov. Ma'lumotlar bazasini boshqarish sistemasi Access (Windows 9x/2006) O'quv qo'llanma. T.: "Fan va texnologiya", 2006 y.
7. Axborot xavfsizligi asoslari, I.M.Karimov Tashkent, 2019
8. Информационная безопасность телекоммуникационных систем (технические аспекты), Кулаков М.В., Гарашин А.В. Учеб. Пособие для вузов. М.: Радио и связь, 2014
9. Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие. М.: 2017.
10. Зегжда Д.П. Основы безопасности информационных систем: Учеб. пособие для студ. вузов. – М.: Горячая линия – Телеком, 2016.