13. Andmekaitse ja kasutajate autoriseerimine

13.1. Ressursid ja nende "piirid"

maailm jaguneb ressurssideks ja alam-ressurssideks

Kõik maailmas olevad väärtused ja “väärtusetused” võime me jagada erinevat tüüpi ja erineva komplektsusega ressurssideks ning alamressurssideks. Eramasti on igal ressursil (ja ka alamressursil) olemas omanik või vähemalt valdaja või haldaja. Vahel aga mõlemad korraga. Kui selleks ei ole mingi isik (olgu siis füüsiline või juriidiline), siis on selleks tavaliselt mingi riik. On olemas ka ressursse, mis otseselt ei kuulu kellelegi. Siiski on tänapäeval tavaliselt ka igal sellise ressursiga seotud kas mõni riiklik või rahvusvaheline organisatsioon, mis tegeleb (või vähemasti üritab tegeleda) selle ressursi kasutamise reglementeerimisega.

NÄIDE

Nii on näiteks maa kas eraisiku, füüsilise isiku, munitsipaal või riigi oma. Samas võib sellel maal olla omanikust erinev kasutaja – omab üks aga kasutab teine. Selline situatsioon saab aga eksisteerida ainult omaniku loal. Siit näitest nähtub, et on olemas ressurss “maa”, mis on jagatud alamressurssideks, millest igal on omanik. See tähendab, et peavad eksisteerima piirid, mis eraldavad “suure ressursi” alamressurssideks. Need piirid peavad olema kusagil fikseeritud ja mingi institutsioon peab tagama nende piiride registreerimise ja ka piiridest kinni pidamise. Maa omand (piirid) on registreeritud riiklikus maakatastris.

intellektuaalne ressurss

Huvitavaim ressurss on intellektuaalne ressurss. Siin on alamressursi piiride määramine palju keerulisem. Lihtsam on see laulude, raamatute, filmide, arvutiprogrammide jne. korral. Raskem on piire määratleda teaduslike meetodite, teooriate jms. korral. Ometi põhineb ka siin kogu omanduse süsteem piiride määramisel, nende piiride registreerimisel ja registreeritud piiridest kinni pidamise tagamise süsteemist (patendid, kaubamärgid, tööstusnäidised, autori õiguse kaitse seadused, autori õiguste kaitse ühingud jne.).

3.1.1. Õigus (privileeg) kasutada

õigus kasutada on suurim õigus

Suurim ja ainus privileeg ressursi korral on selle ressursi kasutamise õigus. Ressursi kasutamise õigus on alati selle ressursi omanikul. Lisaks sellel võib

ressursi omanik delegeerida enda omandi kasutamise õigusi teistele isikutele. Koos õiguste delegeerimisega ressursi kasutamiseks määratakse ka kindlaks ressursi kasutamise piirid, mille ulatuses õigused saanu võib ressurssi kasutada.

Peaaegu kunagi ei anna omanik oma ressursi kasutamise kõiki õigusi üle teisele isikule. Kõige sagedamini jäetakse edasi andmata õigus omandi võõrandmaiseks s.o. omaniku muutmiseks ja omandi õiguste edasi volitamiseks. Kui aga antakse edasi ressursi võõrandamise õigus või omandi õiguste edasi volitamiseks, siis tavaliselt ei kaasne sellega muid kasutamise õigusi.

kunagi ei anna omanik üle kõiki õigusi

Õigused ressursi kasutamiseks saadakse tihti mingi hüvituse vastu. Hüvituseks võib olla ka õiguste andmine mingi teise ressursi kasutamiseks.

õigusi tavaliselt müüakse ja ostetakse

Teatud tingimustes võidakse ressursi omaniku õigusi piirata, muuta või lõpetada tema enda tahte vastaselt. Selleks on kaks võimalust – seaduslik ja ebaseaduslik. Esimesel juhul peab õiguste muutuse teostaja omama ressursi omaniku suhtes mingit “üleolekut” – tavaliselt juriidilist. Teisel juhul on tavaliselt argumendiks “jõud”.

ka omaniku õigusi võib/saab piirata

13.1.2. Õigustatud (volitatud) kasutamine

Ressursi volitatud kasutajaks loetakse ressursi selliste kasutajat, kellele on ressursi omanik (või omaniku poolt selleks volitatud isik) andnud õiguse ressursi kasutamiseks.

volitatud kasutamine on kasutamine omaniku loal

Ressursi volitatud kasutaja on ka ressursi omanik.

Ressursi volitatud kasutamiseks loetakse ressursi kasutamist volitatud kasutaja poolt temale antud õiguste piires. Ressursi omanikul on ressursi kasutamiseks kõik õigused. Ka ressursi omaniku õigusi ressursi kasutamiseks võidakse piirata (näiteks seadusega - looduskaitsealad, Tallinna vanalinn, rannaalad jne.)

ületada ei tohi õiguste piire

Näiteks võib metsa omanik anda mingile teisele subjektile (metsaraie firmale) õiguse teostada raiet oma metsas. Metsaraie firma maksab omanikule selle õiguse eest (ostab ära “raiutava” metsamaterjali). Vaatamata sellele, et metsaraie firmal on õigus raiuda metsa teatava mahu ja muude tingimustega (N: raietihedus, puu liigid jms.) ei ole tal õigus müüa seda õigust edasi (kui

NÄIDE

lepingus pole teisiti sätestatud). Kindlasti pole tal aga õigus muuta lepingu tingimusi ega müüa seda maad, millel tal on õigus raiet teostada.

13.1.3. Õiguseta (volitamata) kasutamine

volitamata kasutamine on kasutamine ilma omaniku loata
volitamata kasutamine on ka see, kui volitatud kasutaja ületab volituse piire

Ressursi volitamata kasutajaks nimetatakse ressursi sellist kasutajat, kes kasutab ressurssi ilma, et tal oleks selle ressursi kasutamiseks mingeid õigusi. Ressursi omanik ei ole talle selliseid õigus andnud.

Ressursi volitamata kasutamiseks nimetatakse ressursi kasutamist kas volitamata kasutaja poolt (kellel ressursi omanik pole mingeid õigusi selle ressursi kasutamiseks andnud) või ressursi kasutamist küll volitatud kasutaja poolt (kellele on ressursi kasutaja mingid õigused ressursi kasutamiseks andnud), kuid sellistes piirides, mis ei ole määratud temale antud õigustega (ületab endale antud õigusi).

13.1.4. Õiguste tagamine

õigusi ei järgita ilma sunni mehhanismita

Üks kõik kui täpselt on määratletud ressursside piirid, ressursside omanikud, ressursside kasutamise õigused ja nende õiguste edasi andmise õigused, ei toimi see süsteem ilma sellest struktuurist kinnipidamise tagamise süsteemita. Igapäevases elus on selleks erinevad seadised, omandi registrid ja protseduurid ressursside piiride ning omanduse muutmiseks (maamõõtjad, maaregistrid, kaubamärgiregistrid, patendiregistrid, patendivolinikud, advokaadid, notarid jne.)

13.2. Andmete kasutamine ja kasutajaõiguste andmine

andmed on ressurss

Ka andmed on ressurss, mis millegi poolest ei erine teistest ressurssidest – neil on piirid, maht ja omanik. Tavaliselt on andmete omanikuks nende säilitusstruktuuride looja ja koguja. Tihti on siiski ka nii, et andmete omanikuks on andmetestruktuuride loomise ja andmete kogumise algataja. Sisuliselt on tegemist haldamisteenuse sisse ostmisega – andmete omanik on üks aga nende haldamisega tegeleb keegi teine.

andmetel on omanik

Andmebaaside korral võib eristada veel juriidilist omanikku ja tehnoloogilist omanikku. Andmete juriidiliseks omanikuks on tavaliselt andmestruktuuride loomist ja andmete kogumist ning töötlemist finantseeriv isik (juriidiline või füüsiline). Andmete tehnoloogiliseks omanikuks on andmebaasi kasutajad – need kasutajad kes loovad ja haldavad neid andmeid.

juriidiline omanik on tegelik omanik

Andmete kasutamise õiguste jagamise tingimused määrab andmete juriidiline (tegelik) omanik. Andmete kasutamise faktilisi õigusi jagavad üks või mitu selleks volitatud tehnoloogilist omanikku – süsteemi administraator(id) ja andmebaasi administraator(id). Mõnedes andmebaasisüsteemis ka ainult süsteemi administraator(id). Seda peamiselt väikestes süsteemides, kus süsteemiadministraator ja andmebaasiadministraator on tavaliselt sama isik. Kõigil peakasutajatel on õigus anda õigusi teistele kasutajatele. Kaasaarvatud on neil õigus “luua” teisi enda sarnaseid õiguste jagajaid – anda mõnedele kasutajatele andmebaasiadministraatori õigused.

andmebaasis talletatud erinevad protseduurid on samuti ressurss

Andmed ei ole andmebaasis olev ainuke ressurss. Ka andmebaasis talletatud andmete töötlusprotseduurid on ressurss ja mitte vähe tähtis ressurss

Kõik andmete kasutamise õigused võib olenemata kasutajast või tema õigustest jagada kolmeks grupiks. Järgnevalt vaatamegi neid kolme õiguste gruppi.

13.2.1. Õigus andmetele juurdepääsuks

andmetele ligi pääsu õigus

Esmane andmete kasutamise õigus on õigus andmetele juurdepääsuks. See õigus ei määra veel, millistes piirides on õigus andmeid kasutada – määratakse ainult, et on “õigus andmete juurde minna”, mitte neid aga vaadata või muuta.

Reaalses maailmas sarnaneb see juhtumiga, kus te saate küll õiguse minna raamatukokku, kuid peate seal hoidma silmad kinni, seisma liigutamata ja midagi, isegi põrandat, puudutamata.

ilma selleta pole teisel õigustel mõtet

Esmaselt vaadatuna tundub see õigus mitte midagi tähendavat, kuid tegelikkuses on see esimene õigus, mis peab andmete kasutamiseks olemas olema – meil võivad olla kõik õigused andmete kasutamiseks muutmiseks jms.,

kuid kui puudub õigus andmetele juurdepääsuks, siis on ka kõik teised õigused kasutud.

Õigus andmetele juurdepääsuks tähendab seda, et isik on registreeritud andmebaasi kasutajaks (talle on omistatud kasutaja nimi ja esmane võtmesõna), kuid talle ei ole antud mingeid muid õigusi. Tegevused, mida kasutaja, kes omab selliseid õigusi, andmebaasiga teha saab on andmebaasi sisse logimine (seansi alustamine) ja sealt välja-logimine (seansi lõpetamine).

Tegelikult on küll igal kasutajal koos andmetele juurdepääsu õigustega vaikimisi olemas ka õigused kirjutada, muuta ja kustutada andmeid enda loodud andmestruktuurides, kuid kuna puuduvad õigused andmestruktuuride loomiseks, siis ei ole võimalik neid õigusi realiseerida.

enda loodud ressursside kasutamise õiguste jagamise õigus

Alati on olemas enda loodud andmebaasistruktuuridele (tabelite, vaadete jms.) teiste kasutajate jaoks õiguste määramise ja muutmise õigus. Kuid neidki ei saa realiseerida, kui struktuuride loomise õigus puudub.

13.2.2. Õigused tegutsemiseks - süsteemsed õigused

süsteemsed õigused

Süsteemsed õigused määravad kasutaja õigused teha erinevaid toiminguid:

- luua uusi kasutajaid ja hävitada olemasolevaid kasutajaid
- anda kasutajatele süsteemseid õigusi ja võtta neilt ära olemasolevaid süsteemseid õigusi
- luua erinevaid andmebaasistruktuure (tabeleid, seoseid tabelite vahel, indekseid, protseduure, trigereid, pakette jms), muuta ja hävitada neid
- muuta erinevate ressursside (tabelite, protseduuride, vaadete jms.) kasutamise õigusi; anda nende kasutamise õigusi kasutajatele ja võtta neilt olemasolevaid õigusi; muuta nende kasutusõiguste "võimsust"
- muuta andmebaaside erinevaid haldusstruktuure (ketta piirkondade eraldamine, operatiivmälu jaotuse muutmine jms.)

Igal andmebaasisüsteemil on süsteemsete õiguste loend erinev

Kõik need tegevused jagunevad loomulikult veel alamtegevusteks, millede kohta on võimalik eraldi õigusi anda või neid ära võtta. Erinevates andmebaasisüsteemides on need õiguste grupid küll kõik olemas, kuid iga

andmebaasisüsteem detailiseerib ja ka käsitleb neid teistes andmebaasisüsteemidest veidi erinevalt.

ühele kasutajale ei anta kunagi kõiki õigusi

Tavaliselt ei anta kunagi kõiki õigusi ühele kasutajale. Seda kas või juba selle pärast, et kunagi ei ole ühe kasutaja kompetents nii suur, et ta kõiki õigusi oskaks sihipäraselt kasutada. Siiski on tähtsamaks põhjuseks see, et igal kasutajal on oma ametialastest kohustustest sõltuvad kohustused, mis tingivad ka nendele andmebaasi kasutamiseks antavad õigused.

Suurema osa andmebaasi kasutajatest ei ole mingeid süsteemseid õigusi. Nende kõik õigused piirduvad ressursi kasutamise õigustega.

13.2.3. Õigused ressursside kasutamiseks

kasutaja seisukohalt jagunevad tema poolt kasutatavad ressursid tema enda poolt loodud ressurssideks ja teiste kasutajate poolt loodud ressursside saadud õiguste alusel kasutatavateks ressurssideks

Lisaks kasutaja enda loodud andmebaasistruktuuridele, mille igakülgseks muutmiseks on kasutajal õigused olemas, on andmebaasis hulgaliselt teiste kasutajate poolt loodud ressursse (tabeleid ja erinevat kiiki protseduure), mida ei ole vaja kasutada mitte ainult nende struktuuride loojal vaid paljudel teistel kasutajatel. Samuti on teistel kasutajatel suure tõenäosusega vaja kasutada kasutaja enda poolt loodud struktuure. Enamik andmebaasikasutajaid ei omagi mingeid õigust luua andmebaasi uusi struktuure – kogu nende töö põhinebki teiste poolt loodud andmestruktuurides olevate andmete käsitlemisel ja teiste loodud protseduuride käivitamisel. Kuna vaikimisi kasutamise õigused on igal kasutajal ainult enda poolt loodud ressurssidele, siis peab igal kasutajal olema õigus enda loodud ressursside kasutamise õiguste teistele kasutajatele “välja jagamiseks”. Selleks peab andmebaasisüsteemil olemas olema õiguste aparatuur – milliseid õigusi ja millises ulatuses enda loodud ressurssidele teistele kasutajatele välja jagada saab.

andmete kasutamise õigusteks on INSERT-, UPDATE-, DELETE- ja SELECT õigusteks

Andmestruktuuride korral on välja jagatavateks õigusteks andmete lisamise (INSERT), uuendamise (UPDATE), kustutamise (DELETE) ja vaatamise (SELECT) õigused. Erinevate protseduuride korral on välja jagatavaks õiguseks õigus käivitada protseduuri. Lisaks sellele saab piirata kasutaja õigusi andmebaasi tabeli veergude kasutamiseks. INSERT-, UPDATE- ja SELECT õigusi saab kirjeldada andmebaasi tabeli iga veeru jaoks.

Iga kasutaja “tegutsemisruum” andmebaasis on kirjeldatav tema enda poolt loodud ressurssidega ja teiste kasutajate poolt tema ja temale antud ressursside kasutamise õigustega.

13.3. Õiguste jagamine ja SQL-keel (andmebaasisüsteemi ORACLE näitel)

13.3.1. Kasutajate haldamine

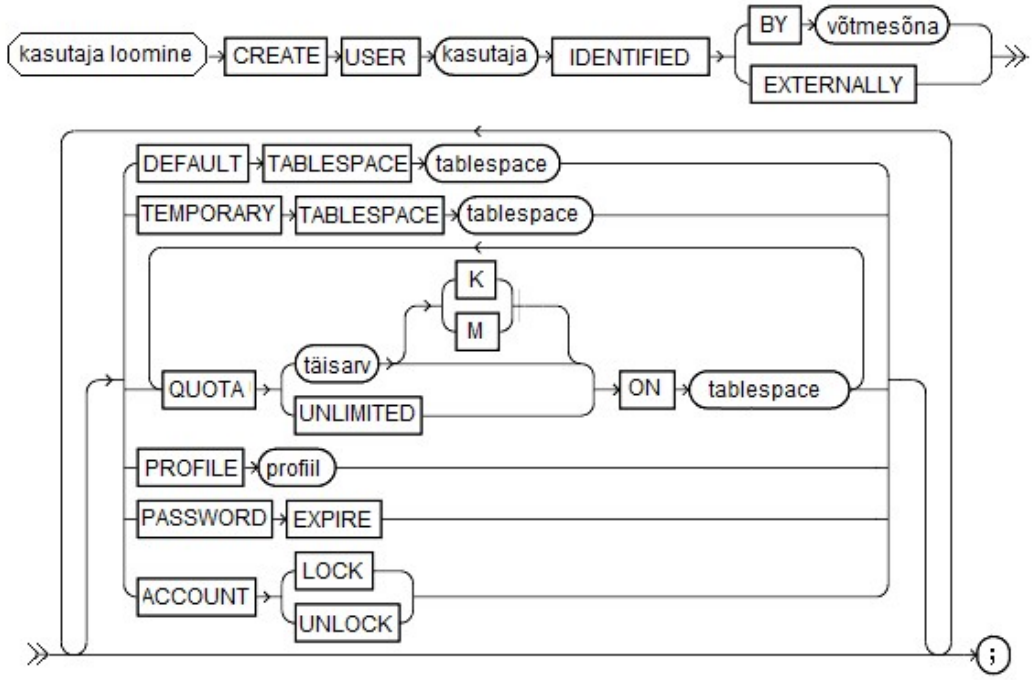
õigusi saab anda ainult kasutajatele

Andmebaasi kasutamise õigusi saab anda ainult andmebaasi kasutajale. Seega on mingile isikule andmebaasi kasutajaõiguste andmise esimeseks sammuks tema jaoks uue kasutaja loomine andmebaasis. Seda tehakse olenemata andmebaasijuhtumise süsteemist

loomisel saab kasutaja baasõigused

Koos kasutaja loomisega antakse kasutajale tavaliselt kohe ka mõned baasõigused, mida tulevikus antavate õigustega laiendatakse või õiguste piiramisega kitsendatakse.

Oracle SQL-keeles on andmebaasi kasutaja loomise lause CREATE USER:



kasutajanimi on unikaalne

kasutaja ::= loodava kasutaja nimi, mis peab olema unikaalne terves andmebaasimootoris (üle kõigi selle andmebaasimootori hallatavate

andmebaaside), on 1-30 sümbolit pikk ja vastav andmebaasisüsteemi ORACLE nime moodustamise standardile.

võtmesõna ::= loodava kasutaja salasõna *(password)*, mis on 1-30 sümbolit pikk sõna.

Kõige lihtsam kasutaja loomise korralduse kuju on:

NÄIDE

CREATE USER MART IDENTIFIED BY Kolla12; (luua kasutaja "MART", kelle salasõna on "Kolla12")

Andmebaasisüsteemi ORACLE andmebaasid on sisemiselt jagatud üksteisest loogiliselt eraldatud kettapiirkondadest, mida kutsutakse *tablespace*'deks. Igal sellisel piirkonnal on nimi. Kasutajale saab kirjeldada õigusi nende kettapiirkondade kasutamiseks.

ORACLE andmebaas on jagatud osadeks - *tablespace*'deks

Fraas EXTERNALLY määrab, et kasutaja õigusi kontrollitakse lokaalse töökoha operatsioonisüsteemi õiguste süsteemist *(single sign on)* ja kui kasutaja on loginud sisse lokaalsesse töökohta, siis andmebaasi eraldi logida pole vaja vaid kasutaja tuvastamine viiakse läbi vastu tööjaama õiguste süsteemi.

EXTERNALLY

Fraas, DEFAULT TABLESPACE, määrab andmebaasi *tablespace*, kuhu tehakse vaikimisi kasutaja poolt loodud andmestruktuurid, kui kasutajal on andmestruktuuride loomise õigus. Seda loomulikult ainult sellisel juhul, kui kasutaja ei ütle andmestruktuuri loomisel, millise nimega kettapiirkonda ta loodavat struktuuri tahab teha. Kui DEFAULT TABLESPACE on kasutajale määramata, siis tehakse kasutaja poolt loodavad andmestruktuurid vaikimisi *tablespace*-sse SYSTEM. See on süsteemne ketta piirkond.

DEFAULT TABLESPACE

Fraas, TEMPORARY TABLESPACE, määrab kasutajale selle andmebaasi *tablespace*, kuhu tehakse kasutaja poolt loodud ajutised andmestruktuurid. Kui see on määramata, siis tehakse need jällegi süsteemsesse *tablespace*-sse SYSTEM.

TEMPORARY TABLE SPACE

Fraas, QUOTA, piirab (M –megabaitides, K-kilobaitides), kui palju mingis konkreetses *tablespace*-s antud kasutajale “ruumi” eraldatakse.

QUOTA

Fraas, PROFILE, kirjeldab õiguste komplekti , profiili, mis omistatakse loodavale kasutajale. Profiil on “eelkirjeldatud” piirangute komplekt, mis on

PROFILE

salvestatud andmebaasi mingi nime all. Antud fraas määrab loodavale kasutajale kõik antud komplektiga määratud piirangud.

PASSWORD EXPIRE

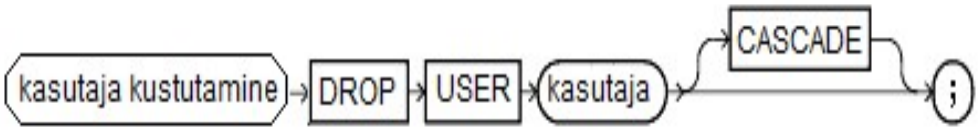
Fraas, PASSWORD EXPIRE, määrab selle, et kasutaja peab esimesel logimisel muutma oma salasõna *(password).*

ACCOUNT

Fraas, ACCOUNT, määrab selle, kas loodud kasutaja on aktiivne (UNLOCK) või lukustatud (LOCK). Kui kasutaja luukse lukustatuna, siis ei saa seda kasutaja nime enne kasutada kui see on lahti lukustatud. Seda kasutatakse selleks, et luua kasutaja koos kõigi õigustega varem ära ja teha aktiivseks alles siis, kui kasutajale reaalselt õigusi andmebaasi kasutamiseks soovitakse anda.

kasutaja kustutamine

Kasutaja saab baasist kustutada DROP USER lausega:



CASCADE

Kui lausele lisada fraas CASCADE, kustutatakse enne kasutaja kustutamist baasist ära ka kõik tema poolt loodud andmestruktuurid (tema skeem).

Kasutaja kustutamiseks baasist, jättes baasis alles kõik tema loodud andmestruktuurid, tuleb andmebaasisüsteemis ORACLE kirjutada SQL-korraldus:

NÄIDE

DROP USER MART:

andmebaasisüsteemil on alati süsteemiadministraator

Igas andmebaasis on alati vähemalt üks selline kasutaja, kelle nimi on määratud. See kasutaja on süsteemiadministraator. Selle kasutaja nime ei saa muuta ega seda kasutajat ei saa kustutada. Erinevates andmebaasisüsteemides on tema nimi erinev. Näiteks Centura SQLBases on süsteemiadministraatori nimi “SYSADM”, SyBase-s ja SQLServer-is “sa” ja ORACLE’s “SYSTEM”.

Süsteemiadministraator on eriline kasutaja – temal on kõik õigused kõikidele andmebaasis olevatele struktuuridele – olenemata sellest, kes need loonud on või kelle omad need parasjagu on! Tema võib kasutada andmebaasi kõiki struktuure, muuta iga kasutaja privileege ja ka neile kuuluvate andmestruktuuride omandust.

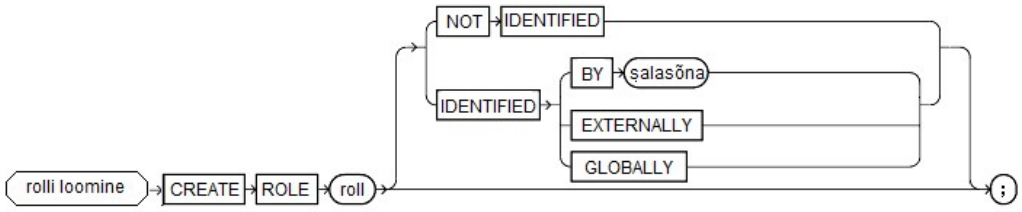
13.3.2. Kasutajagruppide (rollide) haldamine

roll / kasutajagrupp - eeldefineeritud õiguste kogum, millel on nimi

Väga tülikas on spetsifitseerida õigusi igale kasutajale eraldi. Lisaks sellele on see veel ka mõttetu – kasutajad on nii või teisiti päris suurte gruppide kaupa samade õigustega. Seepärast on enamikes andmebaasisüsteemides kas mõiste “kasutajagrupp” või “roll”. Need mõisted on täiesti identsed ja lihtsalt erinevates baasides kasutatakse erinevat mõistet. Roll on kogum õigusi, mis on andmebaasi salvestatud mingi nime all. Kasutajale rolliga kirjeldatud õiguste andmiseks tulen kirjeldada seos kasutaja ja rolli vahel. Anda kasutajale see roll.

CREATE ROLE

Oracle kasutab mõistet “roll”. Rolli loomiseks baasi on käsk CREATE ROLE:



rollil on unikaalne nimi

Rolli nimi on unikaalne ja sisaldab 1-30 sümbolit ja vastab andmebaasisüsteemi ORACLE nime moodustamise standardile.

NOT IDENTIFIED vs. IDENTIFIED

Kui lisatud on fraas NO IDENTIFIED, siis saavad kõik kasutajad, kellega on antud rolli õigused seotud, õigusi kasutada, ilma spetsiaalset salasõna teadmata. Kui on lisatud IDENTIFIED BY fraas, siis antud rolli õiguste kasutusele võtmiseks peab kasutaja teadma rolli nime ja selle rolli salasõna.

GLOBALLY

Fraas GLOBALLY määrab selle, et kasutaja õigust rolli õiguste kasutamiseks kontrollitakse globaalsest õiguste *directory* serverist LDAP, Open Directory vms.)

rollile antakse õigusi samade korraldustega, millega antakse õigusi kasutajatele

Kui roll on loodud. saab rollile anda õigusi samade korraldustega, millistega saab õigusi anda ka kasutajatele. Rollile õiguste andmisel tuleb ainult õiguste andmise korralduses kirjutada kasutajanime asemele rolli nimi.

DROP ROLE

Rolli saab baasist ka kustutada. Selleks kasutatakse käsku DROP ROLE:

Kui roll baasist kustutada kaotavad kõik antud rolliga seotud kasutajad selle rolliga seotud õigused.

kui roll kustutada kaotavad rolliga seotud kasutajad rolliga määratud õigused

Igas andmebaasisüsteemis on teatav hulk eeldefineeritud rolle. Sellisteks rollideks on näiteks süsteemiadministraator ja andmebaasiadministraator. Erinevatel andmebaasisüsteemidel on need rollid erinevad. Siiski on nendeks (olenemata rollide konkreetsetest nimedest erinevates baasides) tavaliselt *"database administrator"* (süsteemi administraator), "user" (lihtkasutaja) ja *"recovery manager"* (andmebaasi kindluskoopiate ja taaste korraldaja)

eelkirjeldatud rollid

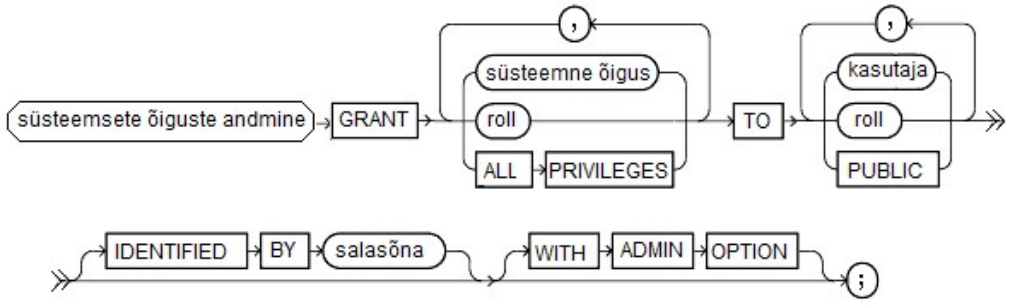
13.3.3. Süsteemsed õigused

Süsteemseteks õigusteks nimetatakse õigusi teostada baasis mingeid toiminguid. Süsteemseid õigusi saab anda kas kasutajale või rollile. Rollile antud õigused saab hiljem volitada komplektina kasutajatele või teistele rollidele. Seda nimetatakse õiguste jagamiseks kaskaadina (CASCADE).

süsteemseid õigusi saab anda kas kasutajale, rollile või kõigile

Andmebaasisüsteemi ORACLE SQL-keeles on süsteemsete õiguste andmise käsu süntaks järgmine:

GRANT-lause süntaks



Esimene grupp kirjeldab, millised privileegid antakse – kas loend (üle koma) süsteemseid privileege ("süsteemne õigus") , rolliga määratud privileege ("roll") või kõik olemasolevad privileegid ("ALL PRIVILEGES"). Viimasel puhul pole loendil mõtet, kuna ühe fraasiga antakse kõik süsteemsed õigused. Teine

grupp määrab loendi rollidest ja kasutajatest ("kasutaja", "roll"), kellele need privileegid antakse või võtmesõna PUBLIC, mis tähendab, et määratud õigused antakse kõigile kasutajatele – nii nendele kes on juba olemas, kui ka nendele kes luuakse tulevikus. Tulevikus loodavatele kasutajale antakse PUBLIC-fraasiga süsteemis kirjeldatud õigused koheselt, vaikimisi.

õigused läbi salasõna

Kui määratud on (IDENTIFYED BY) salasõna, siis saavad neid õigusi kasutada ainult need kasutajad, kes teavad salasõna.

edasi antavad õigused

Kui lisatud on fraas WITH ADMIN OPTION, siis antaks määratud kasutajatele õigus ka administraatorina neid samu õigusi, mis talle endale anti, teistele kasutajatele edasi anda.

NÄIDE

Andmebaasisüsteemis ORACLE on sagedamini antavateks süsteemseteks õigusteks:

CREATE SESSION	õigus logida andmebaasi sisse
EXECUTE ANY PROCEDURE	õigus käivitada kõiki protseduure olenemata nende omanikust
CREATE PROCEDURE	õigus luua uusi andmebaasiprotseduure , muuta ja kustutada enda loodud protseduure
CREATE TABLE	luua andmebaasi uusi tabeleid aj muuta ning kustutada oma loodud andmestruktuure
CREATE VIEW	luua andmebaasi uusi vaateid, ning muuta ning kustutada enda loodud vaateid

See on ainult kaduv väike osa andmebaasisüsteemis ORACLE kirjeldatud süsteemsetest õigustest aga meie eesmärgiks ei ole kirjeldada andmebaasisüsteemi ORACLE vai ainult kasutada teda kasutajaõiguste süsteemi kirjeldamiseks.

Näiteks loome rolli “student” ja anname sellele tudengi jaoks andmebaaside praktikumis vajalikud süsteemsed õigused:

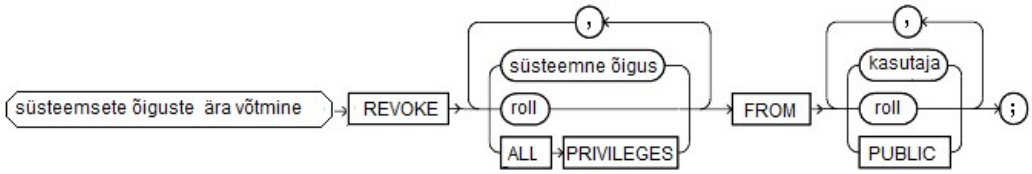
```
CREATE ROLE student;
GRANT AUDIT SYSTEM, CREATE PROCEDURE, CREATE SEQUENCE, CREATE
SESSION, CREATE SYNONYM, CREATE PUBLIC SYNONYM, CREATE TABLE,
SELECT ANY TABLE, CREATE TRIGGER, CREATE TYPE, CREATE VIEW TO student;
```

Ja nüüd anname need õigused kasutajale ”mart”:

GRANT student TO mart;

õiguste ära võtmine

Õiguste andmine võib tähendada ka õiguste ära võtmist. Täpselt nii nagu GRANT käsuga saab anda süsteemseid õigusi, saab neid ära võtta REVOKE-käsuga:



ära saab võtta ainult varem antud õigusi

Siin ei ole midagi pikalt seletada - GRANT-lause kirjelduses kirjeldatu tuleb lihtsalt "tagurpidi pöörata". Teada tuleb ainult seda, et REVOKE-käsuga saab ära võtta ainult neid õigusi, mis eelnevalt on käsuga GRANT antud.

NÄIDE

Võtame näiteks rollilt “student” ära õiguse luua SEQUENCE-sid:

REVOKE CREATE SEQUENCE FROM student;

13.3.4. Õigused ressursside kasutamiseks

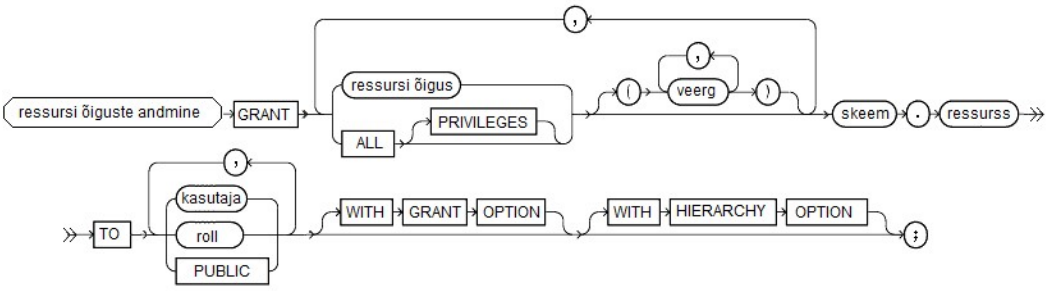
ressursi kasutamise õigusi saab anda kas kasutajale, rollile või kõigile

Lisaks üldistele süsteemsetele õigustele saab igale kasutajale anda õigusi ka teiste kasutajate poolt loodud andmebaasistruktuuride (andmebaasiobjektide) kasutamiseks. Selliseid õigusi saab anda kas ressursi omanik (looja ise) või andmebaasiadministraatori õigustes isik või isik kellele on antud ressursile õigused koos õiguste edasiandmise õigusega (WITH GRANT OPTION).

Ressursi kasutamise õiguse määramiseks tuleb määrata õigus (õigused), mis antakse, seejärel ressurss, millele õigused antakse ja seejärel see (need) kellele õigus (õigused) antakse. "Nendeks kellele õigused antakse" võivad olla kasutajad, rollid ja kõik kasutajad (PUBLIC).

GRANT-lause süntaks

Andmebaasisüsteemis ORACLE näeb käsk GRANT ressursi kasutamise õiguste määramiseks välja järgmine:



Esimeses grupis määratakse ära privileeg (või kõik privileegid – ALL PRIVILEGES) ja ressursi komponendid (näiteks tabeli veerud) , millele antud õigusi rakendatakse. Seejärel määratakse ära andmebaasi ressurss (skeem.ressurss – näiteks tabel), mille komponentidele õigusi määratakse. Seejärel määratakse loend rollidest ja kasutajatest (kasutaja ja/või roll), kellele need privileegid antakse või võtmesõna PUBLIC, mis tähendab, et määratud õigused antakse kõigile kasutajatele – nii nendele kes on juba olemas, kui ka nendele kes luuakse tulevikus.

õigusi saab anda õiguste edasi andmiseks

Kui lisatakse fraas “WITH GRANT OPTION”, siis on nendel kasutajatel või rollidel, kellele õigus antakse, õigus neid õigusi teistele kasutajatele edasi volitada.

kasutusõigusi saab laiendada alam-ressursidele

WITH HIERARHCHY OPTIONS fraasi lisamine garanteerib kirjeldatud õigused ka määratud objektide kohta kirjeldatud alamobjektidele (tabelite korral näiteks ka kõigile antud tabelile kirjeldatud VIEW-dele).

Ressursile antavateks privileegideks on näiteks: DELETE, INSERT, UPDATE või SELECT, mis annavad näiteks õiguse tabelist kustutada kirjeid, lisada sinna uusi kirjeid, uuendada seal olevaid kirjeid ja vaadata (pärida) tabelis olevaid andmeid. Kui kirjeldatud on ka tabeli veerud, siis laienevad kirjeldatud õigused ainult loendis olevatele veergudele.

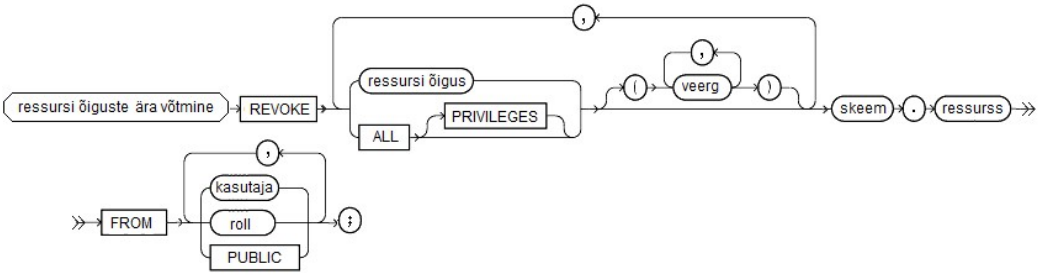
NÄIDE

Anname näiteks kasutajale “mart” ja rollile “student” õiguse vaadata tabeli RASPEL.ISIK (kasutaja RASPEL poolt loodud tabel ISIK) veerge “ID”, “NIMI”, “PERENIMI” ja “PALK”. Uuendada lubame ainult veerge “NIMI” ja “PERENIMI”:

```
GRANT SELECT (ID, NIMI, PERENIMI, PALK), UPDATE (NIMI, PERENIMI)
RASPEL.ISIK TO mart, student;
```

REVOK-lause süntaks

Ressursi kasutamiseks "õiguste andmine" võib tähendada ka õiguste ära võtmist. Täpselt nii nagu GRANT käsuga saab anda ressursi kasutamise õigusi, saab neid ära võtta REVOKE-käsuga:



Siin ei ole midagi pikalt seletada - GRANT-lause kirjelduses kirjeldatu tuleb lihtsalt "tagurpidi pöörata". Teada tuleb ainult seda, et REVOKE-käsuga saab ära võtta ainult neid õigusi, mis eelnevalt on käsuga GRANT antud.

NÄIDE

Võtame näiteks rollilt "student" ära õigused näha tabelis RASPEL.ISIK veeru PALK väärtusi:

```
REVOKE SELECT (PALK) RASPEL.ISIK FROM student ;
```

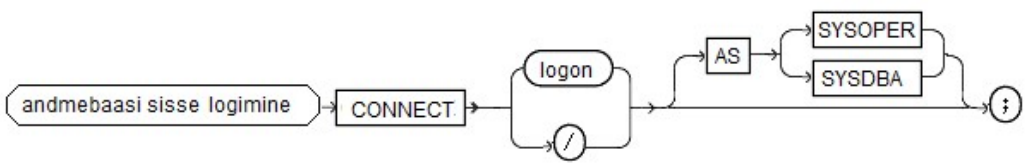
13.4. Kasutajate autoriseerimine

andmeebaasiga ühenduse võtmiseks on vajalik CONNECT-käsk

Kasutaja baasis registreerumiseks on igal andmebaasisüsteemil CONNECT käsk. Kuigi selle süntaks võib olla erinev on sisu üks – kasutaja esitab oma kasutajanime, salasõna ja võib olla veel mingeid juhtandmeid, baas kontrollib nende vastavust enda registreeritud kasutajate omadega ja vastava nimega ning võtmesõnaga registreeritud kasutaja olemasolul käivitab seansi.

CONNECT-lause süntaks

Andmebaasisüsteemis ORACLE on CONNECT-käsu süntaks järgmine:



"logon" tähistab siin literaali (connect-stringi), mis kirjeldab andmebaasi logimise kasutajanime, salasõna ja vajadusel ka andmebaasi nime:

username/password[@database] *(kandilised sulud tähistavad siin seda, et andmebaasi nimi võib puududa)*

vaikimisi andmebaasi sisse logimine

Kui andmebaasi nimi puudub, siis logitakse sisse selle kasutaja õigustega kirjeldatud vaikimisi andmebaasi.

single sign-on

Sümbol "/" - tähistab vaikimisi login-i, kus login parameetrid võetakse lokaalsest operatsioonisüsteemist.

Kui kasutajal on kasutajaõigustega kirjeldatud SYSOPER (andmebaaside loomine) või SYSDBA (juba loodud andmebaaside muutmine) privileegid, siis saab ta baasi logida kas neid privileege kasutades või mitte. Kui vastavaid fraase mitte kasutada logitakse kasutaja baasi kui tavaline kasutaja, kellel on kõik temale antud õigused välja arvatud SYSOPER ja SYSDABA rollidega määratud süsteemi administreerimise õigused.