Administrace Oracle

Práva a role, audit

Filip Řepka 2010

Práva (privileges)

Objekty (tabulky, pohledy, procedury, ...)

jsou v databázi logicky rozděleny do schémat.

Každý uživatel má přiděleno svoje schéma pojmenované podle jeho uživatelského jména.

Předem definovaná schémata

- SYS, SYSTEM
  (odpovídají speciálním systémovým uživatelům)

- PUBLIC
  (odpovídá "skupině" všech uživatelů).

Práva (privileges)

- cílem je omezení uživatele, aby směl manipulovat jen s určitými objekty a to daným způsobem
- každý uživatel má přidělenu množinu práv, kterými disponuje
- dva druhy: **systémová práva** a **práva na objekty**

Systémová práva

- řádově desítky
- používají se pro umožnění nějaké činnosti globálně na všech objektech daného typu

např. SELECT ANY TABLE

umožní uživateli provést příkaz SELECT na libovolné tabulce či pohledu v databázi kromě těch ve schématu SYS

Práva na objekty

- malý počet
- Oracle umožňuje přidělit práva na konkrétní objekty
- každý typ objektu má jistou množinu práv, která mohou být přidělena jeho instancím

	tabulky	pohledy	sekvence	procedury
SELECT	X	X	X	
UPDATE	X	X		
INSERT	X	X		
DELETE	X	X		
ALTER	X		X	
INDEX	X			
REFERENCES	X			
EXECUTE				X

Přidělování práv a rolí

- uživatel může přidělovat systémová práva a role, pokud mu byly přiděleny s nastaveným parametrem ADMIN OPTION

- může také přidělovat práva na objekty ve svém schématu či na objekty, na které my byla přidělena práva s nastaveným parametrem GRANT OPTION

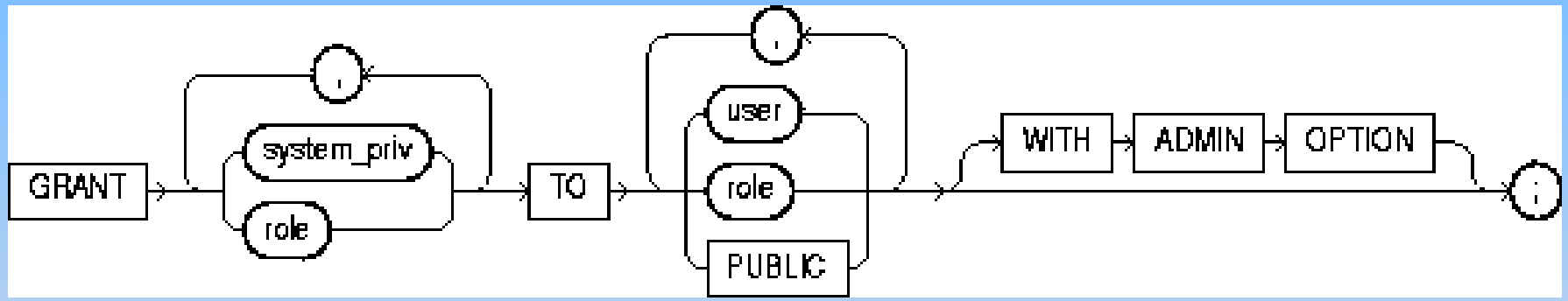
- práva lze přidělit přímo konkrétním uživatelům či roli

  Přidělení práv roli odpovídá jejich přidání do množiny práv, kterou role reprezentuje.

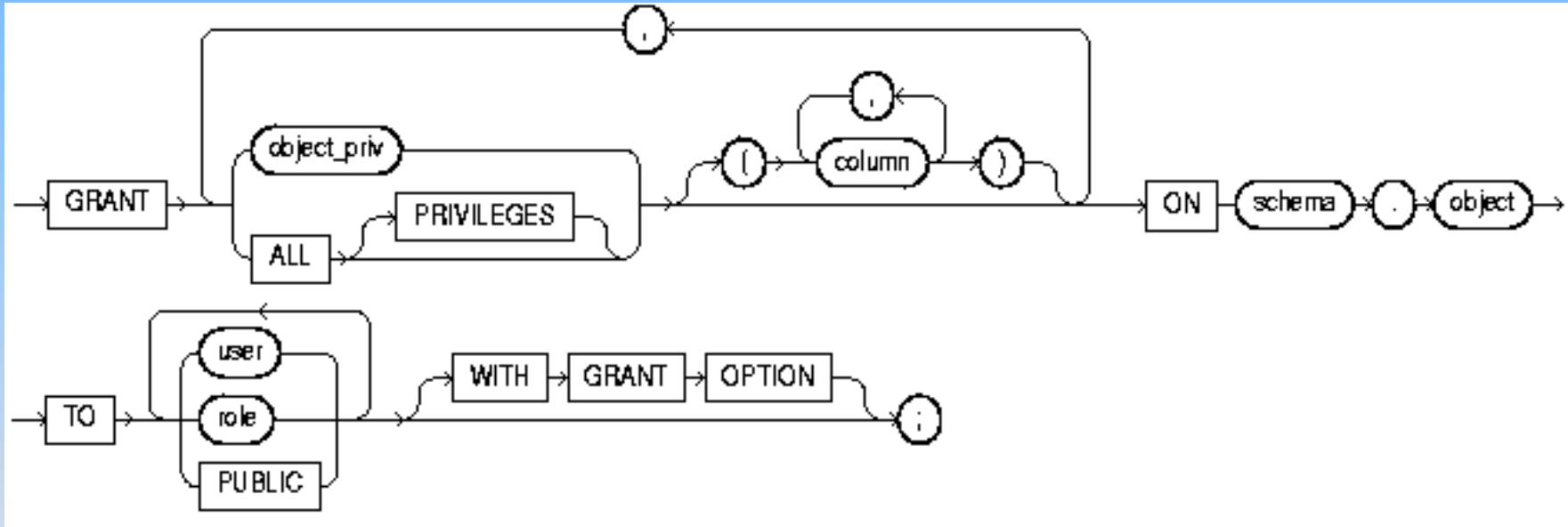
  Analogicky lze přidělit roli (tj. množinu práv) uživateli nebo jiné roli.

- K přidělování práv a rolí slouží dvě verze SQL příkazu GRANT.

Pro systémová práva a role



Pro práva na objekty (zjednodušeno)



Odebírání práv

- příkazem REVOKE

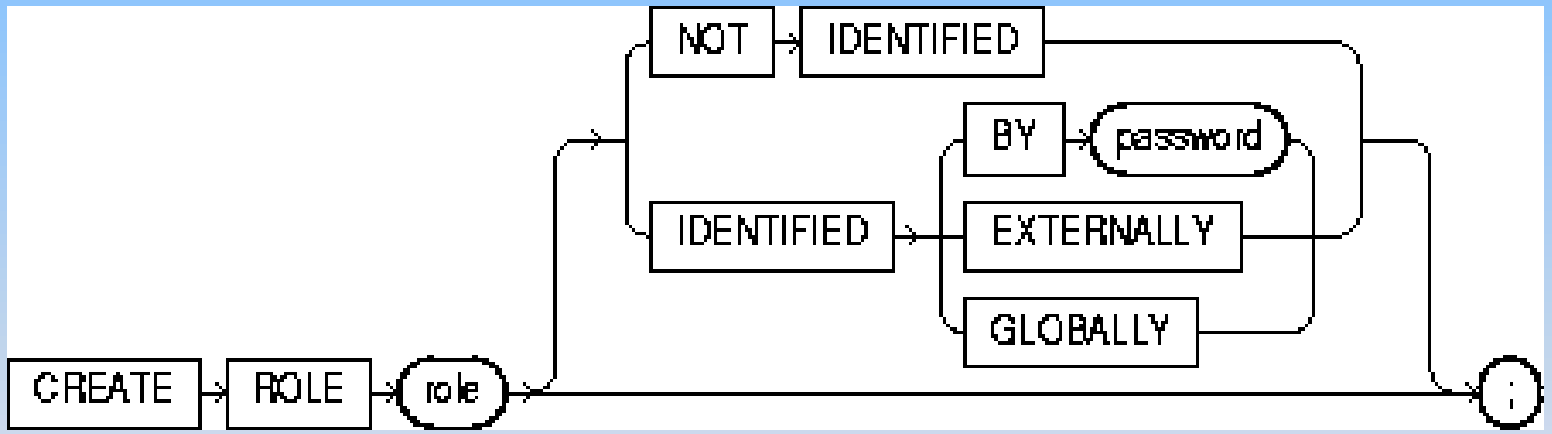
  syntaxe je analogická jako u GRANT s tím rozdílem, že namísto slova TO je slovo FROM.

Role

- je pojmenovaná množina práv
- umožňuje jednoduché přidělení, úpravu a odebrání množiny práv skupinám uživatelů

Vytvoření, změna a zrušení role

- k vytvoření role slouží příkaz CREATE ROLE



Vytvoření, změna a zrušení role

- práva roli se nastavují příkazem GRANT
- roli lze zrušit příkazem DROP ROLE
- změna identifikace se provádí příkazem ALTER ROLE

Předdefinované role

- Jsou v DB ihned po jejím vytvoření

DBA	role administrátora
CONNECT	přidána automaticky každému nově vytvořenému uživateli

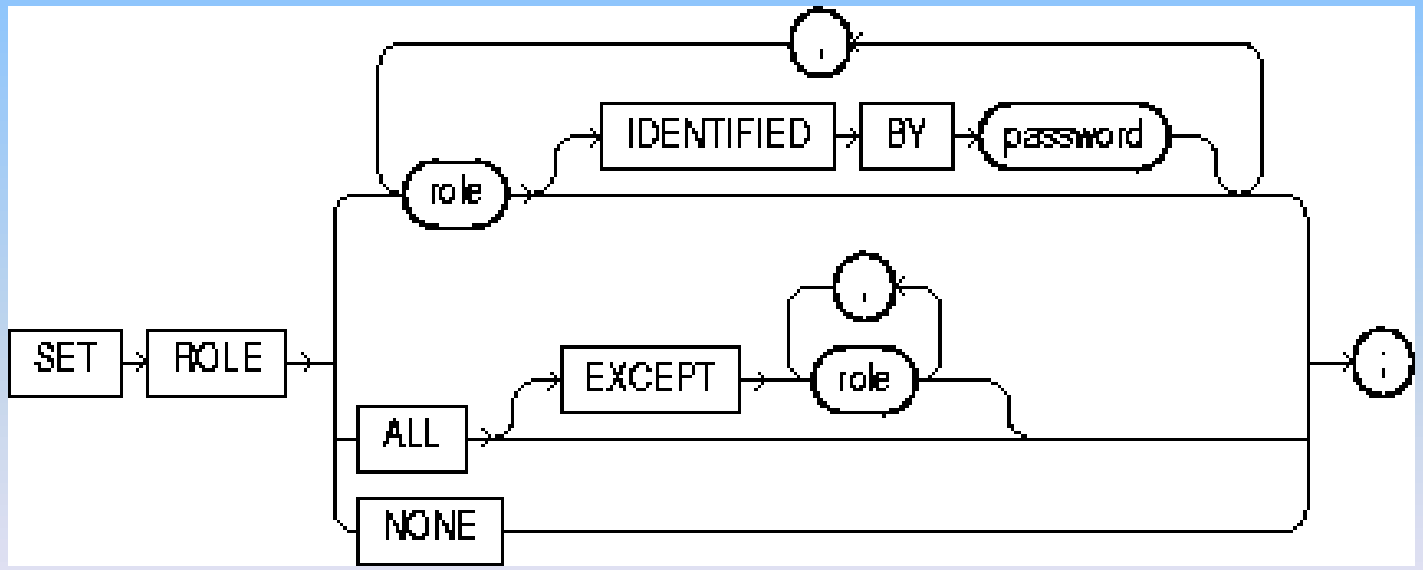
Platnost role

- role může být buď zapnutá - práva, která obsahuje jsou přenesena na uživatele, nebo je vypnutá a práva, která obsahuje jsou uživateli odebrána

- poté, co se uživatel přihlásí k databázi, jsou všechny role, které mu byly přiděleny příkazem GRANT zapnuty

Platnost role

- pokud chce uživatel pro sebe roli zapnout či vypnout, může tak učinit příkazem SET ROLE



Audit DB

Audit DB

- sledování uživatelských aktivit v DB
- lze sledovat operace, uživatele, tabulky ...
- určitá míra auditu je vhodná vždy

Je však důležité si rozmyslet, co vše se bude sledovat, jak mnoho informací to bude produkovat a jak moc to může ovlivnit při velkém zatížení dotazy na DB

Ukládání informací

- Audit Trail
- operační systém
- oboje zároveň

Audit Trail

- uložen v datového slovníku databáze
  - tabulka SYS.AUD$
- lze používat předdefinované pohledy z DB
- Lze použít nástroje Oracle pro tvorbu zpráv (Oracle Reports)

Audit Trail

- obsah závisí na konkrétním nastavení auditu

- Vždy obsahuje:
  - login uživatele (v operačním systému)
  - uživatelské jméno
  - identifikátor session
  - identifikátor terminálu
  - jméno objektu, ke kterému je přistupováno
  - typ prováděné operace
  - návratový kód operací
  - Datum a čas

Operační systém

- podpora OS je různá
  windows – event log

- data z různých programů na jednom místě

- komplexnější analýza činnosti

Operační systém

- ukládají se:
  - stejné informace jako do Audit Trail
  - záznamy generované operačním systémem
  - činnosti DB, které se zaznamenávají vždy
  - činnost administrátorů
- složení záznamů
  - kód akce
  - přístupová práva
  - výsledek akce

Vždy zaznamenávané akce

- ukládají se i v případě vypnutého auditu a to do systémového souboru

- připojení k instanci s administrátorskými právy
- spuštění databáze
  (záznam loginu, terminálu, času, a stavu auditování)
- vypnutí databáze
  (záznam loginu, terminálu, data a času)

Audit administrátorů

- uživatelé s oprávněním SYS
- lze zapnout v konfiguračním souboru
  AUDIT_SYS_OPERATIONS = TRUE (defaultně false)
- data se ukládají do OS
  AUDIT_TRAIL není brán v potaz

Zapnutí a vypnutí auditu

- každý přihlášený uživatel může kdykoliv nastavit sledování příkazů, práv a objektů

- musí být nejdříve povoleno auditování

  nastavuje se v konfiguračním souboru

  zpravidla nastavuje „security administrator“

  pro aplikovaní změn nutné restartovat Oracle

  (jedná se o statické parametry)

Zapnutí a vypnutí auditu

- parametry pro nastavení auditu:

  AUDIT_TRAIL

  AUDIT_SYS_OPERATIONS

  AUDIT_FILE_DEST

AUDIT_TRAIL

- slouží pro nastavení auditování

- možnosti:

  DB – zapne auditing, záznamy ukládány do Audit Trail databáze

  OS - zapne auditing, záznamy ukládány do OS

  NONE - vypíná auditing

AUDIT_FILE_DEST

- nastavuje adresář, kam se ukládají záznamy
  jen pro AUDIT_TRAIL = OS

- defaultní adresář je $ORACLE_HOME/rdbms/audit

- liší se podle OS

Příkaz AUDIT

- Příkazy - zaznamenává vykonávání příkazů
- Privilegia – zaznamenává příkazy v závislosti na přístupových právech
- Objekty - sledování příkazů na určitých objektech

Příkaz AUDIT

- parametry

  BY SESSION - pro všechny příkazy jeden záznam

  BY ACCESS – jeden záznam pro každý příkaz

  WHENEVER (NOT) SUCCESSFUL

  NOT EXISTS

Zdroje

- http://download.oracle.com/docs/cd/B10501_01/server.920/a96521/privs.htm
- http://tmd.havit.cz/Papers/Oracle/Oracle.htm
- http://download.oracle.com/docs/cd/B10501_01/server.920/a96521/audit.htm#ADMIN026