Привилегии и роли

Графеева Н.Г.

2017

- Для осуществления каких-либо действий в базе данных пользователю должно быть дано на это право. Любое действие и любой объект БД могут являться предметом разграничения прав доступа.

- ***Привилегия*** (privilege) – это право выполнить определенное действие над определенным объектом БД.
-
- Привилегии в ORACLE делятся на ***объектные*** и ***системные***.

Примеры объектных привилегий

- SELECT - выбрать данные из таблицы или последовательности
- UPDATE - отредактировать таблицу
- DELETE - удалить записи из таблицы
- EXECUTE - исполнить процедуру

Примеры системных привелегий

- CREATE USER - создать нового пользователя
- ALTER USER - редактировать пользователя
- DROP USER - удалить пользователя
- CREATE TABLE - создать таблицу
- CREATE PROCEDURE - создать процедуру
- CREATE SEQUENCE - создать секвенцию
- CREATE TRIGGER - создать триггер

Выдача объектных привилегий

- Синтаксис:

- GRANT <что> ON <объект> TO <кому> [WITH GRANT OPTION]

Пример

- Пользователь GRIGORY выполнил следующие команды:
- GRANT SELECT ON mytable TO OLEG

- GRANT SELECT ON mytable TO OLEG WITH GRANT OPTION

- GRANT EXECUTE ON myproc TO OLEG

- Пользователь OLEG теперь может выполнять следующие команды:

- select * from GRIGORY.mytable
- GRANT SELECT ON GRIGORY.mytable TO IVAN
- … GRIGORY.myproc(…..)

Упражнение

- Уточните название схемы (в ORACLE APEX) своего соседа слева (или справа).
- Выдайте ему привилегию на просмотр одной из своих таблиц и одной из своих функций или процедур.
- Убедитесь, что можете прочитать содержимое таблицы соседа и выполнить его функцию.

Выдача системных привилегий

- Синтаксис:

- GRANT <что> TO <кому> [WITH ADMIN OPTION]

Пример

- GRANT CREATE USER TO pom WITH ADMIN OPTION;
- GRANT ALTER USER TO pom;
- GRANT DROP USER TO pom;
- GRANT CREATE ROLE TO pom;

Удаление объектных привилегий

- Синтаксис:

- REVOKE <что> ON <объект> FROM <у кого>

Пример

- REVOKE SELECT ON mytable FROM oleg
- REVOKE EXECUTE ON myproc FROM oleg

Удаление системных привилегий

- Синтаксис:

- REVOKE <что> FROM <у кого>

Роли

- Роль – это именованная группа привилегий.
- Роли обеспечивают:
- Эффективность администрирования
- Динамическое управление правами пользователей
- Роли могут создавать пользователи, имеющие системную привилегию CREATE ROLE (такая привилегия есть у администраторов).

Создание роли

- Синтаксис:

- CREATE ROLE <имя роли>

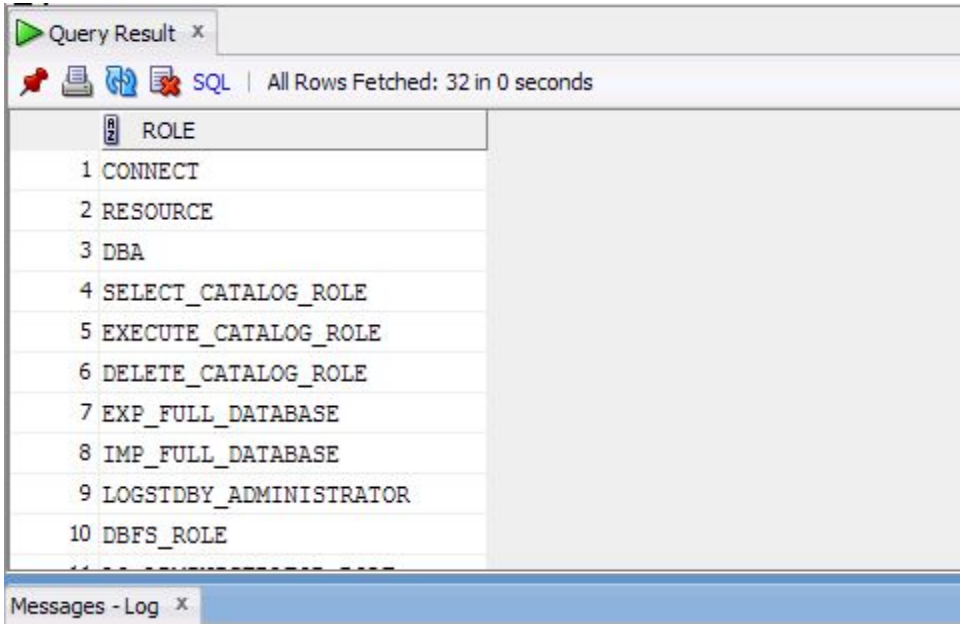
Пример

- Создание роли, выдача объектных привилегий и предоставление роли пользователю VASYA:

- CREATE ROLE manager;
- GRANT select ON mytable TO manager;
- GRANT execute ON myproc TO manager;
- GRANT manager TO VASYA;

Предопределенные роли (как обстоят дела в ORACLE XE 11)

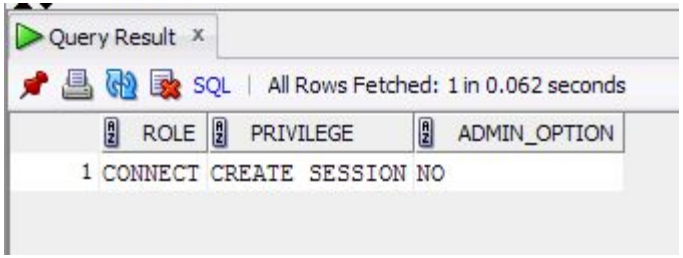
- select role from dba_roles



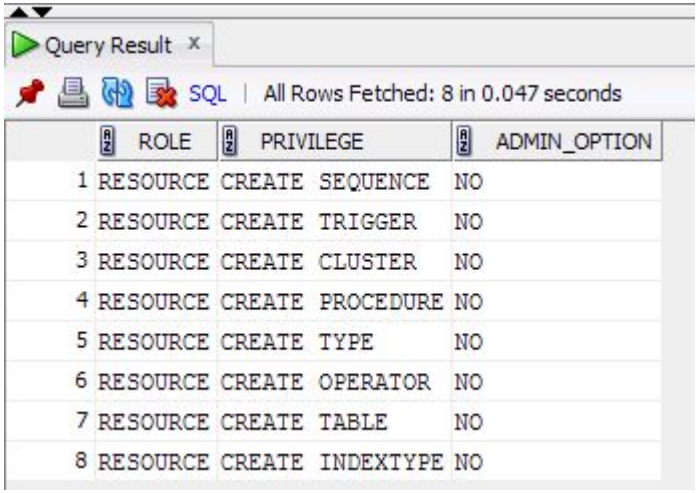
Полезные представления

- ROLE_SYS_PRIVS
- ROLE_TAB_PRIVS
- ROLE_ROLE_PRIVS

select * from role_sys_privs where role = 'CONNECT'

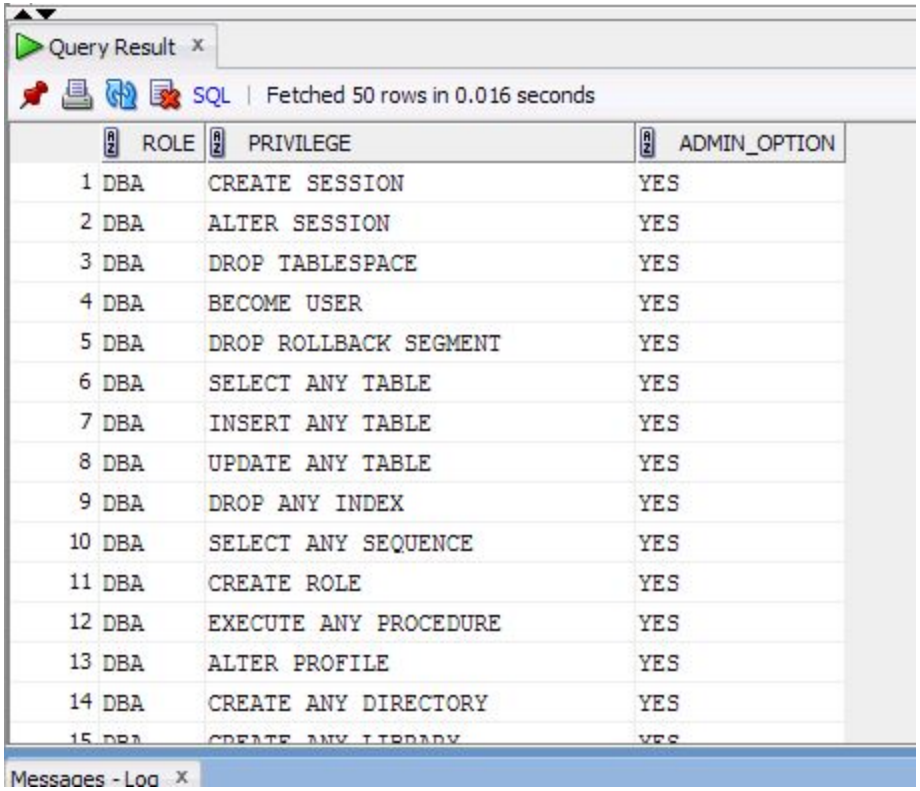
- 

select * from role_sys_privs where role = 'RESOURCE'

- 

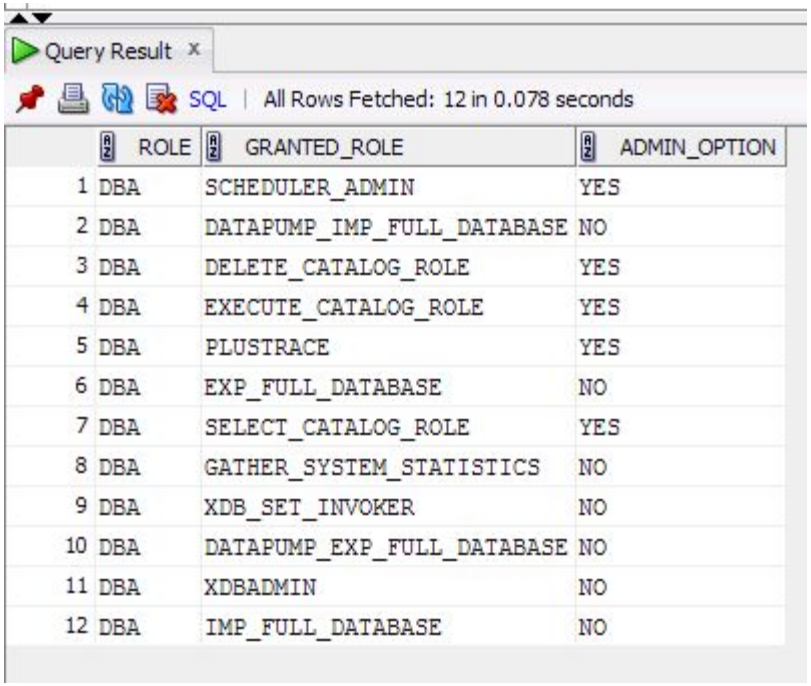
	ROLE	PRIVILEGE	ADMIN_OPTION
1	RESOURCE	CREATE SEQUENCE	NO
2	RESOURCE	CREATE TRIGGER	NO
3	RESOURCE	CREATE CLUSTER	NO
4	RESOURCE	CREATE PROCEDURE	NO
5	RESOURCE	CREATE TYPE	NO
6	RESOURCE	CREATE OPERATOR	NO
7	RESOURCE	CREATE TABLE	NO
8	RESOURCE	CREATE INDEXTYPE	NO

select * from role_sys_privs where role = 'DBA'

- 

	ROLE	PRIVILEGE	ADMIN_OPTION
1	DBA	CREATE SESSION	YES
2	DBA	ALTER SESSION	YES
3	DBA	DROP TABLESPACE	YES
4	DBA	BECOME USER	YES
5	DBA	DROP ROLLBACK SEGMENT	YES
6	DBA	SELECT ANY TABLE	YES
7	DBA	INSERT ANY TABLE	YES
8	DBA	UPDATE ANY TABLE	YES
9	DBA	DROP ANY INDEX	YES
10	DBA	SELECT ANY SEQUENCE	YES
11	DBA	CREATE ROLE	YES
12	DBA	EXECUTE ANY PROCEDURE	YES
13	DBA	ALTER PROFILE	YES
14	DBA	CREATE ANY DIRECTORY	YES
15	DBA	CREATE ANY LIBRARY	YES

select * from role_role_privs where role = 'DBA'

- 
Query Result

SQL | All Rows Fetched: 12 in 0.078 seconds

	ROLE	GRANTED_ROLE	ADMIN_OPTION
1	DBA	SCHEDULER_ADMIN	YES
2	DBA	DATAPUMP_IMP_FULL_DATABASE	NO
3	DBA	DELETE_CATALOG_ROLE	YES
4	DBA	EXECUTE_CATALOG_ROLE	YES
5	DBA	PLUSTRACE	YES
6	DBA	EXP_FULL_DATABASE	NO
7	DBA	SELECT_CATALOG_ROLE	YES
8	DBA	GATHER_SYSTEM_STATISTICS	NO
9	DBA	XDB_SET_INVOKER	NO
10	DBA	DATAPUMP_EXP_FULL_DATABASE	NO
11	DBA	XDBADMIN	NO
12	DBA	IMP_FULL_DATABASE	NO

Как создать пользователя-разработчика

- Типовое создание пользователя-разработчика (создание пользователя + выдача ролей CONNECT, RESOURCE).

- **Пример**

- CREATE USER CAT_DEVELOPER IDENTIFIED BY CAT_DEVELOPER;
- GRANT CONNECT, RESOURCE TO CAT_DEVELOPER;

Как создать типичного пользователя приложения

- Создать роль, наполнить ее объектными и системными привилегиями, создать пользователя и предоставить ему эту роль.

- **Пример**

- CREATE ROLE APP_USER;
- GRANT EXECUTE ON ESTORE.XMLPKG TO APP_USER;
- CREATE USER CAT_APP_USER IDENTIFIED BY CAT_APP_USER;
- GRANT APP_USER TO CAT_APP_USER;