

Administração de Banco de Dados

Aula 12

Prof. Marcos Alexandruk



Aula 12

Privilégios de sistema

Privilégios de objetos



Privilégios de sistema

Privilégios de sistema

- Privilégios de sistema envolvem os direitos de realizar determinadas ações sobre objetos do banco de dados e alteração de parâmetros de sistema, dentre outros.
- A versão 11.2 do Oracle Database oferece **208 privilégios** de sistema que são apresentados na tabela de dicionário de dados **SYSTEM_PRIVILEGE_MAP**.

Privilégios de sistema

```
SELECT NAME FROM SYSTEM_PRIVILEGE_MAP;
```

```
NAME
```

```
-----
```

```
ALTER SYSTEM
```

```
AUDIT SYSTEM
```

```
CREATE SESSION
```

```
CREATE TABLESPACE
```

```
ALTER TABLESPACE
```

```
DROP TABLESPACE
```

```
CREATE USER
```

```
ALTER USER
```

```
DROP USER
```

```
CREATE TABLE
```

```
CREATE ANY TABLE
```

```
ALTER ANY TABLE
```

```
DROP ANY TABLE
```

```
...
```

```
...
```

```
CREATE INDEX
```

```
CREATE ANY INDEX
```

```
ALTER ANY INDEX
```

```
DROP ANY INDEX
```

```
SYSDBA
```

```
SYSOPER
```

```
CREATE VIEW
```

```
ALTER DATABASE
```

```
CREATE PROCEDURE
```

```
CREATE ANY PROCEDURE
```

```
...
```

Privilégios de sistema

PRIVILÉGIO DE SISTEMA	DESCRIÇÃO
SYSDBA SYSOPER	Criar uma nova entrada no arquivo externo de senhas, inicializar ou interromper uma instância, criar, alterar e recuperar um banco de dados, etc.
ALTER SYSTEM	Alterar os parâmetros no arquivo SPFILE. Emitir instruções ALTER SYSTEM.
AUDIT SYSTEM	Fazer auditoria no banco de dados.
CREATE SESSION	Conectar com o banco de dados.
ALTER DATABASE	Alterar o estado de um banco de dados. Exemplo: alterar o estado de MOUNT para OPEN.
CREATE TABLESPACE	Criar novos tablespaces.
ALTER TABLESPACE	Alterar parâmetros dos tablespaces.
DROP TABLESPACE	Eliminar tablespaces.
CREATE USER	Criar novos usuários.
ALTER USER	Alterar privilégios e outros dados dos usuários.
DROP USER	Eliminar usuários.
CREATE TABLE	Criar novas tabelas em seu próprio esquema.
CREATE ANY TABLE	Criar novas tabelas em qualquer esquema.
ALTER ANY TABLE	Alterar as tabelas em qualquer esquema.
DROP ANY TABLE	Eliminar tabelas em qualquer esquema.
CREATE PROCEDURE	Criar uma procedure, função ou pacote em seu próprio esquema.
CREATE ANY PROCEDURE	Criar uma procedure, função ou pacote em qualquer esquema.
...	...

Privilégios de sistema

Concedendo privilégios de sistema

- Privilégios são concedidos aos usuários utilizando-se o comando GRANT. O exemplo a seguir apresenta o comando para conceder ao usuário FULANO os privilégios necessários para criar tabelas e visões em seu próprio esquema:

```
GRANT CREATE TABLE, CREATE VIEW TO FULANO;
```

- Privilégios também podem ser concedidos a todos os usuários do banco de dados. Neste caso, os privilégios devem ser concedidos a um grupo especial denominado PUBLIC:

```
GRANT CREATE TABLE TO PUBLIC;
```


Privilégios de sistema

Concedendo privilégios de sistema

- Pode-se também conceder privilégios a determinado usuário e permitir que ele, por sua vez, também conceda para outros os mesmos privilégios que está recebendo. Para que isto seja possível, deve-se acrescentar a opção **WITH ADMIN OPTION** ao comando **GRANT**:

```
GRANT CREATE TABLE TO FULANO WITH ADMIN OPTION;
```

- Se a permissão do usuário **FULANO** para conceder seus privilégios a outros for revogada, os usuários aos quais ele concedeu os privilégios continuarão a retê-los (não serão revogados).

Privilégios de sistema

Revogando privilégios de sistema

- Os privilégios concedidos aos usuários podem ser revogados. Utiliza-se para isso o comando **REVOKE**. O exemplo a seguir apresenta o comando para revogar o privilégio **CREATE VIEW** concedido anteriormente ao usuário **FULANO**.

```
REVOKE CREATE VIEW FROM FULANO;
```

Privilégios de sistema

Visões de dicionário de dados de privilégios de sistema

- O dicionário de dados apresenta algumas visões que podem ser consultadas para obter-se os privilégios concedidos aos usuários do banco de dados.
- O DBA poderá, por exemplo, listar os privilégios de sistema atribuídos diretamente para o usuário SCOTT através da seguinte consulta ao dicionário de dados:

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'SCOTT' ;
```

Privilégios de sistema

Visões de dicionário de dados de privilégios de sistema

VISÃO	DESCRIÇÃO
DBA_SYS_PRIVS	Privilégios de sistema atribuídos a usuários e papéis.
SESSION_PRIVS	Privilégios de sistema concedidos ao usuário na sessão atual diretamente ou através de um papel.
ROLE_SYS_PRIVS	Privilégios de sistema concedidos ao usuário na sessão atual através de um papel.



Privilégios de objetos

Privilégios de objetos

- Privilégio de objetos é o direito de realizar um tipo específico de ação sobre determinados objetos de um banco de dados (por exemplo: tabelas, visões e procedures) que não fazem parte do esquema do usuário.
- Como ocorre com os privilégios de sistema, para conceder privilégios sobre objetos de banco de dados utiliza-se o comando GRANT e para revogá-los utiliza-se o comando REVOKE.
- Os privilégios de objetos podem ser concedidos a todos os usuários do banco de dados através do grupo especial PUBLIC.
- Pode-se também conceder privilégios de objetos a determinado usuário e permitir que ele, por sua vez, também conceda-os para outros. Para que isto seja possível deve-se acrescentar a opção WITH GRANT OPTION ao comando GRANT.

```
GRANT SELECT ON NOME_TABELA TO FULANO WITH GRANT OPTION;
```

- Porém diferente do que acontece quando se concede permissões de sistema, se os privilégios de objetos do usuário forem revogados, **serão também revogados os privilégios de todos os usuários da cadeia**, isto é, que receberam seus privilégios através deste usuário (FULANO no exemplo acima).

Privilégios de objetos

Privilégios de tabela

- Os privilégios de tabelas podem ser concedidos para operações de DDL (Data Definition Language) e de DML (Data Manipulation Language).
 - As operações de DDL incluem adicionar, modificar ou descartar colunas das tabelas ou ainda criar índices nas tabelas.
 - As operações de DML incluem os comandos INSERT, UPDATE e DELETE. É possível restringir os privilégios a determinadas colunas das tabelas.

```
GRANT UPDATE (ID, NOME) ON FULANO.FUNCIONARIO TO SCOTT;
```

- **O Oracle não permite conceder privilégio SELECT sobre determinadas colunas da tabela. (Solução: Criar uma view apenas com as colunas específicas e conceder o privilégio sobre a view.**
- Os privilégios concedidos anteriormente poderão ser revogado a qualquer momento utilizando-se o comando REVOKE:

```
REVOKE UPDATE ON FULANO.FUNCIONARIO FROM SCOTT;
```

Privilégios de objetos

Visões de dicionário de dados de privilégios de tabela

- O dicionário de dados apresenta algumas visões que podem ser consultadas para obter-se os privilégios de objetos concedidos aos usuários do banco de dados.
- A consulta ao dicionário de dados a seguir apresenta os privilégios de tabela concedidos diretamente ao usuário SCOTT:

```
SELECT * FROM DBA_TAB_PRIVS WHERE GRANTEE = 'SCOTT' ;
```

Privilégios de objetos

Visões de dicionário de dados de privilégios de objetos

VISÃO	DESCRIÇÃO
DBA_TAB_PRIVS	Privilégios de tabelas concedidos a usuários e papéis.
DBA_COL_PRIVS	Privilégios de colunas concedidos ao usuário na sessão atual diretamente ou através de um papel.
SESSION_PRIVS	Privilégios de sistema concedidos ao usuário na sessão atual diretamente ou através de um papel.
ROLE_TAB_PRIVS	Privilégios de tabelas concedidos ao usuário na sessão atual através de um papel.