Administração de Banco de Dados

Aula 13

Prof. Marcos Alexandruk

Aula 13

Gerenciamento de papéis (roles)

Gerenciamento de papéis (roles)

- Papéis ou roles são grupos identificados de privilégios que podem incluir tanto privilégios de sistema como privilégios de objetos.
- A utilização de papéis facilita a administração dos privilégios concedidos aos usuários do banco de dados. Pois, em vez de conceder diversos privilégios individualmente aos usuários, é possível concedê-los a um papel e este, por sua vez, ser concedido aos usuários.
- Caso seja necessária alguma alteração, esta poderá ser feita no papel e, consequentemente, os privilégios de todos os usuários que utilizam este papel serão automaticamente alterados. Isto pode reduzir significativamente os números de comandos GRANT e REVOKE necessários para a administração dos privilégios dos usuários do banco de dados.

Gerenciamento de papéis (roles)

Papéis predefinidos

- A tabela a seguir apresenta alguns dos principais papéis predefinidos:

PAPEL	PRIVILÉGIO
CONNECT	CREATE SESSION
RESOURCE	CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE.
DBA	Todos os privilégios de sistema WITH ADMIN OPTION.
SELECT_CATALOG_ROLE	Privilégio SELECT nos objetos do dicionário de dados.
EXP_FULL_DATABASE	Privilégio para exportar todos os objetos do banco de dados.
IMP_FULL_DATABASE	Privilégio para importar todos os objetos do banco de dados.

Gerenciamento de papéis (roles)

Criando um papel

- Para criar um novo papel (role) deve-se utilizar o comando CREATE ROLE. Porém, é necessário possuir o privilégio de sistema CREATE ROLE que geralmente é concedido apenas aos administradores do banco de dados.

```
CREATE ROLE TESTE;
```

Descartando um papel

- Para descartar um papel deve-se utilizar o comando DROP ROLE, conforme o exemplo apresentado a seguir.

```
DROP ROLE TESTE;
```

Gerenciamento de papéis (roles)

Concedendo privilégios a um papel

- Privilégios são concedidos a um papel da mesma forma que seriam concedidos a um usuário do banco de dados, através do comando GRANT.

- Exemplo: conceder um privilégio de objeto na tabela FUNCIONARIOS ao papel GERENTE_RH. (Nota: o papel GERENTE_RH deve ser criado antes.)

```
GRANT SELECT ON FUNCIONARIOS TO GERENTE_RH;
```

- Exemplo: conceder um privilégio de sistema ao papel GERENTE_RH.

```
GRANT CREATE TRIGGER TO GERENTE_RH;
```

Gerenciamento de papéis (roles)

Atribuindo um papel a um usuário

- Para atribuir um papel a determinado usuário do banco de dados deve-se utilizar o comando GRANT.

  No exemplo a seguir observa-se a atribuição do papel GERENTE_RH ao usuário FULANO.

```
GRANT GERENTE_RH TO FULANO;
```

- Caso sejam concedidos outros privilégios ao papel GERENTE_RH estes serão imediatamente atribuídos ao usuário FULANO.

Gerenciamento de papéis (roles)

Atribuindo um papel a outro papel

- Papéis podem também ser atribuídos a outros papéis permitindo assim que o DBA tenha a sua disposição uma hierarquia de papéis.
- No exemplo a seguir, em vez de atribuir-se privilégios de objetos individuais ao papel TODOS_DEPT, preferiu-se atribuir os papéis MM_DEPT, RH_DEPT, FI_DEPT e SD_DEPT ao papel TODOS_DEPT.

```
GRANT MM_DEPT, RH_DEPT, FI_DEPT, SD_DEPT TO TODOS_DEPT;
```

- Portanto, o papel TODOS_DEPT poderia, por exemplo, ser atribuído ao presidente da empresa e este teria acesso às tabelas de todos os departamentos.

```
GRANT TODOS_DEPT TO USUARIO_PRESIDENTE;
```

- O papel TODOS_DEPT poderia ter também outros privilégios de sistema ou de objetos que não seriam atribuídos aos outros (MM_DEPT, RH_DEPT, FI_DEPT e SD_DEPT).

Gerenciamento de papéis (roles)

Revogando um papel

- Revoga-se um papel através do comando REVOKE:

```
REVOKE GERENTE_RH FROM FULANO;
```

- Caso outros papéis atribuídos ao usuário FULANO tiverem alguns dos privilégios concedidos ao papel GERENTE_RH, o usuário (FULANO) continuará a retê-los até que sejam explicitamente revogados.

Gerenciamento de papéis (roles)

Ativando um papel protegido por senha

- O DBA poderá atribuir uma senha a um papel, aumentando com esta medida a segurança.

```
CREATE ROLE TESTE_SENHA IDENTIFIED BY ABC123;
```

- O papel TESTE_SENHA deve ser concedido normalmente através do comando GRANT.

```
GRANT TESTE_SENHA TO FULANO;
```

- Quando o usuário FULANO conectar-se ao banco de dados deverá fornecer o nome do papel e a sua respectiva senha para que possa "receber" os privilégios.

```
SET ROLE TESTE_SENHA IDENTIFIED BY ABC123;
```

Gerenciamento de papéis (roles)

Visões de dicionário de dados referentes aos papéis

VISÃO	DESCRIÇÃO
DBA_ROLES	Apresenta todos os papéis e se eles requerem senha.
DBA_ROLE_PRIVS	Apresenta os papéis concedidos a outros usuários ou a outros papéis.
ROLE_ROLE_PRIVS	Apresenta os papéis concedidos a outros papéis.
ROLE_SYS_PRIVS	Apresenta os privilégios de sistema que foram concedidos aos papéis.
ROLE_TAB_PRIVS	Apresenta os privilégios de tabelas e colunas de tabelas que foram concedidos aos papéis.
SESSION_ROLES	Apresenta os papéis que estão em efeito na sessão atual.