
ORACLE
Academy

Programação de Banco de Dados com SQL

17-1
Controlando o Acesso do Usuário

ORACLE Academy

Objetivos

Esta lição abrange os seguintes objetivos:

- Identificar a diferença entre privilégios de objeto e privilégios de sistema
- Construir os dois comandos necessários para permitir que um usuário acesse um banco de dados
- Construir e executar uma instrução GRANT… ON …TO para atribuir privilégios aos objetos no esquema a outros usuários e/ou PUBLIC
- Consultar o dicionário de dados para confirmar os privilégios concedidos

Finalidade

- Se você divide um computador com outras pessoas, na escola ou em casa, provavelmente algum trabalho seu já foi visualizado, alterado ou excluído por alguém.
- Não seria bom poder controlar os privilégios que outras pessoas têm em seus arquivos pessoais?
- Assim como na escola ou em casa, a segurança dos dados é muito importante nos bancos de dados.
- Nesta lição, você aprenderá a conceder ou remover o acesso aos objetos de banco de dados como um meio de controlar quem pode alterar, excluir, atualizar, inserir, indexar ou referenciar esses objetos.

Controlando o Acesso do Usuário

- Em um ambiente com vários usuários, você vai querer manter a segurança do acesso e uso dos bancos de dados.
- Com a segurança de banco de dados do Servidor Oracle, você pode fazer o seguinte:
  - Controlar o acesso ao banco de dados
  - Conceder acesso a objetos específicos do banco de dados
  - Confirmar os privilégios concedidos e recebidos no dicionário de dados Oracle
  - Criar sinônimos para objetos de banco de dados

Segurança de Banco de Dados

- A segurança de banco de dados pode ser dividida em duas categorias:
  - Segurança de Sistema
  - Segurança de dados
- Segurança de sistema abrange o acesso e uso do banco de dados no nível do sistema, como a criação de usuários, nomes de usuários e senhas; a alocação de espaço em disco para os usuários; e a concessão dos privilégios de sistema que os usuários podem usar, como criar tabelas, views e sequências.
- Existem mais de 100 privilégios de sistema diferentes.

Segurança de Banco de Dados

- A segurança de dados (também conhecida como segurança de objetos) está relacionada aos privilégios de objeto, que abrangem o acesso e uso dos objetos de banco de dados e as ações que os usuários podem executar nesses objetos.
- Esses privilégios incluem a capacidade de executar instruções DML.

Privilégios e Esquemas

- Privilégio é o direito de executar certas instruções SQL.
- O DBA é um usuário de alto nível com a capacidade de conceder aos usuários acesso ao banco de dados e seus objetos.
- Os usuários precisam de privilégios de sistema para obter acesso ao banco de dados.
- Eles precisam de privilégios de objeto para manipular o conteúdo dos objetos no banco de dados.
- Os usuários também podem receber permissão para conceder privilégios adicionais a outros usuários ou a atribuições, que são grupos nomeados de privilégios relacionados.

Privilégios e Esquemas

- Um esquema é um grupo de objetos, como tabelas, views e sequências.
- O esquema pertence a um usuário do banco de dados e tem o mesmo nome que o usuário.
- Neste curso, o nome do seu esquema é uma combinação do seu país/estado, escola, curso e número do aluno.
- Por exemplo: brsp_etec_sql01_a22

Segurança de Sistema

- Este nível de segurança abrange o acesso e uso do banco de dados no nível do sistema.
- Existem mais de 100 privilégios de sistema diferentes.
- Privilégios de sistema como a capacidade de criar ou remover usuários ou remover ou fazer backup de tabelas geralmente pertencem apenas ao DBA.

Segurança de Sistema

- Esta tabela lista alguns dos privilégios de sistema que o DBA normalmente não concederia a outros usuários.
- Você gostaria que outro usuário pudesse eliminar suas tabelas?

Privilégio de Sistema	Operações Autorizadas
CREATE USER	O grantee pode criar outros usuários Oracle (um privilégio necessário à função de DBA).
DROP USER	O grantee pode eliminar um usuário.
DROP ANY TABLE	O grantee pode eliminar uma tabela em qualquer esquema.
BACKUP ANY TABLE	O grantee pode fazer backup de uma tabela em qualquer esquema com o utilitário de exportação.
SELECT ANY TABLE	O grantee pode consultar tabelas, views ou instantâneos em qualquer esquema.
CREATE ANY TABLE	O grantee pode criar tabelas em qualquer esquema.

Privilégios de Sistema

- O DBA cria o usuário executando a instrução CREATE USER.
- Nesse momento, o usuário não tem privilégios.
- Em seguida, o DBA pode conceder os privilégios necessários a esse usuário.
- Sintaxe:

```
CREATE USER usuário
IDENTIFIED BY senha;
```

- Exemplo:

```
CREATE USER  scott
IDENTIFIED BY ur35scott;
```

Privilégios de Sistema

- Ao usar a instrução ALTER USER, um usuário pode mudar sua senha.
- Exemplo:

```
ALTER USER scott
IDENTIFIED BY imscott35;
```

Privilégios de Sistema do Usuário

- O DBA usa a instrução GRANT para alocar privilégios de sistema para o usuário.
- Os privilégios de sistema determinam o que o usuário pode fazer no nível do banco de dados.
- Após receber os privilégios, o usuário poderá usá-los imediatamente.

```
GRANT privilégio [, privilégio...]
TO usuário [, usuário| atribuição, PUBLIC...];
```

```
GRANT  create session, create table, create sequence, create view
TO scott;
```

Privilégios de Sistema do Usuário

- O usuário deve ter o privilégio CREATE SESSION e um id do usuário para poder acessar um banco de dados.
- Você não pode executar o comando CREATE SESSION no Oracle Application Express. Isso acontece automaticamente em segundo plano.

Privilégio de Sistema	Operações Autorizadas
CREATE SESSION	Conectar-se ao banco de dados.
CREATE TABLE	Criar tabelas no esquema do usuário.
CREATE SEQUENCE	Criar uma sequência no esquema do usuário.
CREATE VIEW	Criar uma view no esquema do usuário.
CREATE PROCEDURE	Criar um procedure, função ou pacote no esquema do usuário.

Segurança de Objetos

- Este nível de segurança abrange o acesso e uso dos objetos de banco de dados e as ações que os usuários podem executar neles.

Privilégios de Objeto

- Cada objeto tem um conjunto particular de privilégios que podem ser concedidos.
- A tabela abaixo lista os privilégios de vários objetos.

Privilégio de Objeto	Tabela	View	Sequência	Procedure
ALTER	X		X	
DELETE	X	X		
EXECUTE				X
INDEX	X	X		
INSERT	X	X		
REFERENCES	X			
SELECT	X	X	X	
UPDATE	X	X		

Privilégios de Objeto

- É importante observar estes três pontos relacionados a privilégios de objeto:
  - Os únicos privilégios que se aplicam a uma sequência são SELECT e ALTER.
  - Lembre-se: uma sequência usa ALTER para alterar as opções INCREMENT, MAXVALUE, CACHE/NOCACHE ou CYCLE/NOCYCLE.
  - START WITH não pode ser modificado usando ALTER.

Privilégios de Objeto

- Você pode conceder os privilégios UPDATE, REFERENCES e INSERT em colunas individuais de uma tabela.
- Por exemplo:

```
GRANT UPDATE (salary)
  ON employees TO steven_king
```

- É possível restringir o privilégio SELECT criando uma view com um subconjunto de colunas e concedendo o privilégio SELECT somente na view.
- Você não pode conceder SELECT em colunas individuais.

Privilégios de Objeto

- Um privilégio concedido em um sinônimo é convertido em um privilégio na tabela básica referenciada pelo sinônimo.
- Em outras palavras, um sinônimo é simplesmente um nome novo e mais fácil de usar.
- Usar esse nome para conceder um privilégio é o mesmo que conceder o privilégio na própria tabela.

Palavra-chave PUBLIC

- O proprietário de uma tabela pode usar a palavra-chave PUBLIC para conceder acesso a todos os usuários.
- O exemplo mostrado abaixo permite que todos os usuários no sistema consultem os dados da tabela DEPARTMENTS de Alice.

```
GRANT select
ON alice.departments
TO PUBLIC;
```

A Palavra-chave PUBLIC

- Se uma instrução não usa o nome completo de um objeto, o servidor Oracle inicia implicitamente o nome do objeto com o nome (ou esquema) do usuário atual.
- Se o usuário Scott consulta a tabela DEPARTMENTS, por exemplo, o sistema seleciona a partir da tabela SCOTT.DEPARTMENTS.
- Se uma instrução não usa o nome completo de um objeto e o usuário atual não possui um objeto com esse nome, o sistema inicia o nome do objeto com PUBLIC.

A Palavra-chave PUBLIC

- Por exemplo, se o usuário Scott consulta a tabela USER_OBJECTS, mas não possui essa tabela, o sistema seleciona a partir da view do dicionário de dados por meio do sinônimo público PUBLIC.USER_OBJECTS.

Confirmando Privilégios Concedidos

- Se você tentar executar uma operação não autorizada, como excluir uma linha de uma tabela para a qual não tenha o privilégio DELETE, o servidor Oracle não permite que a operação seja feita.
- Se o servidor Oracle mostrar a mensagem de erro "table or view does not exist" (a tabela ou view não existe), você executou uma das ações a seguir:
  - Nomeou uma tabela ou view que não existe
  - Tentou executar uma operação em uma tabela ou view para a qual não tem o privilégio apropriado.

Privilégios de Exibição

- Você pode acessar o dicionário de dados para exibir seus privilégios.
- A tabela mostrada descreve várias views do dicionário de dados.
- Usando o Oracle Application Express Developer, acesse SQL Workshop, Utilities, Object Reports.
- Os privilégios do usuário podem ser exibidos na seção Security Reports.

Privilégios de Exibição

View do Dicionário de Dados	Descrição
ROLE_SYS_PRIVS	Privilégios de sistema concedidos a atribuições
ROLE_TAB_PRIVS	Privilégios de tabela concedidos a atribuições
USER_ROLE_PRIVS	Atribuições que podem ser acessadas pelo usuário
USER_TAB_PRIVS_MADE	Privilégios de objeto concedidos nos objetos do usuário
USER_TAB_PRIVS_RECD	Privilégios de objeto concedidos ao usuário
USER_COL_PRIVS_MADE	Privilégios de objeto concedidos nas colunas dos objetos do usuário
USER_COL_PRIVS_RECD	Privilégios de objeto concedidos ao usuário em colunas específicas
USER_SYS_PRIVS	Lista os privilégios de sistema concedidos ao usuário

Terminologia

Estes são os principais termos usados nesta lição:

- Privilégio CREATE SESSION
- Privilégio GRANT
- Privilégios de objeto
- Segurança de objetos
- Privilégio
- Privilégio PUBLIC
- Atribuição

Terminologia

Estes são os principais termos usados nesta lição:

- Esquema
- Privilégios de sistema
- Segurança de Sistema

Resumo

Nesta lição, você deverá ter aprendido a:

- Identificar a diferença entre privilégios de objeto e privilégios de sistema
- Construir os dois comandos necessários para permitir que um usuário acesse um banco de dados
- Construir e executar uma instrução GRANT… ON …TO para atribuir privilégios aos objetos no esquema a outros usuários e/ou PUBLIC
- Consultar o dicionário de dados para confirmar os privilégios concedidos


ORACLE
Academy