
ORACLE
Academy

Programação de Banco de Dados com SQL

17-2
Criando e Revogando Privilégios de Objeto

ORACLE Academy

Objetivos

Esta lição abrange os seguintes objetivos:

- Explicar o que uma atribuição e quais são suas vantagens
- Construir uma instrução para criar uma atribuição e conceder privilégios para ela
- Construir uma instrução GRANT .. ON .. TO.. WITH GRANT OPTION para atribuir privilégios em objetos no seu esquema a outros usuários e/ou PUBLIC
- Construir e executar uma instrução para revogar privilégios de objeto de outros usuários e/ou PUBLIC

Objetivos

Esta lição abrange os seguintes objetivos:

- Distinguir entre privilégios e atribuições
- Explicar a finalidade de um link de banco de dados

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.

Atribuições

- Uma atribuição é um grupo nomeado de privilégios relacionados que podem ser concedidos a um usuário.
- Esse método torna mais fácil revogar e manter privilégios.
- Um usuário pode ter acesso a várias atribuições, e vários usuários podem receber a mesma atribuição.
- As atribuições normalmente são criadas para um aplicativo de banco de dados.

Atribuições

- Para conceder uma atribuição, o DBA deve primeiro criá-la.
- Em seguida, ele pode conceder privilégios à atribuição, e a atribuição aos usuários.

```
CREATE ROLE manager;
```

```
Atribuição criada.
```

```
GRANT create table, create view TO manager;
```

```
Concessão dada com êxito.
```

```
GRANT manager TO jennifer_cho;
```

```
Concessão dada com êxito.
```

Atribuições

- Use a seguinte sintaxe para criar uma atribuição:

```
CREATE ROLE nome_atribuição;
```

- Depois que a atribuição é criada, o DBA pode usar a instrução GRANT para conceder a atribuição aos usuários e conceder privilégios à atribuição.

Atribuições

- O exemplo mostrado cria uma atribuição de gerente e, em seguida, permite que os gerentes criem tabelas e views.
- Depois, concede a atribuição ao usuário.
- Agora, o usuário pode criar tabelas e views.

```
CREATE ROLE manager;
```

```
Atribuição criada.
```

```
GRANT create table, create view TO manager;
```

```
Concessão dada com êxito.
```

```
GRANT manager TO jennifer_cho;
```

```
Concessão dada com êxito.
```

Atribuições

- Se forem concedidas várias atribuições aos usuários, eles recebem todos os privilégios associados a todas as atribuições.
- Observação: CREATE ROLE é um privilégio de sistema que não foi emitido para as aulas do Academy.

```
CREATE ROLE manager;
```

```
Atribuição criada.
```

```
GRANT create table, create view TO manager;
```

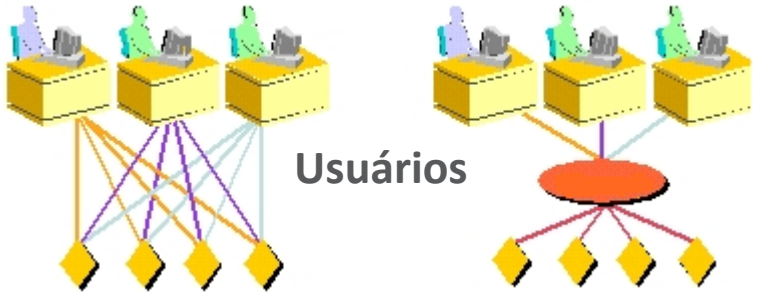
```
Concessão dada com êxito.
```

```
GRANT manager TO jennifer_cho;
```

```
Concessão dada com êxito.
```

Características de Atribuições

- Atribuições são grupos nomeados de privilégios relacionados.
- Podem ser concedidas a usuários.
- Simplificam o processo de concessão e revogação de privilégios.
- São criadas por um DBA.



Concedendo Privilégios de Objeto

- Use a seguinte sintaxe para conceder privilégios de objeto:

```
GRANT priv_objeto [(lista_colunas)]
ON nome_objeto
TO {usuário|atribuição|PUBLIC}
[WITH GRANT OPTION];
```

Sintaxe	Definição
priv_objeto	é o privilégio de objeto a ser concedido
lista_colunas	especifica uma coluna de uma tabela ou view na qual privilégios são concedidos
ON nome_objeto	é o objeto no qual os privilégios são concedidos
TO usuário|atribuição	identifica o usuário ou a atribuição à qual o privilégio é concedido
PUBLIC	concede privilégios de objeto para todos os usuários
WITH GRANT OPTION	Permite ao grantee conceder os privilégios de objeto a outros usuários e atribuições

Diretrizes de Privilégios de Objeto

- Para conceder privilégios em um objeto, ele deve estar no seu próprio esquema, ou você deve ter recebido o privilégio por meio de WITH GRANT OPTION.
- O proprietário de um objeto pode conceder qualquer privilégio de objeto para qualquer outro usuário ou atribuição do banco de dados.
- O proprietário de um objeto adquire automaticamente todos os privilégios de objeto.

Exemplos de GRANT

- Scott King (nome de usuário: scott_king) criou uma tabela de clientes.
- No Exemplo 1 à direita, todos os usuários recebem permissão para selecionar a partir dessa tabela.
- O Exemplo 2 concede privilégios UPDATE para Jennifer e para a atribuição de gerente em colunas específicas da tabela de Scott.

```
1. GRANT SELECT
   ON clients
   TO PUBLIC;

2. GRANT UPDATE(first_name,
       last_name)
   ON clients
   TO jennifer_cho, manager;

3. SELECT  *
   FROM scott_king.clients;

4. CREATE SYNONYM clients
   FOR scott_king.clients;

5. SELECT *
   FROM clients;
```

Exemplos de GRANT

- Se Jennifer agora quiser selecionar dados da tabela de Scott, a sintaxe que ela deverá usar está no Exemplo 3.
- Jennifer também poderia criar um sinônimo para a tabela de Scott e selecionar a partir dele.
- Veja a sintaxe nos Exemplos 4 e 5.

```
1. GRANT SELECT
   ON clients
   TO PUBLIC;

2. GRANT UPDATE(first_name,
       last_name)
   ON clients
   TO jennifer_cho, manager;

3. SELECT  *
   FROM scott_king.clients;

4. CREATE SYNONYM clients
   FOR scott_king.clients;

5. SELECT *
   FROM clients;
```

Exemplos de GRANT

- Privilégios de objeto diferentes estão disponíveis para tipos diferentes de objetos de esquema.
- Um usuário automaticamente possui todos os privilégios de objetos contidos em seu esquema.
- Um usuário pode conceder qualquer privilégio de objeto em qualquer esquema de objeto que possua para qualquer outro usuário ou atribuição.

```
1. GRANT SELECT
   ON clients
   TO PUBLIC;

2. GRANT UPDATE(first_name,
       last_name)
   ON clients
   TO jennifer_cho, manager;

3. SELECT  *
   FROM scott_king.clients;

4. CREATE SYNONYM clients
   FOR scott_king.clients;

5. SELECT *
   FROM clients;
```

WITH GRANT OPTION

- Um privilégio que seja concedido usando a cláusula WITH GRANT OPTION pode ser passado pelo grantee para outros usuários e atribuições.
- Quando o privilégio do concessor é revogado, os privilégios de objeto concedidos usando a cláusula WITH GRANT OPTION também o são.

WITH GRANT OPTION

- O exemplo abaixo dá ao usuário Scott acesso à sua tabela de clientes, com privilégios para consultar e adicionar linhas à tabela.
- O exemplo também permite a Scott conceder esses privilégios a outras pessoas:

```
GRANT  SELECT, INSERT
ON   clients
TO   scott_king
WITH GRANT OPTION;
```

A 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 de clientes de Jason:

```
GRANT  SELECT
ON   jason_tsang.clients
TO   PUBLIC;
```

Objeto DELETE

- 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:
  - Referenciou uma tabela ou view que não existe
  - Tentou executar uma operação em uma tabela ou view para a qual não tem os privilégios apropriados

Revogando Privilégios de Objeto

- Você pode remover os privilégios concedidos a outros usuários usando a instrução REVOKE.
- Quando você usa a instrução REVOKE, os privilégios especificados são revogados dos usuários indicados e de quaisquer outros usuários a quem eles foram concedidos usando a cláusula WITH GRANT OPTION.

Revogando Privilégios de Objeto

- Use a seguinte sintaxe para revogar privilégios de objeto:

```
REVOKE {privilégio [, privilégio...]|ALL}
ON  objeto
FROM {usuário[, usuário...]|atribuição|PUBLIC}
[CASCADE CONSTRAINTS];
```

- CASCADE CONSTRAINTS é necessário para remover as constraints de integridade referencial feitas para o objeto por meio do privilégio REFERENCES.

With Grant Option

- O exemplo abaixo revoga os privilégios SELECT e INSERT dados aos usuário Scott na tabela de clientes.

```
REVOKE SELECT, INSERT
ON clients
FROM scott_king;
```

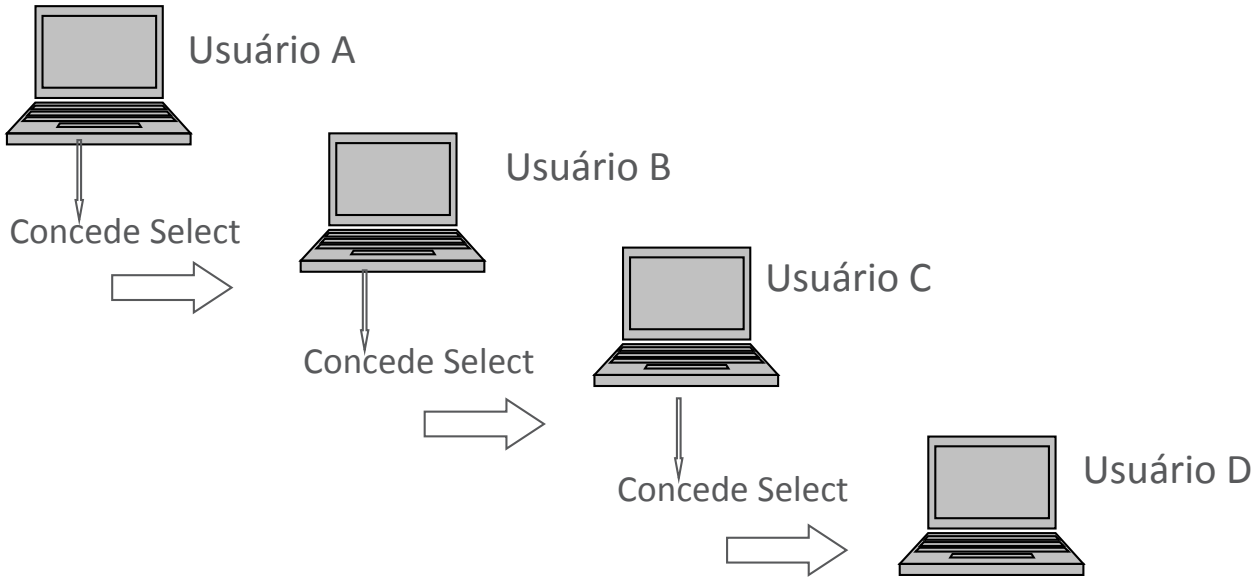
- Se um usuário receber um privilégio com a cláusula WITH GRANT OPTION, ele também poderá concedê-lo usando a mesma cláusula.
- Isso significa que é possível haver uma cadeia longa de grantees, mas não são permitidas concessões circulares.

With Grant Option

- Se o proprietário revogar um privilégio de um usuário que concedeu privilégios para outros usuários, a instrução de revogação se estende para todos os privilégios concedidos.

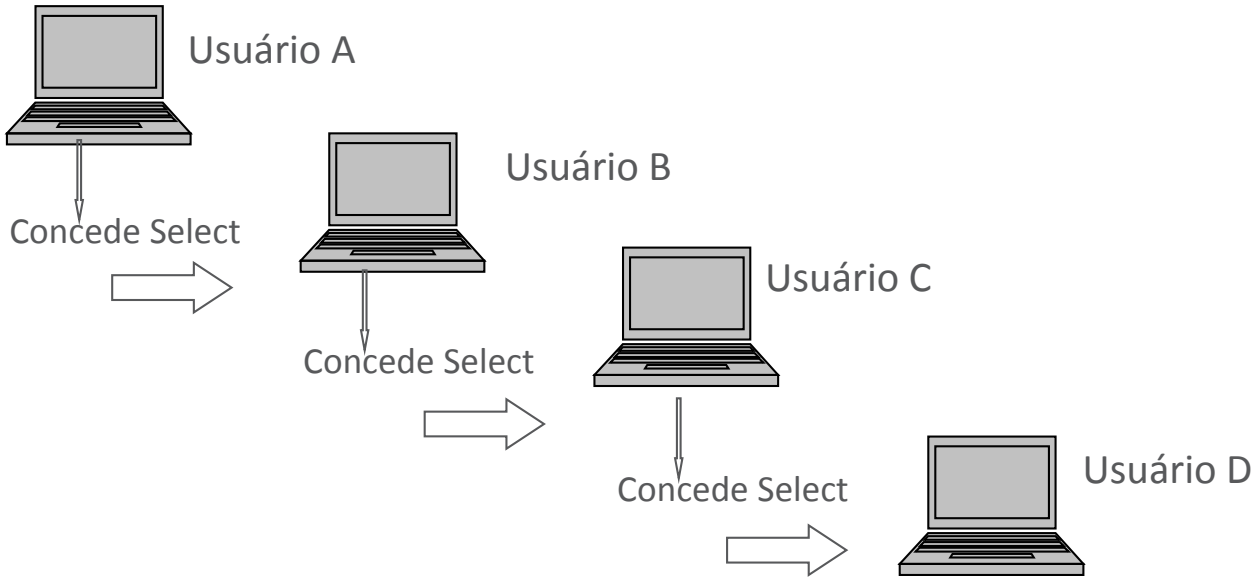
With Grant Option

- Por exemplo, se o usuário A conceder privilégios SELECT em uma tabela para o usuário B, incluindo a cláusula WITH GRANT OPTION, o usuário B poderá conceder ao usuário C o privilégio SELECT, incluindo a cláusula WITH GRANT OPTION também.



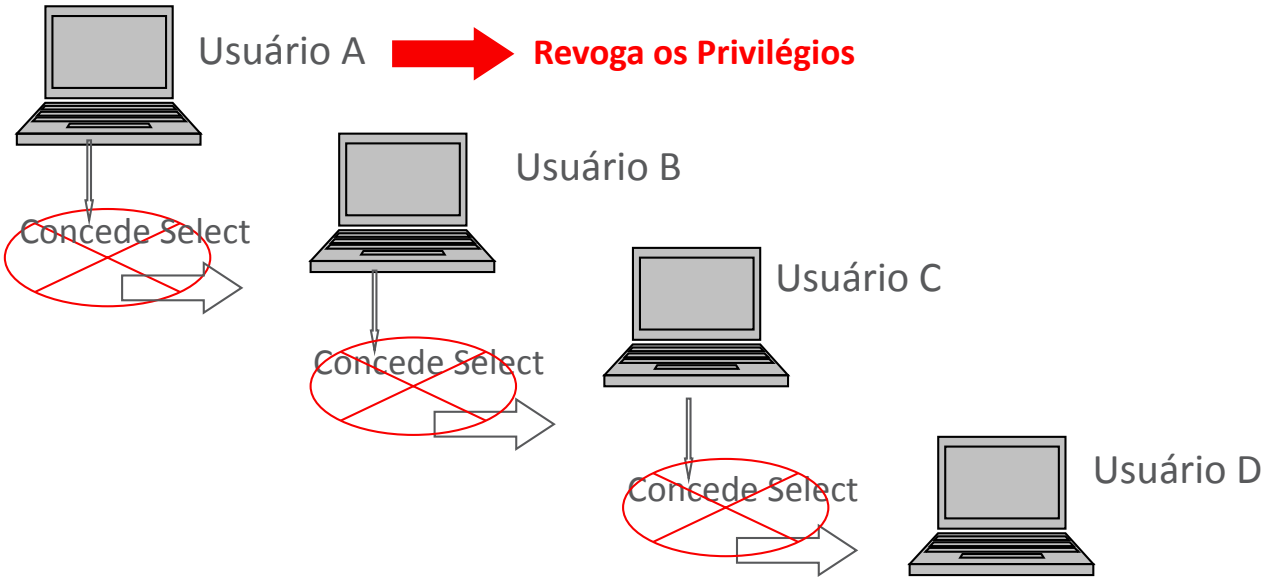
With Grant Option

- Agora, o usuário C pode conceder ao usuário D o privilégio SELECT.



With Grant Option

- No entanto, se o usuário A revogar os privilégios do usuário B, os privilégios concedidos aos usuários C e D também o serão.



Sinônimos Privados e Públicos

- Como mencionado anteriormente nesta lição, você pode criar um sinônimo para eliminar a necessidade de qualificar o nome do objeto com o esquema e obter um nome alternativo para uma tabela, view, sequência, procedure ou outro objeto.
- Os sinônimos podem ser privados (padrão) ou público.
- Um sinônimo público pode ser criado pelos Administradores do Banco de Dados ou pelos usuários do banco de dados que receberam privilégios para isso, mas nem todos podem criar sinônimos públicos automaticamente.
- Observação: o privilégio CREATE PUBLIC SYNONYM não foi concedido para os alunos do Academy.

Atribuições e Privilégios

- Há várias diferenças entre Atribuições e Privilégios:
- O privilégio de um usuário é seu direito de executar um tipo particular de instrução SQL ou de acessar o objeto de outro usuário.
- Todos os privilégios são definidos pelo Oracle.
- As atribuições, por sua vez, são criadas pelos usuários (geralmente, administradores) e são usados para agrupar privilégios ou outras atribuições.

Atribuições e Privilégios

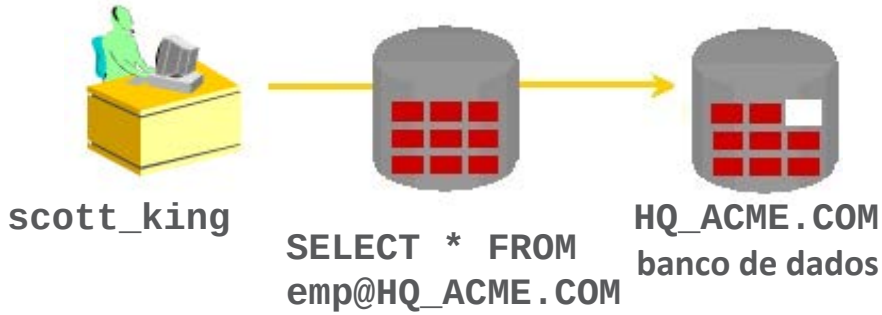
- Eles são criados para facilitar o gerenciamento da concessão de vários privilégios ou atribuições aos usuários.
- Os Privilégios vêm com o banco de dados e as Atribuições são feitas pelos Administradores do Banco de Dados ou pelos usuários de um banco de dados em particular

Links de Banco de Dados

- Um link de banco de dados é um ponteiro que define um caminho unidirecional de comunicação entre um banco de dados Oracle e outro banco de dados.
- O ponteiro de link é, na verdade, definido como um registro em uma tabela do dicionário de dados.
- Para acessar o link, você deve estar conectado ao banco de dados local que contém o registro do dicionário de dados.

Links de Banco de Dados

- A conexão de um link de banco de dados é "unidirecional" porque um cliente conectado ao banco de dados local A pode usar um link armazenado no banco de dados A para acessar informações no banco de dados remoto B, mas os usuários conectados ao banco de dados B não podem usar o mesmo link para acessar o banco de dados A.
- CREATE DATABASE LINK – No Oracle Application Express, não existe uma conexão constante com o banco de dados e, como resultado, este recurso não está disponível.



Links de Banco de Dados

- Se os usuários locais no banco de dados B quiserem acessar os dados no banco de dados A, eles deverão definir um link que seja armazenado no dicionário de dados do banco de dados B.
- A conexão de um link de banco de dados fornece aos usuários locais acesso aos dados em um banco de dados remoto.
- Para essa conexão ocorrer, cada banco de dados no sistema distribuído deverá ter um nome global exclusivo.
- O nome global do banco de dados identifica exclusivamente um servidor de banco de dados em um sistema distribuído.

Links de Banco de Dados

- A grande vantagem dos links de banco de dados é que eles permitem aos usuários acessar os objetos de outro usuário em um banco de dados remoto, de modo que estejam vinculados pelo conjunto de privilégios do proprietário do objeto.
- Em outras palavras, um usuário local pode acessar um banco de dados remoto sem precisar ser um usuário dele.
- O exemplo mostra o usuário scott_king acessando a tabela EMP no banco de dados remoto com o nome global HQ.ACME.COM.

Links de Banco de Dados

- Normalmente, o Administrador do Banco de Dados é responsável por criar o link de banco de dados.
- A view do dicionário USER_DB_LINKS contém informações sobre os links aos quais um usuário tem acesso.
- Depois que o link de banco de dados for criado, você poderá gravar instruções SQL para os dados na instalação remota.
- Se um sinônimo for definido, você poderá usá-lo na gravação das instruções SQL.

Links de Banco de Dados

- Por exemplo:

```
CREATE PUBLIC SYNONYM HQ_EMP
 FOR emp@HQ.ACME.COM;
```

- Em seguida, grave uma instrução SQL que use o sinônimo:

```
SELECT *
FROM HQ_EMP;
```

- Você não pode conceder privilégios em objetos remotos.

Terminologia

Estes são os principais termos usados nesta lição:

- Privilégio CREATE ROLE
- WITH GRANT OPTION
- Privilégio REVOKE
- Instrução REVOKE
- Sinônimo Público
- Sinônimo Privado
- Links de Banco de Dados

Resumo

Nesta lição, você deverá ter aprendido a:

- Explicar o que uma atribuição e quais são suas vantagens
- Construir uma instrução para criar uma atribuição e conceder privilégios para ela
- Construir uma instrução GRANT .. ON .. TO.. WITH GRANT OPTION para atribuir privilégios em objetos no seu esquema a outros usuários e/ou PUBLIC
- Construir e executar uma instrução para revogar privilégios de objeto de outros usuários e/ou PUBLIC

Resumo

Nesta lição, você deverá ter aprendido a:

- Distinguir entre privilégios e atribuições
- Explicar a finalidade de um link de banco de dados


ORACLE
Academy