12

Controlando o Acesso dos Usuários

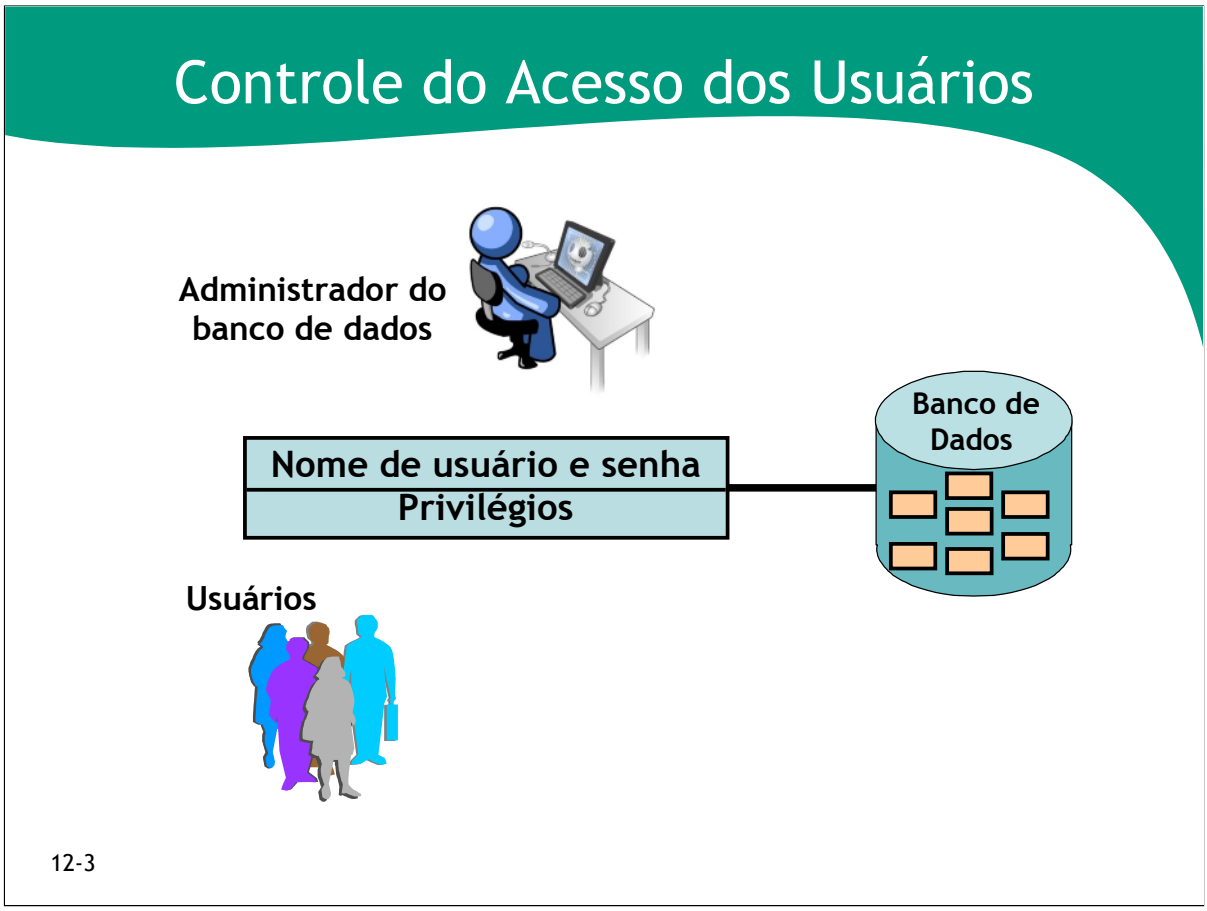
Objetivos deste Capítulo

- Ao concluir este capítulo, você poderá:
  - Diferenciar privilégios de sistema de privilégios de objeto
  - Conceder privilégios em tabelas
  - Exibir privilégios do dicionário de dados
  - Criar e conceder roles
  - Distinguir privilégios de roles

12-2

Objetivos deste Capítulo

Neste capítulo, você aprenderá a controlar o acesso a objetos específicos do banco de dados e a adicionar novos usuários com níveis distintos de privilégios de acesso.



Controle do Acesso dos Usuários

Em um ambiente com vários usuários, você deve manter a segurança de acesso e uso do banco de dados. Com a segurança de banco de dados do Oracle, você pode fazer o seguinte:

- Controlar o acesso ao banco de dados
- Permitir acesso a objetos específicos do banco de dados
- Confirmar privilégios concedidos e recebidos com o dicionário de dados Oracle
- Criar sinônimos para objetos de banco de dados

É possível classificar a segurança de um banco de dados em duas categorias: segurança do sistema e segurança de dados. A segurança do sistema abrange o acesso e o uso do banco de dados no nível do sistema, como o nome de usuário e a senha, o espaço em disco alocado para os usuários e as operações do sistema que os usuários podem executar. A segurança do banco de dados abrange o acesso e o uso dos objetos do banco de dados e as ações que os usuários podem executar nesses objetos.

Privilégios

- Segurança do banco de dados:
  - Segurança do sistema
  - Segurança de dados
- Privilégios de sistema: acesso ao banco de dados.
- Privilégios de objeto: manipulação do conteúdo dos objetos do banco de dados
- Esquemas: conjuntos de objetos, como tabelas, visões e sequências

12-4

Privilégios

Privilégios são direitos de executar comandos SQL específicos. O DBA (administrador de banco de dados) é o usuário que deve ter a capacidade de criar usuários e conceder acesso de usuários ao banco de dados e seus objetos. Os usuários precisam de *privilégios do sistema* para obter acesso ao banco de dados, e de *privilégios de objeto* para manipular o conteúdo dos objetos do banco de dados. Também é possível oferecer aos usuários o privilégio de conceder privilégios adicionais a outros usuários ou roles.

Esquemas

Um *esquema* é um conjunto de objetos, como tabelas, visões e sequências. O esquema pertence a um usuário do banco de dados e tem o mesmo nome do usuário.

Privilégios de Sistema

- Existem mais de 100 privilégios disponíveis.
- O administrador de banco de dados tem privilégios de sistema de alto nível para tarefas como:
  - Criar novos usuários
  - Remover usuários
  - Remover tabelas
  - Fazer backup de tabelas

12-5

Privilégios de Sistema

Existem mais de 100 privilégios de sistema distintos disponíveis para usuários e roles. Em geral, eles são fornecidos pelo administrador do banco de dados.

Privilégios Típicos de DBA

Privilégio de Sistema	Operações Autorizadas
CREATE USER	O usuário pode criar outros usuários Oracle
DROP USER	O usuário pode eliminar outro usuário.
DROP ANY TABLE	O usuário pode eliminar tabelas de qualquer esquema.
BACKUP ANY TABLE	O usuário pode efetuar backup de qualquer tabela em qualquer esquema com o utilitário de exportação.
SELECT ANY TABLE	O usuário pode consultar tabelas, visões ou snapshots de qualquer esquema
CREATE ANY TABLE	O usuário pode criar tabelas em qualquer esquema.

Criando Usuários

- O DBA cria usuários com o comando `CREATE USER`.

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

```
CREATE USER   rh
IDENTIFIED BY rh;
Usuário criado.
```


Criando Usuários

O DBA (administrador de banco de dados) cria o usuário executando o comando `CREATE USER`. Nesse momento, o usuário não tem nenhum privilégio. Depois, o DBA pode conceder privilégios a esse usuário. Esses privilégios determinam o que o usuário pode fazer no do banco de dados.

O slide informa a sintaxe resumida de criação de um usuário.

Na sintaxe:

usuário	é o nome do usuário a ser criado
senha	especifica que o usuário deve efetuar login com esta senha

Privilégios de Sistema

- Depois de criar um usuário, o DBA pode conceder privilégios de sistema específicos a ele.

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

- Um desenvolvedor de aplicações, por exemplo, pode ter os seguintes privilégios de sistema:
  - CREATE SESSION
  - CREATE TABLE
  - CREATE SEQUENCE
  - CREATE VIEW
  - CREATE PROCEDURE

12-7

Privilégios de Sistema

Depois de criar um usuário, o DBA pode conceder privilégios a ele.

Privilégio de Sistema	Operações Autorizadas
CREATE SESSION	Estabelecer conexão com o banco de dados
CREATE TABLE	Criar tabelas no esquema do usuário
CREATE SEQUENCE	Criar uma sequência no esquema do usuário
CREATE VIEW	Criar uma visão no esquema do usuário
CREATE PROCEDURE	Criar um procedimento, uma função ou um pacote armazenado no esquema do usuário

Na sintaxe:

privilégio	é o privilégio de sistema a ser concedido
usuário|role|PUBLIC	é o nome do usuário, o nome da role ou PUBLIC designa que todo usuário receberá o privilégio

Os privilégios de sistema que o usuário conectado possui podem ser encontrados na visão de dicionário de dados SESSION_PRIVS.

Privilégios de Sistema

- O DBA concede privilégios de sistema a um usuário através do comando `grant`

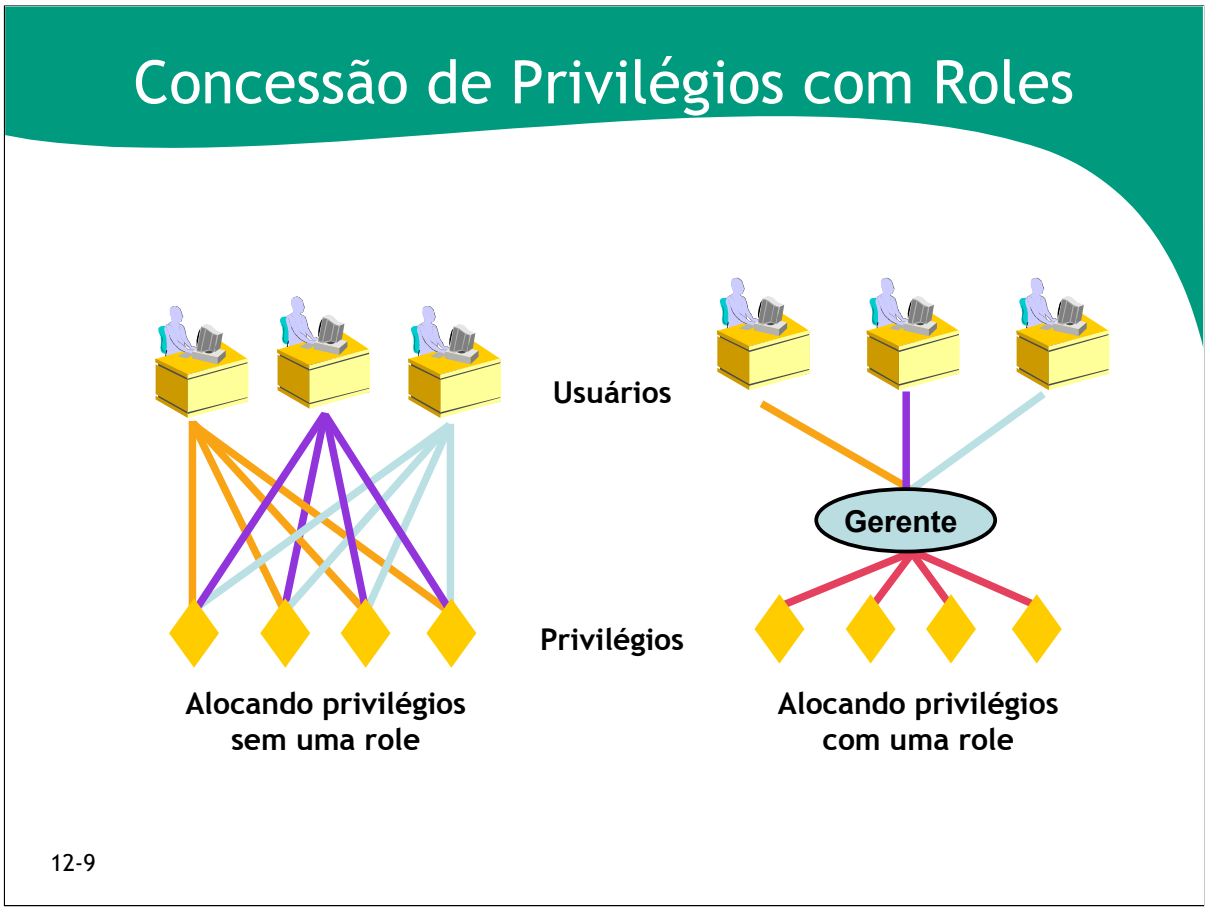
```
GRANT  create session, create table,
       create sequence, create view
TO     usuario;
Concessão bem-sucedida.
```

12-8

Privilégios de Sistema (continuação)

O DBA usa o comando `GRANT` para conceder privilégios de sistema para um usuário. Após receber os privilégios, o usuário pode usá-los imediatamente.

No exemplo do slide, o usuário recebeu os privilégios para criar sessões, tabelas, sequências e visões.



Concessão de Privilégios com Roles

Uma role é um grupo nomeado de privilégios que podem ser concedidos com a usuários de banco de dados. Esse método facilita a revogação e a manutenção de privilégios.

Um usuário pode ter acesso a várias roles e é possível atribuir a mesma role a vários usuários. Em geral, as roles são criadas para aplicações de banco de dados.

Criando e Atribuindo uma Role

Primeiro, o DBA deve criar a role. Depois, ele pode atribui privilégios e usuários para a role.

Sintaxe

```
CREATE   ROLE role;
```

Na sintaxe:

role é o nome da role criada

Após a criação da role, o DBA pode usar o comando `GRANT` para atribuir usuários e privilégios à role.

Concessão de Privilégios com Roles

- Crie uma role

```
CREATE ROLE gerente;
Atribuição criada.
```

- Conceda privilégios a uma role

```
GRANT create table, create view
TO gerente;
Concessão bem-sucedida.
```

- Conceda uma role a usuários

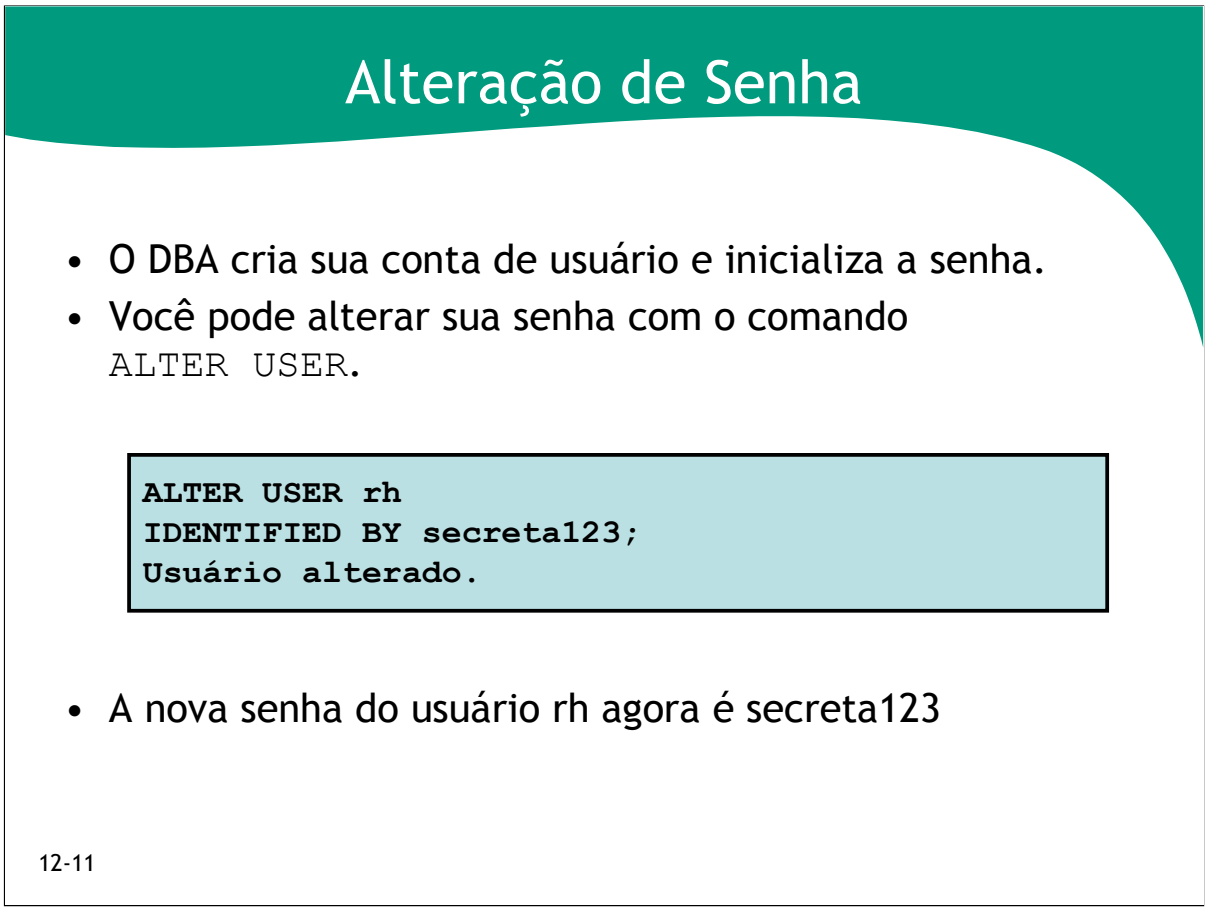
```
GRANT gerente TO usuario1, usuario2;
Concessão bem-sucedida.
```

12-10

Concessão de Privilégios com Roles

O exemplo do slide cria uma role de gerente e permite que os gerentes criem tabelas e visões. Em seguida, a role de gerente é concedida aos usuários USUARIO1 e USUARIO2. Agora, USUARIO1 e USUARIO2 podem criar tabelas e visões.

Se os usuários receberam a concessão de várias roles, eles receberão todos os privilégios associados a todas as roles.



Alteração de Senha

O DBA cria uma conta e inicializa uma senha para cada usuário. Você pode alterar sua senha com o comando `ALTER USER`.

Sintaxe

```
ALTER USER usuário IDENTIFIED BY nova_senha;
```

Na sintaxe:

user	é o nome do usuário
nova_senha	especifica a nova senha

Embora seja possível usar esse comando para alterar a senha, existem várias outras opções de alteração que podem ser feitas com o comando `ALTER USER`. Você precisa ter o privilégio `ALTER USER` para alterar outras opções.

O SQL*Plus conta com um comando `PASSWORD` (`PASSW`) que pode ser usado para alterar a senha de um usuário quando ele está conectado.

Privilégios de Objeto

Privilégio de Objeto	Tabela	Visão	Sequência	Procedimento
ALTER	√		√	
DELETE	√	√		
EXECUTE				√
INDEX	√			
INSERT	√	√		
REFERENCES	√			
SELECT	√	√	√	
UPDATE	√	√		

12-12

Privilégios de Objeto

Um *privilégio de objeto* é um privilégio ou direito de realizar determinada ação em uma tabela, uma visão, uma sequência ou um procedimento específico. Cada objeto tem um conjunto determinado de privilégios que podem ser concedidos. A tabela do slide lista os privilégios de vários objetos. Lembre-se de que os únicos privilégios que se aplicam a uma sequência são `SELECT` e `ALTER`. Você pode restringir `UPDATE`, `REFERENCES` e `INSERT` com a especificação de um subconjunto de colunas atualizáveis. É possível restringir um privilégio `SELECT` criando uma visão com um subconjunto de colunas e concedendo esse privilégio à visão. Um privilégio concedido em um sinônimo é convertido em um privilégio na tabela-base referenciada pelo sinônimo.

Privilégios de Objeto

- Os privilégios de objeto variam de acordo com o objeto.
- O proprietário tem todos os privilégios no objeto.
- O proprietário pode conceder privilégios específicos em seus próprios objetos com o comando GRANT

```
GRANT {privilégio [, privilégio...]|ALL} [(colunas)]
ON     objeto
TO     {usuário[, usuário...]|role|PUBLIC}
[WITH GRANT OPTION];
```

12-13

Privilégios de Objeto (continuação)

Existem privilégios de objeto distintos disponíveis para tipos diferentes de objetos de esquema. Um usuário tem automaticamente todos os privilégios para os objetos contidos no seu próprio esquema. Um usuário pode conceder privilégios de objeto em qualquer objeto de seu próprio esquema a outros usuários ou roles através do comando GRANT. Se a concessão incluir WITH GRANT OPTION, o usuário que recebeu o privilégio poderá conceder com o privilégio de objeto a outros usuários. Caso contrário, ele poderá usar o privilégio, mas sem poder concedê-lo a outros usuários.

Na sintaxe:

privilégio	é o privilégio de objeto a ser concedido
ALL	especifica todos os privilégios do objeto
colunas	especifica a coluna de uma tabela ou visão na qual os privilégios são concedidos
objeto	é o objeto no qual os privilégios são concedidos
usuário	identifica a quem o privilégio é concedido
PUBLIC	concede privilégios de objeto a todos os usuários
WITH GRANT OPTION	permite a quem recebeu o privilégio concedê-los a outros usuários ou roles

Concessão de Privilégios de Objeto

- Conceda privilégios de consulta na tabela FUNCIONARIO.

```
GRANT  select
ON     funcionario
TO     joao, maria;
Concessão bem-sucedida.
```

- Conceda privilégios para atualizar colunas específicas a usuários e roles.

```
GRANT  update (nome_departamento, cod_localidade)
ON     departamento
TO     jose, gerente;
Concessão bem-sucedida.
```

12-14

Concessão de Privilégios de Objeto

- Para conceder privilégios em um objeto, esse objeto deve estar no seu próprio esquema ou você precisa ter recebido os privilégios com a opção WITH GRANT OPTION.
- Um proprietário de objeto pode conceder qualquer privilégio no objeto a outros usuários ou roles do banco de dados.
- O proprietário de um objeto adquire automaticamente todos os privilégios nesse objeto.

O primeiro exemplo do slide concede aos usuários Joao e Maria o privilégio para consultar a tabela FUNCIONARIO. O segundo exemplo concede privilégios UPDATE em colunas específicas da tabela DEPARTAMENTO a Jose e à role chamada gerente.

Para usar um comando SELECT a fim de obter dados da tabela FUNCIONARIO, Joao ou Maia deverá usar esta sintaxe:

```
SELECT  * FROM proprietario.funcionario;
```

Como alternativa, esses usuários podem criar um sinônimo para a tabela e executar o comando SELECT com o sinônimo:

```
CREATE SYNONYM func FOR proprietario.funcionario;
SELECT * FROM func;
```

Opção WITH GRANT OPTION

- Ofereça a um usuário autoridade para passar adiante privilégios.

```
GRANT  select, insert
ON     departamento
TO     miguel
WITH   GRANT OPTION;
Concessão bem-sucedida.
```

- Permita a todos os usuários do sistema consultar dados da tabela DEPARTAMENTO de Alice.

```
GRANT  select
ON     alice.departamento
TO     PUBLIC;
Concessão bem-sucedida.
```

12-15

Opção WITH GRANT OPTION

Um usuário que tenha recebido um privilégio com a cláusula WITH GRANT OPTION poderá passá-lo a outros usuários e roles. Os privilégios de objeto concedidos com a cláusula WITH GRANT OPTION são revogados quando o privilégio do concessor é revogado.

O exemplo do slide concede ao usuário Miguel acesso à tabela DEPARTAMENTO com os privilégios para consultá-la e adicionar linhas a ela. O exemplo também mostra que Miguel pode conceder esses privilégios a outros usuário do banco de dados.

Palavra-chave PUBLIC

Um proprietário de uma tabela pode conceder acesso a todos os usuários usando a palavra-chave PUBLIC.

O segundo exemplo permite a todos os usuários do banco de dados consultar dados da tabela DEPARTAMENTO de Alice.

Confirmando Privilégios Concedidos

Visão de Dicionário de Dados	Descrição
ROLE_SYS_PRIVS	Privilégios de sistema concedidos a roles
ROLE_TAB_PRIVS	Privilégios de tabela concedidos a roles
USER_ROLE_PRIVS	Roles acessíveis ao usuário
USER_TAB_PRIVS_MADE	Privilégios de objeto concedidos para os 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	Privilégios de sistema concedidos ao usuário

Confirmando Privilégios Concedidos

Se você tentar executar uma operação não autorizada – por exemplo, remover uma linha de uma tabela na qual não tem o privilégio `DELETE` – o Oracle não permitirá que a operação ocorra.

Se o Oracle enviar a mensagem de erro "ORA-00942: a tabela ou view não existe", você executou uma destas operações:

- Referenciou uma tabela ou uma visão que não existe
- Tentou executar uma operação em uma tabela ou visão cujo privilégio apropriado você não tem

Você pode acessar o dicionário de dados para exibir os privilégios que tem. A tabela do slide descreve diversas visões de dicionário de dados que têm essa finalidade.

Revogando Privilégios de Objeto

- Use o comando REVOKE para revogar privilégios concedidos
- Os privilégios concedidos a outros através da cláusula WITH GRANT OPTION também são revogados

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

12-17

Revogando Privilégios de Objeto

Você pode revogar privilégios concedidos a outros usuários usando o comando REVOKE. Quando você usa o comando REVOKE, os privilégios especificados são revogados dos usuários especificados e dos outros usuários aos quais esses privilégios são concedidos pelo usuário revogado (cláusula WITH GRANT OPTION do comando GRANT).

Na sintaxe:

A opção CASCADE é necessária para remover constraints de integridade referenciais feitas para o objeto que está tendo seu privilégio revogado por meio do privilégio REFERENCES.

Revogando Privilégios de Objeto

- Como usuária Alice, revogue os privilégios SELECT e INSERT concedidos com grant ao usuário Miguel na tabela DEPARTAMENTO.

```
REVOKE  select, insert
ON      departamento
FROM    scott;
Revogação bem-sucedida.
```

12-18

Revogando Privilégios de Objeto (continuação)

O exemplo do slide revoga os privilégios SELECT e INSERT concedidos ao usuário Miguel na tabela DEPARTAMENTO.

Se for concedido a um usuário um privilégio com a cláusula WITH GRANT OPTION, esse usuário também poderá conceder o privilégio com essa cláusula, possibilitando a existência de uma longa cadeia de usuários com permissões de objetos, mas não são permitidos grants circulares. Se o proprietário revogar um privilégio de um usuário que concedeu esse privilégio a outros usuários, todos os privilégios concedidos serão revogados em cascata.

Por exemplo, se o usuário A conceder o privilégio SELECT em uma tabela ao usuário B, incluindo a cláusula WITH GRANT OPTION, o usuário B também poderá conceder ao usuário C o privilégio SELECT com a mesma cláusula, e o usuário C poderá, então, conceder ao usuário D o privilégio SELECT. Se o usuário A revogar os privilégios do usuário B, os privilégios concedidos aos usuários C e D também serão revogados.

Exercício 12

12-19

Exercício 12

1. Que privilégio deve ser concedido a um usuário para que ele efetue logon no servidor Oracle? Este privilégio é de sistema ou de objeto?

   _____

2. Que privilégio deve ser concedido a um usuário para que ele crie tabelas?

   _____

3. Se você criar uma tabela, quem poderá passar privilégios a outros usuários da sua tabela?

   _____

4. Você é o DBA. Você está criando vários usuários que precisam dos mesmos privilégios de sistema. O que você deve usar para facilitar o seu trabalho?

   _____

5. Que comando você pode usar para alterar a senha?

   _____

Forme equipes ou duplas para executar o restante dos exercícios.

6. Conceda a outra Equipe acesso à sua tabela `DEPARTAMENTO`. Faça com que a outra Equipe conceda a você acesso de consulta à tabela `DEPARTAMENTO` dela.
7. Consulte todas as linhas da sua própria tabela `DEPARTAMENTO`.
8. Adicione uma nova linha à tabela `DEPARTAMENTO`. A Equipe 1 deve adicionar Educação como departamento número 500. A Equipe 2 deve adicionar Recursos Humanos como departamento número 510. Consulte a tabela da outra equipe.
9. Crie um sinônimo para a tabela `DEPARTAMENTO` da outra equipe.
10. Consulte todas as linhas da tabela `DEPARTAMENTO` da outra equipe, usando o sinônimo.

Exercício 12 (continuação)

11. Consulte o dicionário de dados `USER_TABLES` para ver as informações das suas tabelas.
12. Consulte a visão de dicionário de dados `ALL_TABLES` para ver as informações de todas as tabelas que você pode acessar. Exclua as suas tabelas.
13. Revogue o privilégio `SELECT` da outra equipe.
14. Remova a linha que você inseriu na tabela `DEPARTAMENTO` na etapa 8 e salve as alterações.