20

管理权限

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.

目标

完成这一课的学习后，您应该能达到下列目标：

- 标识系统与对象权限
- 授予和撤消权限

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.

管理权限

有两种 Oracle 用户权限：

- 系统权限：具备该权限的用户可在数据库中执行特定操作
- 对象权限：具备该权限的用户可访问并操纵特定对象

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.

权限

权限是指执行特定类型的 SQL 语句或访问另一个用户的对象的权利。包括以下权利：

- 连接到数据库
- 创建表
- 从另一用户的表中选择行
- 执行另一用户的已存储过程

系统权限：

每一系统权限都允许用户执行某一特定的数据库操作或某类数据库操作，例如，创建表空间的权限就是一种系统权限。

大约240项

对象权限：

每一对象权限都允许用户对特定对象（如表、视图、序列、过程、函数或程序包）执行特定的操作。

DBA 的权限控制包括：

- 为用户提供执行某种操作的权限
- 授予和撤消执行系统功能的权限
- 将权限直接授予用户或角色

- 将权限授予所有用户（PUBLIC）

系统权限

- 有 240 种不同的系统权限。
- 权限中的关键字 ANY 表示用户在任何方案中都具备这种权限。
- GRANT 命令为一个用户或一组用户添加一项权限。
- REVOKE 命令则用来删除权限。

ORACLE

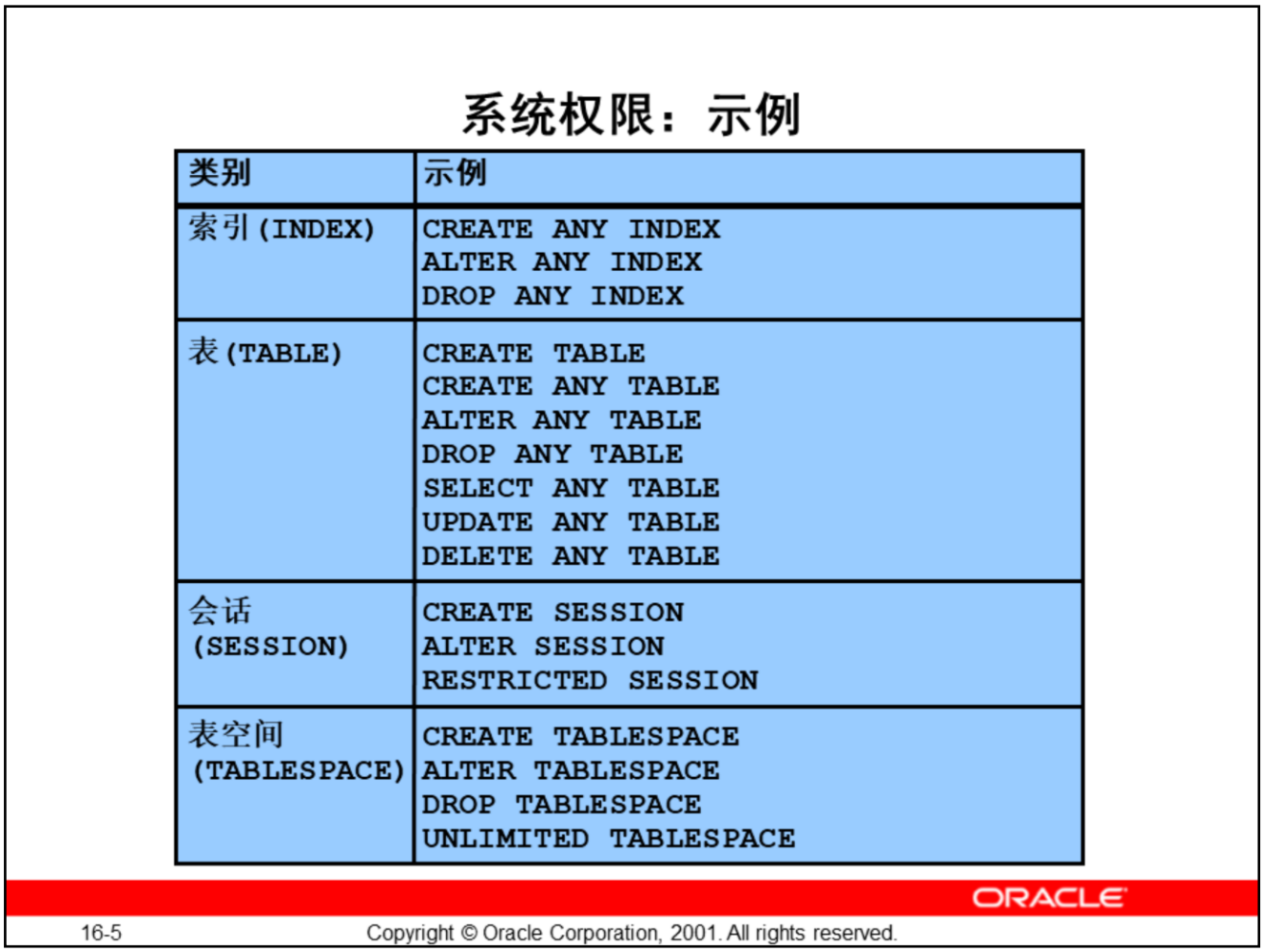
Copyright © Oracle Corporation, 2001. All rights reserved.

系统权限

系统权限可分为以下几类：

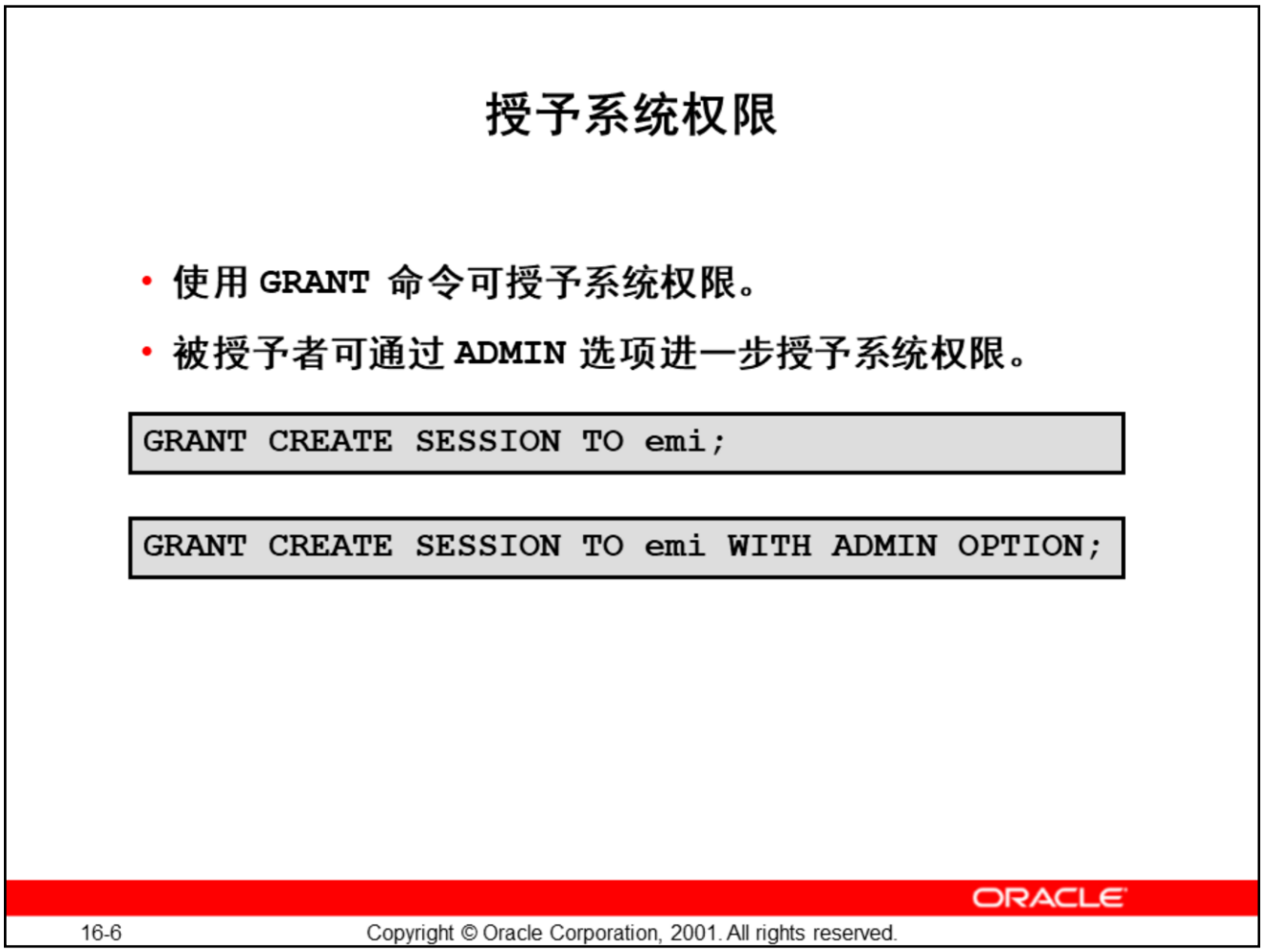
- 允许执行系统范围操作的权限；如 CREATE SESSION，CREATE TABLESPACE
- 允许管理用户自己方案中的对象的权限；如 CREATE TABLE
- 允许管理任何方案中的对象的权限；如 CREATE ANY TABLE

可使用 DDL 命令 GRANT 和 REVOKE 控制权限，这两个命令为用户或角色添加和撤消系统权限。有关角色的详细信息，请参考 “管理角色” 一课。



系统权限：示例

- 没有 CREATE INDEX 权限。
- CREATE TABLE 包括 CREATE INDEX 和 ANALYZE 命令。用户必须有表空间的限额，或必须被授予 UNLIMITED TABLESPACE 权限。
- 诸如 CREATE TABLE、CREATE PROCEDURE 或 CREATE CLUSTER 等权限包括删除这些对象的权限。
- 无法将 UNLIMITED TABLESPACE 授予角色。
- DROP ANY TABLE 权限是截断另一方案中的表所必需的。



授予系统权限

使用 SQL 语句 GRANT 为用户授予系统权限。

被授予者可通过 ADMIN 选项进一步为其他用户授予系统权限。使用 ADMIN 选项授予系统权限时应小心。这样的权限通常只限于安全管理员使用，很少授予其他用户。

```
GRANT {system_privilege|role}
     [, {system_privilege|role} ]...
    TO {user|role|PUBLIC}
     [, {user|role|PUBLIC} ]...
    [WITH ADMIN OPTION]
```

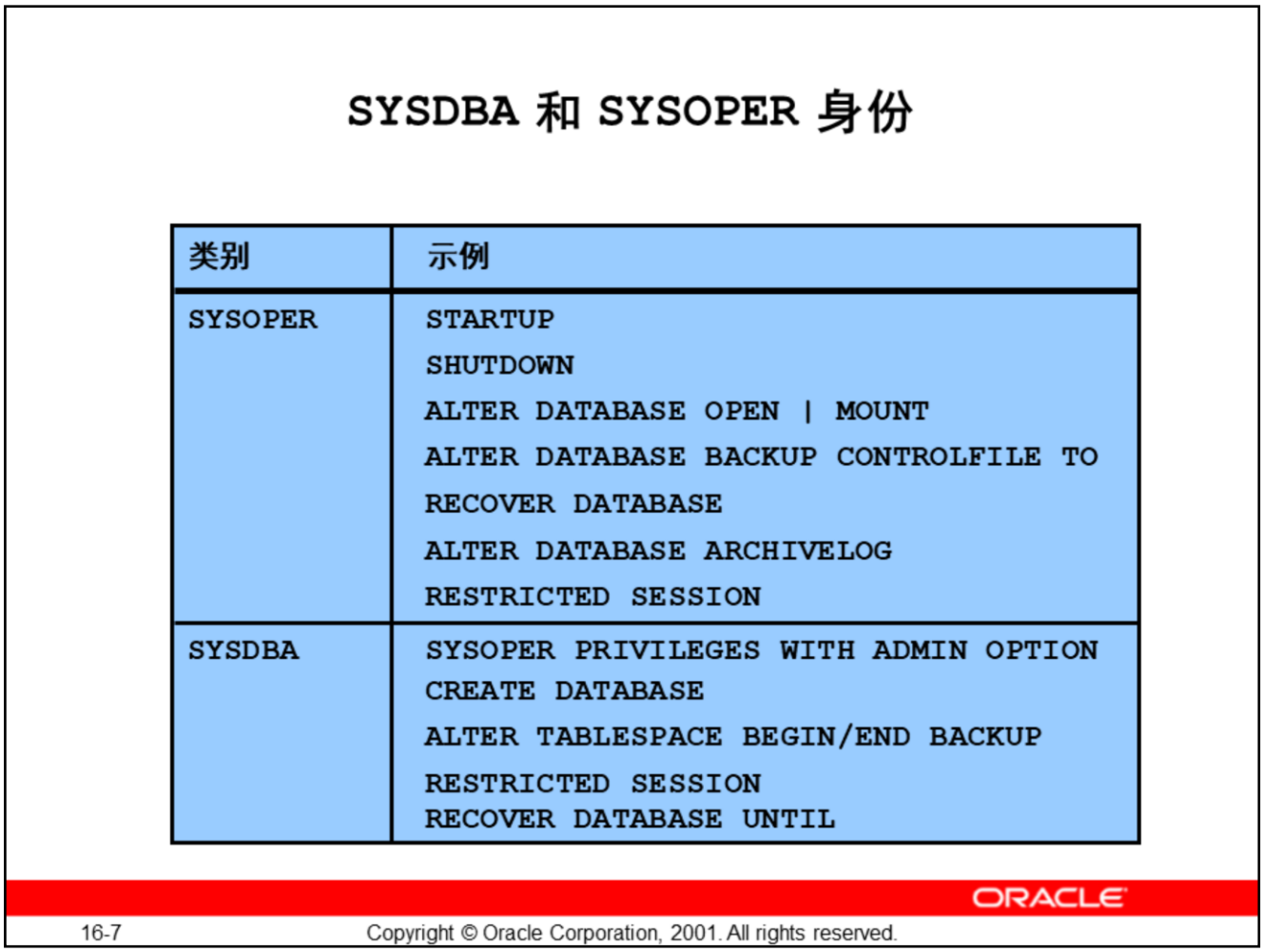
其中：

system_privilege：指定要授予的系统权限

Role：指定要授予的角色名

PUBLIC：将系统权限授予所有用户

WITH ADMIN OPTION：允许被授予者进一步为其他用户或角色授予权限或角色



SYSDBA 和 SYSOPER 身份

只有数据库管理员可以使用管理员权限与数据库连接。以 SYSDBA 身份连接可以授予用户不受限制的权限，以便对数据库或数据库中的对象执行任何操作。

Sys用户可以执行

grant sysdba|sysoper to xxx

给某个用户赋以sysdba或sysoper身份。

系统权限限制

- O7_DICTIONARY_ACCESSIBILITY 参数（此参数自12.2版本后不再支持）
- 控制有关 SYSTEM 权限的限制
- 如果设置为 TRUE，允许访问 SYS 方案中的对象
- 缺省值为 FALSE：可确保允许访问任何方案的系统权限不允许访问 SYS 方案

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.

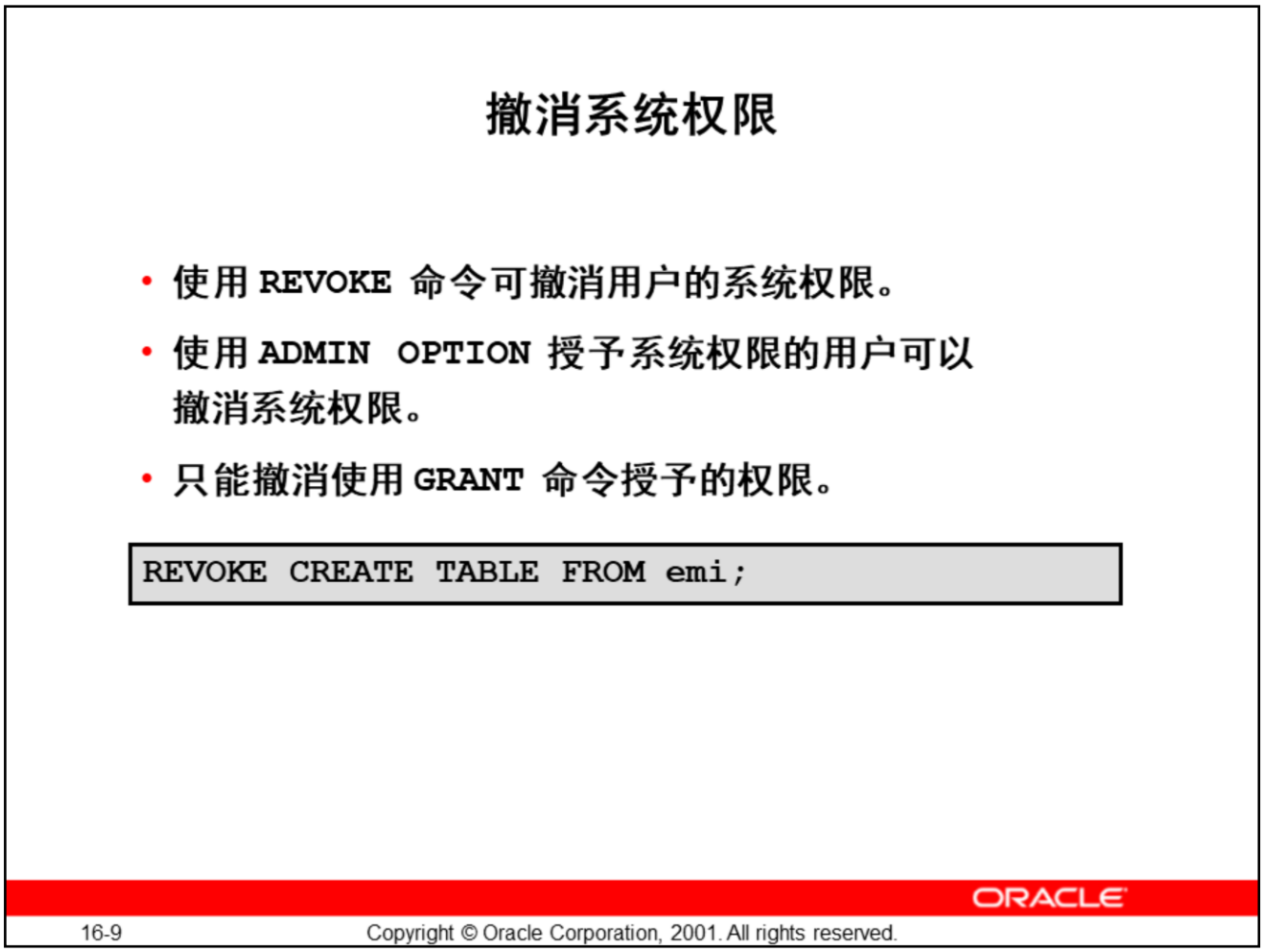
系统权限限制

Oracle中的字典保护机制可防止未经授权的用户访问字典对象。

只有角色 SYSDBA 和 SYSOPER 可以访问字典对象。允许访问其他方案中的对象的系统权限并不授予您对字典对象的访问权限。例如，SELECT ANY TABLE 权限允许您访问其它方案中的视图和表，但不允许您选择字典对象（基表、视图、程序包和同义词）。

如果该参数设置为 TRUE, 则允许访问 SYS 方案中的对象（Oracle7 行为）。如果该参数设置为 FALSE，则允许访问其它方案中的对象的 SYSTEM 权限不允许访问字典方案中的对象。

例如，如果 O7_DICTIONARY_ACCESSIBILITY=FALSE，则 SELECT ANY TABLE 语句将允许访问除 SYS 方案外的任何方案中的视图或表（例如，不能访问字典）。系统权限 EXECUTE ANY PROCEDURE 将允许访问除 SYS 方案外的任何其它方案中的过程。



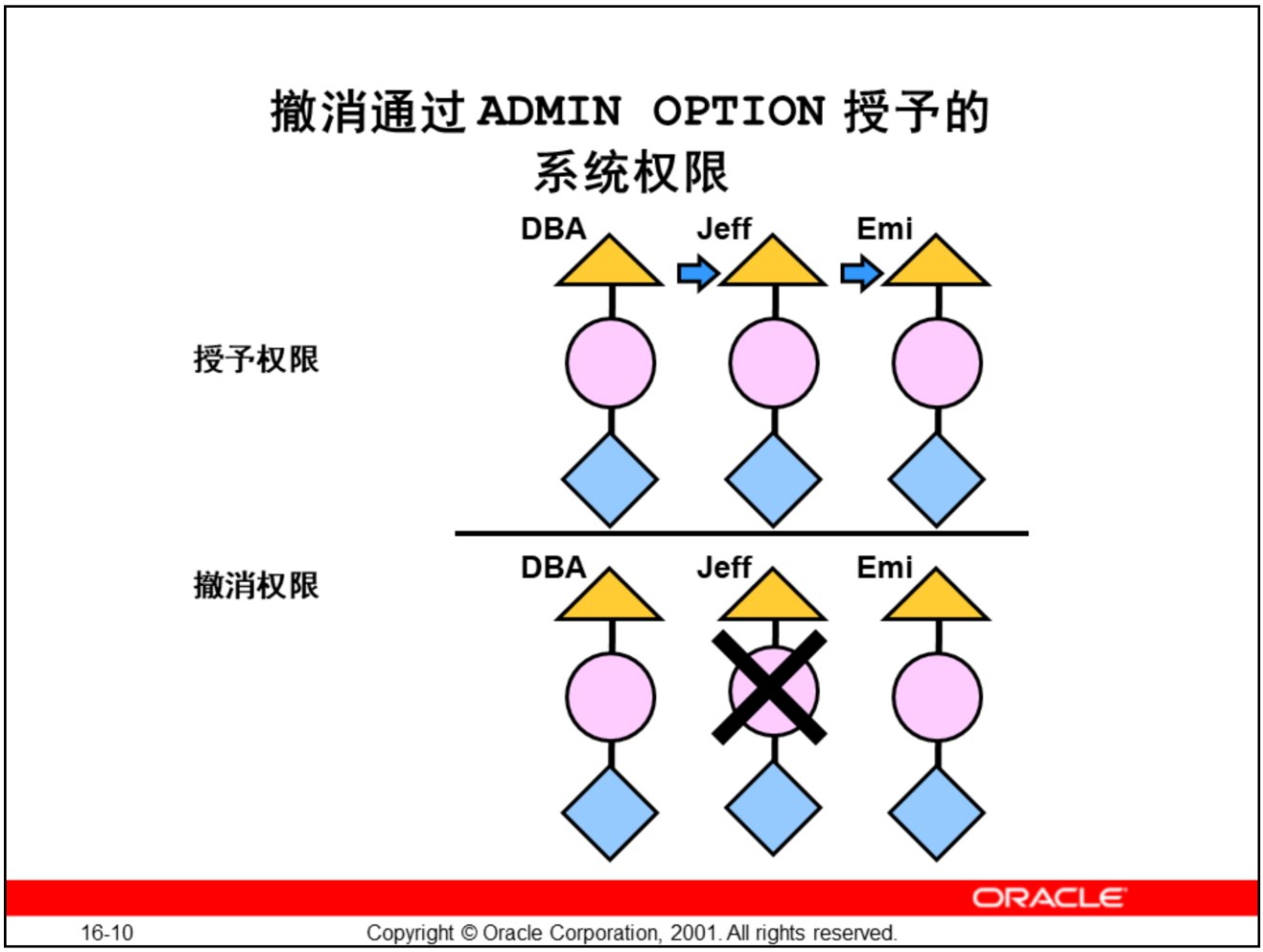
撤消系统权限

可以使用 REVOKE SQL 语句撤消系统权限。使用 ADMIN OPTION 授予系统权限的用户可以撤消任何其他数据库用户的权限。撤消者不必是原先授予该权限的那个用户。

```
REVOKE {system_privilege|role}
 [, {system_privilege|role} ]...
FROM {user|role|PUBLIC}
 [, {user|role|PUBLIC} ]...
```

注：

- REVOKE 命令只能撤消使用 GRANT 命令直接授予的权限。
- 撤消系统权限可能对一些相关对象有影响。例如，如果将 SELECT ANY TABLE 授予某用户，而该用户已创建了使用其它方案中的表的过程或视图，则撤消该权限将使这些过程或视图无效。



撤消系统权限（续）

撤消系统权限时没有级联效果，这与该系统权限是否使用 ADMIN OPTION 授予无关。请仔细阅读下列步骤，它们对这种特性进行了说明。

情况

1. DBA 使用 ADMIN OPTION 将系统权限 CREATE TABLE 授予 Jeff。
2. Jeff 创建一个表。
3. Jeff 将系统权限 CREATE TABLE 授予 Emi。
4. Emi 创建一个表。
5. DBA 撤消 Jeff 的 CREATE TABLE 系统权限。

结果

Jeff 的表依然存在，但是，无法创建新表。

Emi 的表依然存在，并且她仍然拥有 CREATE TABLE 系统权限。

对象权限

对象权限	表	视图	序列	过程
ALTER	√	√	√	√
DELETE	√	√		
EXECUTE				√
INDEX	√	√		
INSERT	√	√		
REFERENCES	√			
SELECT	√	√	√	
UPDATE	√	√		

ORACLE

16-11

Copyright © Oracle Corporation, 2001. All rights reserved.

对象权限

对象权限是一种对于特定的表、视图、序列、过程、函数或程序包执行特定操作的一种权限或权利。上表列出了各种对象的权限。需要注意的是适用于序列的权限只有 SELECT 和 ALTER。通过指定可更新列的子集可以对 UPDATE、REFERENCES 和 INSERT 权限加以限制。通过用列的子集创建视图并授予对于该视图的 SELECT 权限，则可对 SELECT 权限加以限制。对于同义词的授权会转换为对于该同义词所引用的基表的授权。

注：该幻灯片未提供有关对象权限的完整列表。

授予对象权限

- 使用 GRANT 命令授予对象权限。
- 授权必须在授予者方案中，或者授予者必须具有 GRANT OPTION 权限。

```
GRANT EXECUTE ON dbms_output TO jeff;
```

```
GRANT UPDATE ON emi.customers TO jeff WITH
GRANT OPTION;
```

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.

授予对象权限

```
GRANT { object_privilege [(column_list)]
      [, object_privilege [(column_list)] ]...
      |ALL [PRIVILEGES]}
ON  [schema.]object
TO  {user|role|PUBLIC}[, {user|role|PUBLIC} ]...
    [WITH GRANT OPTION]
```

其中：

object_privilege：指定要授予的对象权限

column_list：指定表或视图列（只在授予 INSERT、REFERENCES 或 UPDATE 权限时才指定。）

ALL：将所有权限授予已被授予 WITH GRANT OPTION 的对象

ON object：标识将要被授予权限的对象

WITH GRANT OPTION：使被授予者能够将对象权限授予其他用户或角色

授予对象权限（续）

使用 GRANT 语句授予对象权限。

- 要授予权限，对象必须在您的方案中，或者您已通过 GRANT OPTION 被授予权限。
- 缺省情况下，如果拥有某个对象，则自动获得对该对象的所有权限。
- 若有安全方面的考虑，则将您的对象权限授予其他用户时应谨慎。

撤消对象权限

- 使用 REVOKE 命令可撤消对象权限。
- 撤消权限的用户必须是将被撤消的对象权限的原始授予者。

```
REVOKE SELECT ON emi.orders FROM jeff;
```

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.

撤消对象权限

REVOKE 语句用来撤消对象权限。要撤消对象权限，撤消者必须是将被撤消的对象权限的原始授予者。

使用下列命令撤消对象权限：

```
REVOKE { object_privilege
         [, object_privilege ]...
         | ALL [PRIVILEGES] }
ON  [schema.]object
FROM {user|role|PUBLIC}
         [, {user|role|PUBLIC} ]...
         [CASCADE CONSTRAINTS]
```

撤消对象权限（续）

其中：

object_privilege：指定将撤消的对象权限

ALL：撤消已授予用户的所有对象权限

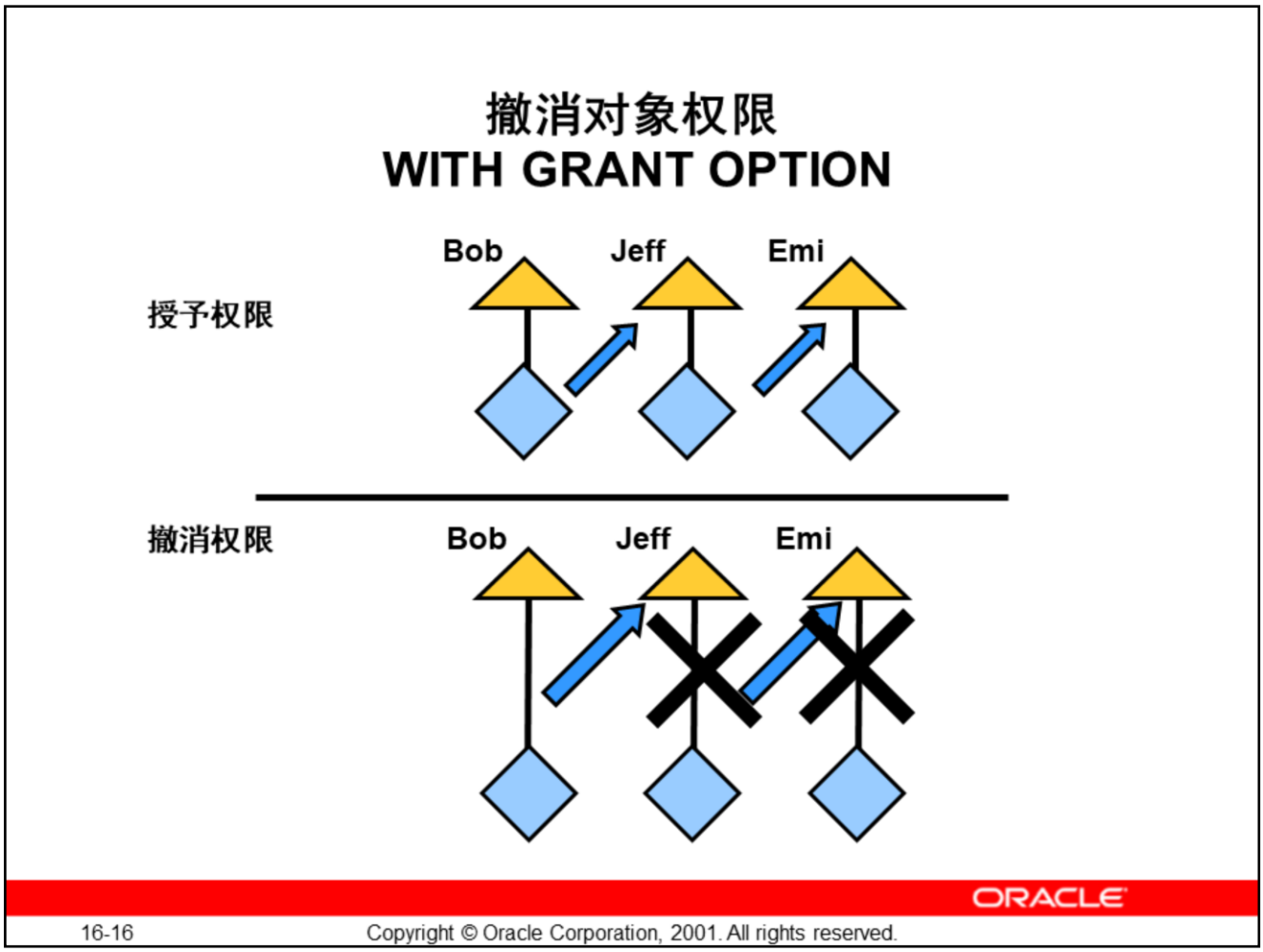
ON：标识将撤消其对象权限的对象

FROM：标识将撤消其对象权限的用户或角色

CASCADE CONSTRAINTS：删除撤消使用 REFERENCES 或 ALL 权限定义的任何引用完整性约束

限制：

授予者只能对其已经授予权限的用户撤消对象权限。



撤消对象权限（续）

撤消与 DML 操作有关的系统权限时，可看到级联效果。例如，如果为某用户授予 SELECT ANY TABLE 权限，并且该用户已经创建了使用某个表的过程，则必须对该用户的方案中包含的所有过程进行重新编译之后，才能使用这些过程。

如果对象权限是用 WITH GRANT OPTION 授予的，则撤消对象权限也将导致级联效果。

请仔细阅读下列步骤，它们对这种特性进行了说明。

情况：

- 通过 GRANT OPTION 授予 Jeff 对于 EMPLOYEES 的 SELECT 对象权限。
- Jeff 将对于 EMPLOYEES 的 SELECT 权限授予 Emi。
- 之后，撤消 Jeff 的 SELECT 权限。该撤消也对 Emi 产生级联影响。

获取权限信息

可以通过查询以下视图来获取有关权限的信息：

- DBA_SYS_PRIVS：授予用户的系统权限
- DBA_TAB_PRIVS：授予用户的对象权限
- DBA_COL_PRIVS：授予用户的字段级对象权限
- SESSION_PRIVS：当前会话具有的系统权限

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.

小结

在这一课中，您应该能够掌握：

- 标识系统与对象权限
- 授予和撤消权限

ORACLE

Copyright © Oracle Corporation, 2001. All rights reserved.