22

审计

目标

完成这一课的学习后，您应该能达到下列目标：

- 概述审计类别
- 对例程启用审计
- 概述审计选项

ORACLE

审计

- 审计即监视选定的用户数据库操作，可用于以下目的：
  - 调查可疑的数据库活动
  - 收集有关特定数据库活动的信息
- 可以按会话审计或按访问审计。

ORACLE

审计

如果任何未经授权的用户试图删除数据，DBA 可以决定对数据库的所有连接，以及对数据库中所有表的所有成功和未成功的删除操作进行审计。DBA 会收集下面这些统计信息，如哪些表正在更新、已执行的逻辑输入/输出 (I/O) 次数、峰期时的并发连接用户数等。

审计项目

- 确定要审计的内容：
  - 用户、语句、系统权限、对象权限
  - 语句执行情况
  - 成功的语句执行情况与/或未成功的语句执行情况
- 管理审计线索：
  - 监视审计线索的增长。
  - 防止未经授权而访问审计线索。

ORACLE

审计原则

通过首先确定审计要求，然后设置可以满足这些要求的最少审计选项来限定审计。要尽可能使用对象审计来减少生成的条目。如果必须使用语句或权限审计，则下列设置可以让审计生成的内容减至最少：

- 指定要审计的用户
- 按会话审计，而不是按访问审计
- 审计成功或失败，但不要既成功又失败

注：审计记录可以写入 SYS.AUD$ 或操作系统的审计线索。能否使用操作系统的审计线索要取决于操作系统。

监视审计线索的增长：

如果审计线索已满，则不能再插入任何审计记录，并且审计过的语句不能成功执行。发布已审计语句的所有用户都将收到错误消息。您必须先释放审计线索中的一些空间，而后才能执行这些语句。

审计原则（续）

监视审计线索的增长（续）：

要确保审计线索不会增长太快，应注意以下要求：

- 只有需要时才启用审计。
- 选择特定的审计选项。
- 严格控制方案对象审计。用户可以对自己拥有的对象打开审计。
- 尽量避免授予 AUDIT ANY 权限，因为它还能让用户打开审计。

定期使用 DELETE 或 TRUNCATE 命令删除审计线索中的审计记录。审计文件位于 $ORACLE_HOME/rdbms/audit 目录中。

保护审计线索：

应保护审计线索，以防添加、修改或删除审计信息。发出以下命令：

```
SQL> AUDIT delete ON sys.aud$ BY ACCESS;
```

可防止审计线索未经授权即被删除；只有 DBA 才拥有 DELETE_CATALOG_ROLE 角色。

将审计线索移到系统表空间外：

随着新记录插入数据库审计线索，表 AUD$ 将无限增长。尽管不应丢弃 AUD$ 表，但是可以从中删除或截断信息，因为其中的行只是为了提供信息，对于运行 Oracle 例程并不是必需的。由于 AUD$ 表在增长后又会收缩，所以应将其存储在系统表空间之外。

若要将 AUD$ 移至 AUDIT_TAB 表空间，则：

- 确保审计当前是禁用的。
- 输入以下命令：

```
SQL> ALTER TABLE aud$ MOVE TABLESPACE AUDIT_TAB;
```

- 输入以下命令：

```
SQL> CREATE INDEX i_aud1 ON aud$(sessionid, ses$tid)
 2   TABLESPACE AUDIT_IDX;
```

- 对例程启用审计。

审计类别

不论是否启用数据库审计，Oracle 都始终将一些数据库操作记录到操作系统审计线索中。这些记录包括：

- 例程启动：审计记录会详述正启动例程的操作系统用户、用户终端标识符、日期和时间戳，以及已启用还是已禁用数据库审计。
- 例程关闭：详述正关闭例程的操作系统用户、用户的终端标识符以及日期和时间戳。
- 管理员权限：详述正以管理员权限连接 Oracle 的操作系统用户。

数据库审计：

数据库审计监视并记录选定的用户数据库操作。有关事件的信息存储在审计线索中。审计线索可用于调查可疑操作。例如，如果未授权的用户正在删除表中的数据，DBA 会决定审计数据库的所有连接，以及对数据库中表行的成功与不成功的删除操作。

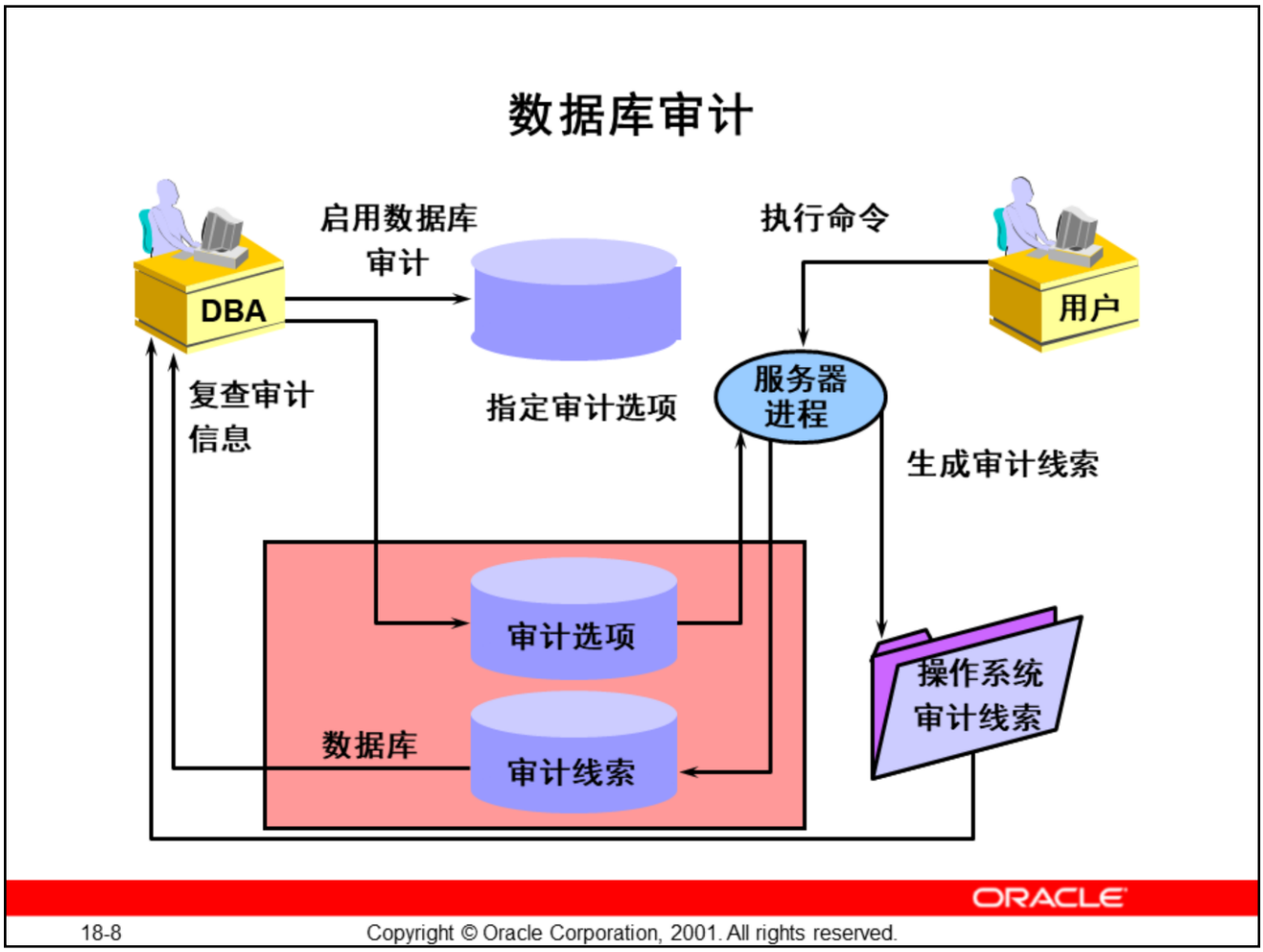
审计类别（续）

数据库审计（续）：

审计也可用于监视并收集关于特定数据库活动的数据。例如，DBA 可以收集有关哪些表正在更新、执行的逻辑 I/O 的操作次数以及峰期时的并发用户连接数等统计信息。

基于值的审计：

数据库审计无法记录列值。若需要跟踪数据库列的更改并存储每个更改的列值，则使用应用程序审计。可以通过客户代码、存储过程或数据库触发器进行应用程序审计。



数据库审计

启用和禁用数据库审计：

确定要审计的内容后，设置初始化参数 AUDIT_TRAIL 对例程启用审计。该参数指明是将审计线索写入数据库表还是操作系统审计线索。

```
AUDIT_TRAIL = value
```

其中，值可以是下列之一：

TRUE 或 DB：启用审计并将所有审计记录定向到数据库审计线索（SYS.AUD$）

OS：启用审计并将所有审计记录定向到操作系统审计线索（如果操作系统上允许）

FALSE 或 NONE：禁用审计

注：没有缺省值。

数据库审计（续）

除非 DBA 已将参数 AUDIT_TRAIL 设置为 DB 或 OS，否则不将审计记录写入审计线索。尽管可随时使用 SQL 语句 AUDIT 和 NOAUDIT，但如果 DBA 已经在初始化文件中设置了参数 AUDIT_TRAIL，则只将记录写入审计线索。

注：操作系统的*安装和配置指南*提供了有关将审计记录写入操作系统审计线索的信息。

指定审计选项：

接下来，使用 AUDIT 命令设置特定的审计选项。通过 AUDIT 命令，可以指出要审计的命令、用户、对象或权限。也可以指出是针对每个事件生成一个审计记录还是针对每个会话生成一次审计记录。如果不再需要某个审计选项，可使用 NOAUDIT 命令关闭它。

语句的执行：

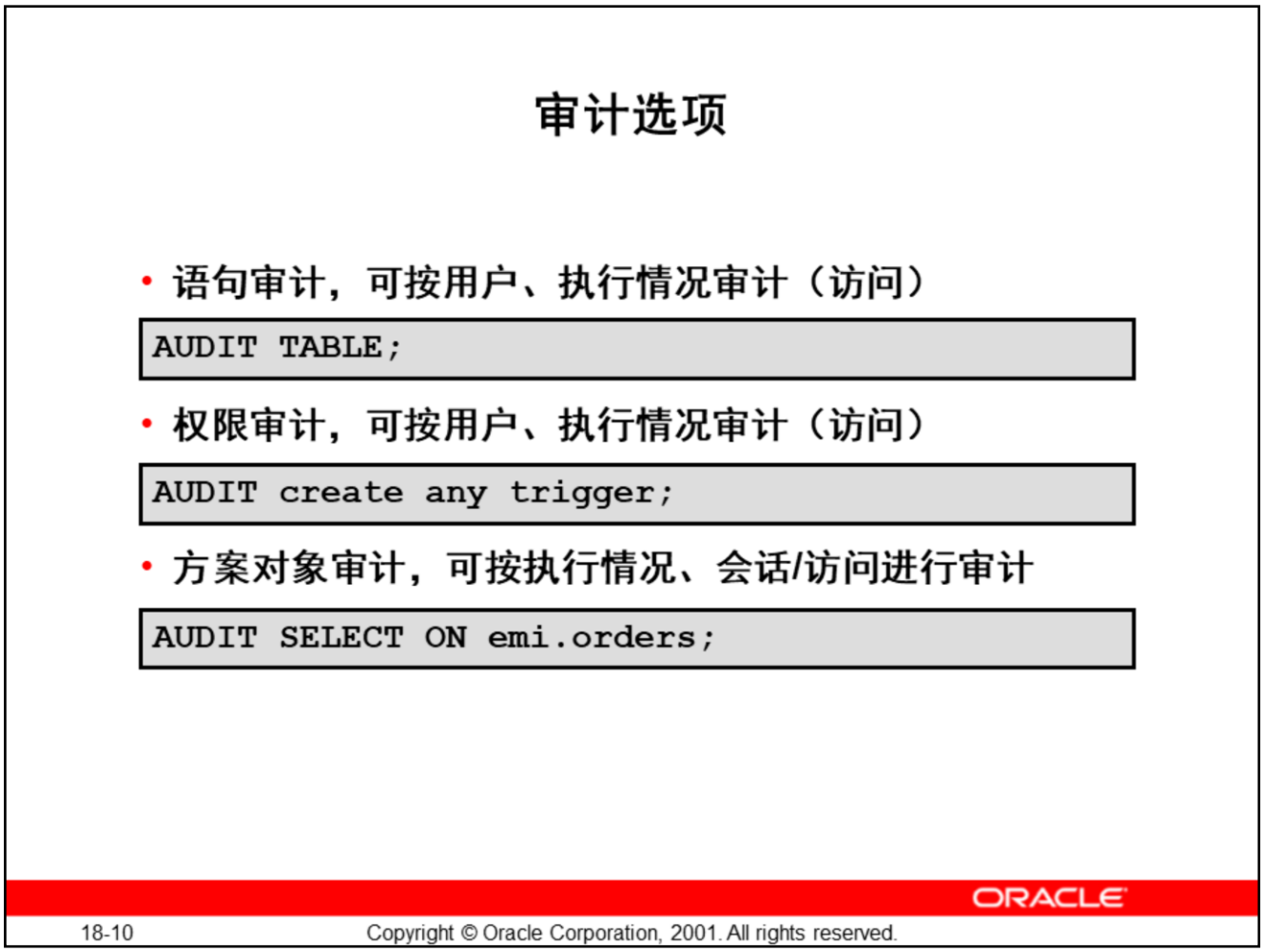
当用户执行 PL/SQL 和 SQL 语句时，服务器进程检查这些审计选项以确定正在执行的语句是否生成审计记录。如果执行的是 PL/SQL 程序单元，则会根据需要对其中的 SQL 语句分别进行审计。由于视图和过程可能引用其它数据库对象，所以执行单个语句可能会生成多个审计记录。

生成审计数据：

审计线索记录的生成和插入与用户的事务处理无关；因此，即使用户的事务处理回退，审计线索记录仍保持原样。由于审计记录在执行阶段生成，语法分析阶段出现的语法错误并不会导致生成审计线索记录。

复查审计信息：

通过从审计线索数据字典视图中选择，或使用操作系统实用程序查看操作系统审计线索，可以检查审计过程中生成的信息。该信息用于调查可疑操作并监视数据库操作。



审计选项

语句审计：

该种审计对 SQL 语句进行选择性审计，而并不审计语句针对的特定方案对象。例如，AUDIT TABLE 跟踪多个 DDL 语句，而与这些语句针对的表无关。可以设置语句审计，以便对数据库中的所选用户或每个用户进行审计，可以针对执行情况（成功/失败）进行审计。只能针对访问审计。

权限审计：

该种审计对执行操作应具有的相应系统权限进行选择性审计，如 AUDIT CREATE ANY TRIGGER。可以设置权限审计对数据库中的所选用户或每个用户进行审计，可以针对执行情况（成功/失败）进行审计，只能针对访问审计。

方案对象审计：

该种审计对特定方案对象上的特定语句进行选择性审计，如 AUDIT SELECT ON HR.EMPLOYEES。方案对象审计始终适用于所有数据库用户。

可以指定任何审计选项，并指定下列条件：

- WHENEVER SUCCESSFUL/WHENEVER NOT SUCCESSFUL
- BY SESSION/BY ACCESS

审计选项

小粒度审计

- 对基于内容的数据访问进行监视
- 通过 DBMS_FGA 程序包实施

ORACLE

审计选项

小粒度审计：对于基于内容的数据访问进行监视。可通过 PL/SQL 程序包 DBMS_FGA 来管理基于值的审计策略。使用 DBMS_FGA 时，DBA 会创建一个针对目标表的审计策略。如果从查询块返回的任何行符合审计条件，就会向审计线索插入一个审计事件条目，包括用户名、SQL 文本、绑定变量、策略名、会话 ID、时间戳与其它属性。

禁用审计：

使用 NOAUDIT 语句以停止由 AUDIT 命令选择的审计。

注：NOAUDIT 语句可以取消先前 AUDIT 语句的作用。要注意 NOAUDIT 语句必须与先前的 AUDIT 语句具有相同的语法，并且它只能取消那个特定语句的作用。因此，如果一个 AUDIT 语句（语句 A）对特定用户启用审计，另一个语句（语句 B）对所有用户启用审计，则对所有用户禁用审计的 NOAUDIT 语句只取消语句 B 的作用，而语句 A 仍然有效，可继续审计其指定的用户。

获取审计信息

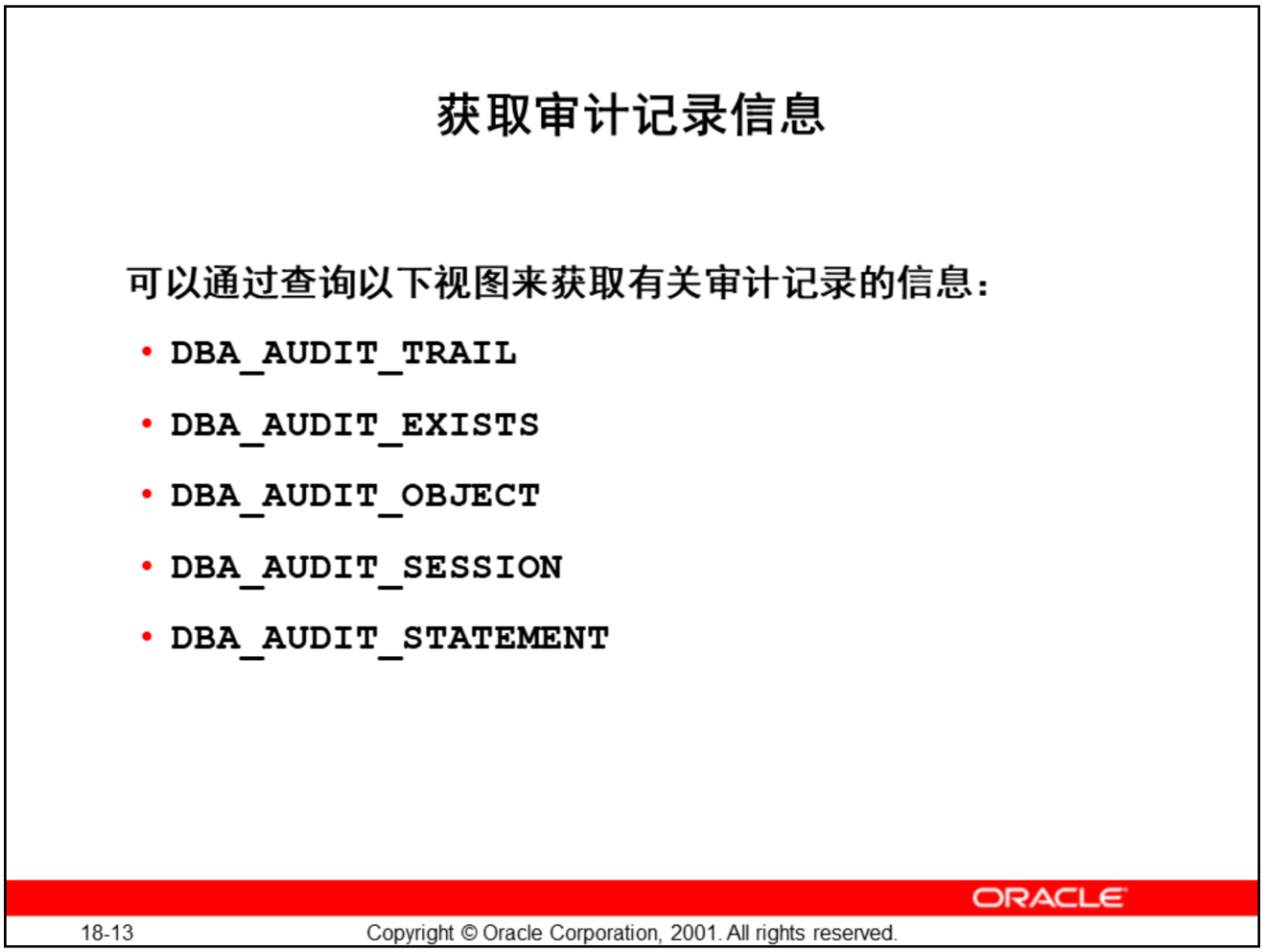
可以通过查询以下视图来获取有关审计的信息：

- ALL_DEF_AUDIT_OPTS
- DBA_STMT_AUDIT_OPTS
- DBA_PRIV_AUDIT_OPTS
- DBA_OBJ_AUDIT_OPTS

ORACLE

获取审计信息

数据字典视图	说明
ALL_DEF_AUDIT_OPTS	缺省审计选项
DBA_STMT_AUDIT_OPTS	语句审计选项
DBA_PRIV_AUDIT_OPTS	权限审计选项
DBA_OBJ_AUDIT_OPTS	方案对象审计选项



获取审计记录信息

列出审计记录：

数据库审计线索（SYS.AUD$）是一个包含在每个 Oracle 数据库字典中的单独表，其中有若干预定义视图。幻灯片中列出了其中的一些视图，这些视图是 DBA 创建的。

数据字典视图	说明
DBA_AUDIT_TRAIL	所有审计线索条目
DBA_AUDIT_EXISTS	有关 AUDIT EXISTS/NOT EXISTS 的记录
DBA_AUDIT_OBJECT	有关方案对象的记录
DBA_AUDIT_SESSION	所有连接和断开连接条目
DBA_AUDIT_STATEMENT	语句审计记录

统一审计(unified auditing)

- CREATE AUDIT POLICY
- ALTER AUDIT POLICY
- DROP AUDIT POLICY
- AUDIT
- NOAUDIT

ORACLE

统一审计

从12C开始的特征

统一审计相关信息

- AUDIT_UNIFIED_POLICIES
- DBA_AUDIT_POLICIES
- DBA_AUDIT_POLICY_COLUMNS

ORACLE

涉及的数据存储的视图

小结

在这一课中，您应该能够掌握：

- 概述审计需要
- 启用和禁用审计
- 确定和使用各种审计选项

ORACLE